Regulamento Interno	Código: RIN.INST.TI.IS.001
Institucional	Versão: 004
Tecnologia da Informação	Data da Emissão: 28/08/2024
Infraestrutura e Segurança da Informação	Vencimento: 5 anos após emissão

REGULAMENTO DE SEGURANÇA DA INFORMAÇÃO

Histórico de Versões

001 - Substituição do documento POL.GE.CTI.INO.001.001 - 19/07/2021

002 - Atualização do Regulamento - Inserido seção LGPD e reorganização do Comitê de Segurança da Informação - 29/11/2021;

003 - Atualização do Art.80º deste documento - 29/04/2022;

004 - Revisão do Regimento por vencimento 28/08/2024.

Fase	Nome	Setor/Unid.	Data	Documento
Elaboração	Rodrigo Silva Santa Rita	Sustentação	19/07/2021	Matrícula: 018691
Análise	Rodrigo Silva Santa Rita	Sustentação	14/08/2024	Matrícula: 018691
	Bryan Valdez Nakasato	Infraestrutura e Segurança da Informação	14/08/2024	Matrícula: 44490
	Vinicius Gomes Silva	Infraestrutura e Segurança da Informação	14/08/2024	Matrícula: 16854
	Rodrigo Miranda	Gestão da Inovação e Tecnologia	20/08/2024	Matrícula: 019974
	Alexandre Garcia D'Aurea	Coordenação Jurídica	28/08/2024	Matrícula: 019772
Aprovação	Floriza Mendes	Diretoria Executiva	28/08/2024	Matrícula: 003368
Aprovação	João Romano	Diretoria Executiva	28/08/2024	Matrícula: 012687

Centro de Estudos e Pesquisas "Dr. João Amorim"
Rua Dr. Lund, 41 - Liberdade
São Paulo-SP - CEP: 01513-020
11 3469-1818
cejam@cejam.org.br
cejam.org.br

SUMÁRIO

CAPÍTULO I - DO OBJETIVO **4**
CAPÍTULO II - DAS DISPOSIÇÕES GERAIS **4**
SEÇÃO I - PERMISSÕES E ORIENTAÇÕES GERAIS 5
SEÇÃO II - ATIVIDADES NÃO PERMITIDAS 5
CAPÍTULO III - GESTÃO DE ATIVOS **6**
SEÇÃO I - ESTAÇÕES DE TRABALHO 7
SEÇÃO II - TELEFONES FIXOS CORPORATIVOS 9
SEÇÃO III - DISPOSITIVOS MÓVEIS CORPORATIVOS 10
SEÇÃO IV - IMPRESSORAS CORPORATIVAS 11
SEÇÃO V - DA UTILIZAÇÃO DE COMPARTILHAMENTO E ARMAZENAMENTO DE ARQUIVOS (SERVIDOR) 11
SEÇÃO VI - DESCARTE DE EQUIPAMENTOS 12
CAPÍTULO IV - GERENCIAMENTO DE IDENTIDADE E ACESSO **13**
SEÇÃO I - CRIAÇÃO DE USUÁRIOS 13
SEÇÃO II - SENHAS 13
SEÇÃO III - BLOQUEIO DE USUÁRIOS 14
SEÇÃO IV - EXCLUSÃO DE USUÁRIOS 14
SEÇÃO V - ALTERAÇÃO DE ACESSO 14
CAPÍTULO V - DO ACESSO A INTERNET **15**
CAPÍTULO VI - CANAIS DE COMUNICAÇÃO VIRTUAL **15**
SEÇÃO I - DA UTILIZAÇÃO DO E-MAIL CORPORATIVO 16
SEÇÃO II - PLATAFORMA DE MENSAGENS INSTANTÂNEAS 17
SEÇÃO III - VÍDEO CHAMADAS E CONFERÊNCIAS VIRTUAIS 18
CAPÍTULO VII - DO ACESSO À REDE CORPORATIVA (CABEADA/WIRELESS) **19**
SEÇÃO I - REDE CORPORATIVA CABEADA 19
SEÇÃO II - REDE CORPORATIVA WIRELESS 19
SEÇÃO II - ACESSO REMOTO À REDE CORPORATIVA 20
CAPÍTULO VIII - DA GESTÃO DE SISTEMAS, SOFTWARES E LICENÇAS **21**
SEÇÃO I - DA UTILIZAÇÃO DE SISTEMAS CORPORATIVOS 22
SEÇÃO II - DA UTILIZAÇÃO PRONTUÁRIO ELETRÔNICO 23
CAPÍTULO IX - DA SEGURANÇA FÍSICA E DO AMBIENTE **26**
CAPÍTULO X - DAS MÍDIAS SOCIAIS **27**
CAPÍTULO XI - DA GESTÃO DE BACKUP **28**
CAPÍTULO XII - DA GESTÃO DE MUDANÇA **28**
CAPÍTULO XIII - DA GESTÃO DE INCIDENTES **29**
SEÇÃO I - PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS 30
CAPÍTULO XIV - DO PLANO DE CONTINGÊNCIA **30**
CAPÍTULO XV - DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO **31**
CAPÍTULO XVI - DA DISCIPLINA NA PROTEÇÃO DE DADOS – LGPD **32**
SEÇÃO I - ORIENTAÇÃO PARA O TRATAMENTO DE DADOS PESSOAIS 34

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

SEÇÃO II - TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS 36
CAPÍTULO XVII – REVISÃO 37
ANEXO I - TERMO DE CONFIDENCIALIDADE 38
ANEXO II - TERMO DE RESPONSABILIDADE DA GUARDA E USO DE CELULAR CORPORATIVO 40

Centro de Estudos e Pesquisas "Dr. João Amorim"
Rua Dr. Lund, 41 - Liberdade
São Paulo-SP - CEP: 01513-020
11 3469-1818
cejam@cejam.org.br
cejam.org.br

CAPÍTULO I - DO OBJETIVO

Art.1°. Este regulamento tem por objetivo normatizar as condutas de todos que atuam no CEJAM ou em seu nome e nortear a construção de procedimentos e manuais internos, referentes à utilização dos recursos tecnológicos utilizados para desempenhar as atividades do CEJAM além da observância à Lei Geral de Proteção de Dados (LGPD) e demais normas em legislação digital, a fim de resguardar as informações da Instituição e das partes interessadas.

Parágrafo único. Todas as orientações contidas neste regulamento estão apoiadas no Código de Ética e Conduta CEJAM, o qual determina a aplicação de medidas em caso de não cumprimento das normativas institucionais.

Art.2°. Além das disposições contidas no **Art.1º**, o presente regulamento é composto de orientações gerais de medidas de segurança da informação, as quais são consolidadas através dos procedimentos e manuais direcionados à tecnologia da informação (TI), considerando a disponibilidade de recursos e a complexidade do serviço na realidade das unidades do CEJAM.

CAPÍTULO II - DAS DISPOSIÇÕES GERAIS

Art.3°. A utilização correta e responsável dos recursos de TI são aplicadas a todos os usuários, inclusive prestadores de serviço e voluntários que, por algum motivo justificado, necessitem da disponibilização destes.

Parágrafo único. Todos os conteúdos produzidos pelos colaboradores do CEJAM são de propriedade da Instituição, não sendo permitido o compartilhamento, cópia ou distribuição sem autorização da Instituição.

Art.4°. Os canais de comunicação com a TI institucional são através da:

I. Abertura de requisições por meio do sistema de registro de chamados;

II. Envio de *e-mail* para seg.infor@cejam.org.br em casos de dúvidas, violação deste regulamento, julgamentos de casos suspeitos ou informações sobre incidentes relacionados a Segurança da Informação.

Centro de Estudos e Pesquisas "Dr. João Amorim"
Rua Dr. Lund, 41 - Liberdade
São Paulo-SP - CEP: 01513-020
11 3469-1818
cejam@cejam.org.br
cejam.org.br

SEÇÃO I - PERMISSÕES E ORIENTAÇÕES GERAIS

Art.5°. Antes de iniciar as atividades no CEJAM, a pessoa (sendo colaborador, prestador de serviços ou voluntário) recebe o Termo de Confidencialidade (ANEXO I) para leitura e assinatura.

Parágrafo Único: O Departamento de Inovação e Tecnologia estabelece e orienta a adoção de práticas como:

I. Utilizar as ferramentas, recursos e sistemas de informação que são disponibilizados pela Instituição e considerados como meios oficiais pelo CEJAM e/ou por seus parceiros;

II. Armazenar os conteúdos produzidos, preferencialmente, no servidor de arquivos ou Drives disponibilizados pela Instituição a fim de que os riscos de perda do conteúdo sejam minimizados;

III. Utilizar dos recursos sem violação dos direitos de propriedade intelectual de qualquer pessoa (sendo paciente, colaborador, prestador de serviço, voluntário ou qualquer pessoa no âmbito externo à Instituição), como marcas e patentes, domínio na internet, ou qualquer material que não tenha autorização expressa do autor ou proprietário dos direitos;

IV. Criar, transmitir, disponibilizar, armazenar documentos e conteúdos, desde que respeite às leis e regulamentações vigentes, em específico àquelas cuja temática refere-se à crimes cibernéticos, ética, decência, honra, pornografia, vida privada, imagem de pessoas ou empresas;

V. As equipes de TI devem seguir o que é estabelecido no Manual de Governança de TI em Serviços de Saúde;

VI. Adotar as medidas cabíveis estabelecidas na Lei Federal nº. 13.709/2018 (LGPD) para o tratamento dos dados pessoais, de forma segura e eficaz;

VII. Resguardar a confidencialidade dos dados pessoais dos usuários e de terceiros, em conformidade com o estabelecido na "Política de Privacidade" do CEJAM.

SEÇÃO II - ATIVIDADES NÃO PERMITIDAS

Art.6°. O Departamento de Inovação e Tecnologia considera como atividade não permitida:

I. Revelar códigos de identificação, autorização e autenticação (conta, senhas, chaves privadas) ou permitir o uso por terceiros de recursos liberados por esses códigos, mesmo que o terceiro seja um colaborador CEJAM. Ressalta-se que esses códigos são

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

de uso pessoal e intransferível, sendo de responsabilidade do proprietário a atualização periódica e a preservação do seu sigilo;

II. Utilizar os recursos e sistemas de TI para divulgar ou comercializar produtos, itens ou serviços;

III. Utilizar os recursos e sistemas de TI para finalidades pessoais;

IV. Utilizar equipamentos, licenças, aplicações, *softwares* e/ou sistemas próprios/particulares para fins de desenvolvimento do escopo do trabalho;

V. Instalar e utilizar aplicativos e/ou sistemas não homologados pela Instituição;

VI. Violar as medidas de segurança determinadas pela instituição;

VII. Divulgar informações da Instituição, dos seus colaboradores ou fornecedores em grupos de discussão, *e-mails*, aplicativos de mensagens instantâneas, listas, bate-papo, entre outros;

VIII. O tratamento inadequado dos dados pessoais, por meio de procedimentos, sistemas aplicativos ou base de dados, que possam mantê-los desprotegidos, em desacordo com a Lei Federal nº. 13.709/2018 (LGPD);

IX. Não garantir que todas as medidas de anonimização sejam rigorosamente implementadas e respeitadas durante o tratamento de informações que estejam armazenadas e dispostas em documentos, planilhas, base de dados, sistemas, *dashboards* ou sistemas de apresentação;

X. Violar a confidencialidade dos dados pessoais de usuários, colaboradores e terceiros.

CAPÍTULO III - GESTÃO DE ATIVOS

Art.7°. Garantir que todos os ativos da instituição, sejam eles físicos, lógicos ou digitais, sejam identificados, catalogados, protegidos e gerenciados de forma adequada para mitigar riscos e assegurar a integridade, confidencialidade e disponibilidade das informações.

Art.8°. Todos os ativos de informação devem ser identificados e catalogados em um sistema centralizado. Cada ativo deve ser classificado de acordo com a sua importância e o impacto potencial em caso de perda, comprometimento ou indisponibilidade.

Art.9°. É dever de cada Gestor Regional ter o levantamento e controle dos ativos sob sua responsabilidade, preparar um plano para assegurar a proteção desses ativos, incluindo equipamentos, instalações e pessoas, contra ameaças físicas que possam comprometer a segurança da informação, a continuidade dos negócios, obsolescência e integridade das operações da instituição.

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

Art.10°. Os ativos devem ser gerenciados ao longo de todo o seu ciclo de vida, desde a aquisição até o descarte seguro. Isso inclui:

I. Aquisição: Garantir que novos ativos sejam adquiridos conforme os procedimentos de segurança estabelecidos;

II. Gestão e Rastreamento: Manter um registro atualizado e preciso de todos os ativos;

III. Manutenção: Realizar a manutenção periódica para garantir que os ativos permaneçam em bom estado e seguros;

IV. Desativação: Realizar a desativação de acesso ao ativo, para que não seja possível alteração das informações;

V. Descarte Seguro: Garantir que os ativos sejam descartados de forma segura, minimizando o risco de perda ou exposição de dados sensíveis.

SEÇÃO I - ESTAÇÕES DE TRABALHO

Art.11°. Os recursos de tecnologia e comunicação disponibilizados aos colaboradores são parte integrante para o desenvolvimento das atividades do CEJAM e é dever e responsabilidade de todos zelar pela segurança e integridade das informações e do patrimônio da Instituição, bem como desempenhar suas atividades de acordo com as normas estabelecidas.

Art.12°. As estações de trabalho devem utilizar solução de antivírus corporativo.

Art.13°. Não é permitido a utilização de equipamentos pessoais para realização das atividades sob qualquer pretexto.

Art.14°. Ao ser constatada a necessidade de instalação de um novo *software*, troca ou manutenção de equipamentos, o colaborador deve solicitar através do sistema de chamados direcionado à equipe de TI, conforme instruções do sistema de chamados internos.

§1º. Todas as manutenções em equipamentos deverão ser realizadas pela área de TI, não sendo permitido a outros colaboradores realizarem qualquer manutenção nestas.

§2º. Todas as movimentações de locais das estações devem ser realizadas pela equipe de TI, através da abertura de chamado, ou por colaboradores autorizados dentro da unidade de saúde.

§3º. Por motivo de segurança e padronização, quando possível os modelos de computadores com Gabinete, deverão ser instalados sobre a mesa.

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

Art.15°. O CEJAM reserva-se o direito de auditar, a qualquer momento e sem aviso prévio, o conteúdo dos computadores corporativos que seus colaboradores utilizam.

Art.16°. É dever do colaborador:

I. Instalar as atualizações automáticas sempre que o sistema operacional indicar a necessidade de aplicar as mesmas e aguardar até a finalização do processo para desligar o equipamento;
II. Realizar o bloqueio da estação de trabalho sempre que for se ausentar de sua mesa, em casos onde existe computadores de uso coletivo, sempre que se ausentar do computador o colaborador deve desconectar todos os *logins* realizados, para que não seja possível utilização indevida dos seus acessos;
III. Realizar o desligamento correto da sua estação, ao final do seu expediente ou por motivo de se ausentar desta por um longo período, evitando o uso dos recursos além do necessário;
IV. Não efetuar qualquer alteração na configuração de *hardware* (instalação ou remoção de peças internas e externas dos equipamentos);
V. Não executar *softwares* que não foram disponibilizados pela TI (ou que não fazem parte do seu escopo de trabalho).

Art.17°. É vedado ao colaborador:

I. Disponibilizar a sua estação de trabalho logada com seu usuário e senha para terceiros, mesmo que sejam colaboradores;
II. Acessar, visualizar, armazenar ou transmitir conteúdo obsceno ou pornográfico nos equipamentos da Instituição;
III. Instalar qualquer *software* na estação de trabalho sem prévia autorização;
IV. Deixar documentos salvos apenas na estação de trabalho;
V. Realizar o *download* ou armazenar na sua estação filmes, vídeos, músicas, *softwares*, livros em pdf ou outros arquivos que possua direitos autorais;
VI. Executar programas que habilitem conexão remota na sua estação como *Anydesk*, *Team Viewer* ou similar, conforme apresentado no **CAPÍTULO XII** deste documento;
VII. Trocar periféricos (teclado, *mouse* e monitor) por conta própria sem a devida autorização;
VIII. Desconectar os cabos de energia ou de rede da sua estação;
IX. Fraudar ou desativar as configurações de segurança implementadas na sua estação de trabalho;

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

X. Introduzir qualquer forma de vírus de computador na sua estação de trabalho;

XI. Desativar itens de segurança da estação como o *firewall* ou antivírus;

XII. Apagar arquivos do sistema operacional e de aplicativos instalados;

XIII. Retirar a estação de trabalho ou qualquer um dos seus periféricos da Instituição sem autorização da área de TI;

XIV. Ter acesso com permissão de Administrador da sua estação de trabalho;

XV. Utilizar a estação de trabalho disponibilizada pela Instituição para fins pessoais.

SEÇÃO II - TELEFONES FIXOS CORPORATIVOS

Art.18°. Os ramais são de uso coletivo e devem ser utilizados pelos colaboradores da Instituição de forma a auxiliá-los na execução dos seus trabalhos.

Art.19°. Caso seja necessário a manutenção do aparelho, o usuário deve solicitar a manutenção através do sistema de chamado.

Art.20°. O CEJAM reserva-se o direito de auditar, a qualquer momento e sem aviso prévio, o conteúdo das ligações realizadas nos telefones fixos corporativos.

Art.21°. Os equipamentos corporativos podem ser configurados com o software de telefonia virtual homologado, esta instalação deve ser realizada pela equipe de TI, assegurando que todas as normas de segurança e compatibilidade sejam seguidas.

Art.22°. É dever do usuário:

I. Zelar pelo bom funcionamento do aparelho;

II. Assegurar com que o softphone sempre esteja operacional evitando interrupções no funcionamento;

III. Fazer uso das orientações de uso do softphone fornecidas pela equipe de TI.

Art.23°. É vedado ao usuário:

I. Mudar o telefone de local;

II. Alterar as configurações do aparelho;

III. Desconectar os cabos de rede ou energia;

IV. Realizar qualquer tipo de manutenção no seu equipamento;

V. Repassar informações de pacientes, colaboradores, fornecedores e outros através de ligação telefônica para qualquer pessoa sem prévia autorização.

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

SEÇÃO III - DISPOSITIVOS MÓVEIS CORPORATIVOS

Art.24°. O CEJAM disponibiliza números ou dispositivos móveis corporativos para uso por colaboradores, em cargos específicos, ou por setores/equipes, cujas atividades justifiquem a utilização desse recurso.

Parágrafo único. Celulares corporativos que são utilizados dentro dos setores devem ser guardados pelos responsáveis em local seguro. Se o dispositivo tem de ser utilizado somente dentro da Instituição, o mesmo não pode ser retirado, sob qualquer pretexto.

Art.25°. O CEJAM reserva-se o direito de auditar, a qualquer momento e sem aviso prévio, o conteúdo dos celulares corporativos.

Art.26°. Qualquer suporte necessário deste equipamento deve ser solicitado à equipe de TI, através do sistema de chamado.

Art.27°. É dever do usuário:

I. Conservar o equipamento;
II. Utilizar o dispositivo disponibilizado pela Instituição;
III. Passar sempre seu número de telefone corporativo para tratar de assuntos pertinentes ao trabalho;
IV. Abrir boletim de ocorrência e informar a perda/roubo do celular corporativo ao gestor imediato e a área de TI da Instituição, para que sejam redefinidas as senhas de acesso aos sistemas corporativos e desvinculação do aparelho a rede da Instituição;
V. Devolver o aparelho com todas suas configurações e informações de forma intacta, quando solicitado;
VI. Manter o dispositivo atualizado instalando atualizações/ *patches* de aplicativos quando eles estiverem disponíveis;
VII. Assinar o termo de responsabilidade de uso, conforme **ANEXO II**.

Art.28°. É vedado ao usuário:

I. Utilizar o dispositivo para atividades particulares;
II. Armazenar dados, informações, documentos e arquivos pessoais no aparelho;
III. Configurar *e-mail* pessoal no aparelho corporativo.
IV. Instalar aplicativos que não sejam utilizados para suas atividades corporativas.
V. O tratamento de dados de pacientes ou não em dispositivos móveis pessoais.

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

SEÇÃO IV - IMPRESSORAS CORPORATIVAS

Art.29°. As impressoras são de uso coletivo e devem ser utilizadas pelos colaboradores e terceiros da Instituição de forma a auxiliá-los na execução das suas atividades diárias.

Art.30°. Toda a manutenção nos equipamentos de impressão deve ser realizada pela equipe de TI ou da empresa contratada, sendo estritamente proibido que outros a realizem.

Art.31°. É dever do colaborador:

I. Manter e zelar pelos equipamentos de impressão da Instituição;

II. Retirar a impressão imediatamente após o envio da mesma, evitando que o documento fique na impressora além do necessário.

Art.32°. É vedado ao usuário:

I. Mudar a impressora do seu local;
II. Alterar as configurações de rede;
III. Desconectar os cabos de rede ou energia;
IV. Tirar cópias ou realizar impressões particulares;
V. Realizar e deixar as impressões junto da impressora.

SEÇÃO V - DA UTILIZAÇÃO DE COMPARTILHAMENTO E ARMAZENAMENTO DE ARQUIVOS (SERVIDOR)

Art.33°. Servidor de arquivos é uma área de armazenamento que possibilita o compartilhamento de pastas e arquivos com o devido controle de acesso e segurança entre os colaboradores da Instituição.

Art.34°. Essas pastas devem possuir níveis de segurança implementados e, caso necessite de acesso a alguma pasta além da pasta da sua área/setor/departamento, deve solicitar via sistema de chamados, com a devida autorização do responsável da área.

Art.35°. As equipes de TI devem utilizar as recomendações estabelecidas no **Art. 5º, inciso V** deste regimento e orientações contidas no Manual de Governança de TI em Serviços de Saúde.

Art.36°. O CEJAM reserva-se o direito de auditar, a qualquer momento e sem aviso prévio, os conteúdos salvos no servidor de arquivos.

Art.37°. É dever do usuário:

I. Organizar os documentos nos diretórios;
II. Excluir arquivos que não estão sendo mais utilizados, evitando o acúmulo de arquivos desnecessários no servidor;
III. Evitar duplicar arquivos dentro do compartilhamento do servidor.

Art.38°. É vedado ao usuário:

I. Deletar arquivos do servidor com a intenção de prejudicar um colaborador ou a Instituição;
II. Salvar arquivos pessoais no servidor;
III. Utilizar de *softwares* para armazenamento e compartilhamento de arquivos na nuvem não são permitidos, exceto o Google Drive, vinculado a um *e-mail* corporativo da Instituição;
IV. Armazenar no servidor quaisquer materiais com direitos reservados, de propriedade intelectual ou com *copyright* (vídeos, músicas, *softwares*, jogos, livros digitais entre outros);
V. Armazenar no servidor qualquer material relacionado a *hacking/cracking*, incluindo links para sites com conteúdo desse tipo;
VI. Criar compartilhamento de pastas ou arquivos na sua estação de trabalho;
VII. Armazenar ou compartilhar os arquivos da Instituição em contas pessoais de sistemas em nuvem;
VIII. Sabotar ou tentar sabotar de alguma forma o servidor da Instituição.

SEÇÃO VI - DESCARTE DE EQUIPAMENTOS

Art.39°. Todo descarte ou baixa patrimonial de equipamentos de informática é realizado pela equipe de TI alinhado ao time de Gestão Ambiental respeitando as diretrizes ambientais. Cada contrato deve seguir o Plano de Gerenciamento de Resíduos de Serviço de Saúde (PGRSS) para realização do descarte correto de equipamentos inutilizáveis, obsoletos e inservíveis.

Parágrafo único. É proibido que colaboradores descartem qualquer equipamento de tecnologia sem que esse tenha passado por todo o processo de baixa.

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

CAPÍTULO IV - GERENCIAMENTO DE IDENTIDADE E ACESSO

Art.40°. Os *logins* de acesso são de uso exclusivo e pessoal de cada colaborador que atua no CEJAM, sendo proibido emprestar ou compartilhar com outro colaborador ou a terceiros.

Art.41°. Não é permitido que o colaborador use seu acesso aos meios e sistemas de TI para obtenção de informações para proveito próprio ou de terceiros.

Art.42°. Seguir o que está estabelecido na Política de Gerenciamento de Usuários, para procedimentos de criação, modificação, exclusão e gerenciamento de usuários da rede e dos sistemas internos da Instituição.

SEÇÃO I - CRIAÇÃO DE USUÁRIOS

Art.43°. A solicitação de criação de usuário para um colaborador deve ser feita através de chamados individuais para cada acesso que o colaborador necessita, seguindo as orientações indicadas no sistema de chamados.

§1º. Ao colaborador, cuja solicitação foi gerada, é disponibilizado um usuário (*login* e senha) que o identifique e forneça acesso aos sistemas de informática da Instituição de forma individual.

§2º. Não é recomendável a criação de usuários com nomes genéricos.

§3º. Não é permitido que o colaborador tenha perfis/acessos que não condizem com suas atribuições.

SEÇÃO II - SENHAS

Art.44°. As recomendações para a utilização das senhas são:

I. Não anotar as senhas em papel, agendas, blocos de anotações ou outros lugares;
II. Evitar utilizar a mesmas senhas pessoais no ambiente de trabalho;
III. Evitar realizar acessos com sua senha da Instituição, em computadores e redes de internet que ofereçam pouca ou nenhuma segurança, tais como "*Lan House*" ou locais com "*wi-fi* abertos / públicos / gratuitos";
IV. Atualizar sua senhas de acesso aos sistemas periodicamente, recomenda-se a cada 3 (três) meses;

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

V. Utilizar senhas que contenham, no mínimo 8 (oito) caracteres, compostos por letra, números e símbolos, evitando uso de nomes, sobrenomes, datas, números de documentos e outros que facilitem a identificação da senha;

VI. Utilizar senhas diferentes para outros acessos (*e-mail*, rede, sistemas internos), isso dificulta a ação de uma pessoa mal intencionada, no caso de ter uma credencial roubada;

VII. Nunca utilize a opção de "salvar suas credenciais" em navegadores de internet, prefira sempre ter que digitá-las.

SEÇÃO III - BLOQUEIO DE USUÁRIOS

Art.45°. Em caso de desligamento, transferência, afastamento ou licenças de colaboradores, o gestor imediato deve solicitar imediatamente o bloqueio dos acessos do mesmo, via sistema de chamados.

§1º. A equipe responsável deve priorizar o atendimento de desligamento de colaboradores, de modo a assegurar que todos os acessos foram bloqueados.

§2º. Os acessos do colaborador desligado permanecem bloqueados por 90 dias para casos de necessidade de recuperação de documentos ou informações salvas em algum sistema.

§3º. O bloqueio de usuários também pode ocorrer de forma automática pelo sistema (no caso de várias tentativas de *login* com a senha errada) ou de forma manual, e caso ocorra o bloqueio o colaborador deve solicitar desbloqueio para a equipe responsável através do sistema de chamados.

SEÇÃO IV - EXCLUSÃO DE USUÁRIOS

Art.46°. A exclusão de usuários é responsabilidade das equipes encarregadas pela liberação do acesso.

Art.47°. A exclusão de usuários deve ser analisada individualmente, levando em consideração o impacto dessa atividade, sempre esta ação deve ser registrada através do sistema de chamados, para garantir uma execução eficaz, é necessário criar fluxos e processos bem definidos e alinhados com as áreas envolvidas.

SEÇÃO V - ALTERAÇÃO DE ACESSO

Art.48°. É permitida a alteração de perfil de acesso, de forma temporária ou permanente, de acordo com a necessidade da instituição.

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

Parágrafo único. A solicitação de alteração de acesso deve ser feita pelo gestor imediato do colaborador, via sistema de abertura de chamados. O mesmo deve descrever o motivo da solicitação e, em caso de alteração temporária, deverá ser informado o período em que a mesma será válida.

CAPÍTULO V - DO ACESSO A INTERNET

Art.49°. É vedado ao usuário:

I. Acessar sites de jogos online, apostas, jogos de azar, filmes, pornográficos, séries e outros;
II. Usar a internet para enviar material ofensivo, difamatório ou de assédio para outras pessoas ou entidades;
III. Fazer qualquer tipo de ação que se caracterize como uma atitude *hacker*, atacar, pesquisar ou tentar obter informações em áreas não autorizadas;
IV. Realizar atividades pessoais sem relação com as tarefas de sua responsabilidade na Instituição;
V. Realizar propositalmente, *download* de vírus ou *software* que comprometa a segurança ou desempenho da internet, da rede corporativa ou equipamentos da Instituição;
VI. Qualquer tentativa de fraudar restrições de uso da internet implementadas pela Instituição;
VII. Enviar ou disponibilizar qualquer *software* da Instituição, sem prévia autorização.

CAPÍTULO VI - CANAIS DE COMUNICAÇÃO VIRTUAL

Art.50°. No cenário corporativo atual, as comunicações virtuais desempenham um papel central na condução das atividades diárias, facilitando a troca de informações e a colaboração entre equipes, independentemente de sua localização geográfica. No entanto, o uso dessas ferramentas requer uma abordagem cuidadosa para garantir a segurança das informações e a conformidade com as políticas internas e regulamentações aplicáveis.

Art.51°. Entende-se como canais homologados de comunicação virtual da Instituição:

I. E-mail Corporativo: E-mail do domínio cejam.org.br fornecido pela instituição;

II. Plataforma de Mensagem Instantânea: Google Chat vinculado ao e-mail Institucional e Whatsapp vinculado a um celular/número corporativo.

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

III. Vídeo Chamadas e Conferências Virtuais: Google Meet do e-mail Institucional;

Art.52°. Não é recomendado a utilização de qualquer canal de comunicação virtual que não esteja listado acima para tratamento de dados dentro da Instituição.

SEÇÃO I - DA UTILIZAÇÃO DO E-MAIL CORPORATIVO

Art.53°. Todas as ações de criação, bloqueio e exclusão de *e-mails* ou grupos devem ser solicitadas através do sistema de chamados.

Art.54°. O CEJAM reserva-se o direito de auditar, a qualquer momento e sem aviso prévio, o conteúdo dos *e-mails* corporativos.

Art.55°. É dever do usuário:

I. Utilizar o *e-mail* corporativo para quaisquer assuntos relativos à Instituição;
II. Utilizar o *e-mail* corporativo e o sistema de mensagens instantâneas com bom senso e de acordo com o Código de Ética e Conduta do CEJAM;
III. Atentar-se ao abrir anexos de *e-mails*. Em caso de dúvidas, acionar a área de Segurança da informação para verificar o *e-mail*, conforme **Art.4º**;
IV. Manter sua senha segura, e seguir as recomendações de segurança do **CAPÍTULO IV**, **Seção II**;
V. Solicitar através do sistema de chamados a alteração de qualquer informação na assinatura do *e-mail* Institucional;
VI. Acompanhar diariamente os *e-mails* em sua caixa postal.

Art.56°. É vedado ao usuário:

I. Utilizar o *e-mail* corporativo para tratar de assuntos pessoais;
II. Utilizar sua conta de *e-mail* particular para interagir com outros colaboradores, clientes ou fornecedores da Instituição;
III. Abrir arquivos, links e executar programas anexados ao *e-mail*, sem antes verificar sua procedência;
IV. Vincular sua conta de *e-mail* Corporativo para efetuar *login* em sites ou sistemas que não sejam os disponibilizados pela Instituição;
V. Criar uma conta de *e-mail* em outra plataforma para utilização dentro da Instituição;
VI. Forjar qualquer das informações do cabeçalho do remetente;
VII. Modificar manualmente qualquer informação da assinatura do *e-mail* Institucional;

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

VIII. Cadastrar o *e-mail* corporativo em listas que não fazem parte da rotina de trabalho como sites de compras, lojas online entre outros;

IX. Disponibilizar listas de *e-mails* da Instituição para outras empresas ou pessoas sem prévia autorização;

X. Disponibilizar seu *login* e senha para outras pessoa, sob qualquer pretexto;

XI. Acessar a caixa postal de outro usuário sem autorização;

XII. O envio de:

A. Propagandas ou mensagens em cadeia, do tipo de pirâmides ou corrente para serem transmitidas para os clientes, fornecedores ou outros colaboradores;

B. Material relacionado à nacionalidade, raça, orientação sexual, religiosa, convicção política ou qualquer outro assunto que possa vir a difamar outra pessoa como cidadão, fornecedor ou empresa;

C. Material que não tenha relação com o serviço do destinatário, seja por mensagem instantânea ou correio eletrônico;

D. Informações ou documentos sobre a Instituição que prejudique sua imagem ou de seus clientes e fornecedores;

E. Informações com intuito de difamar, caluniar, injuriar, assediar qualquer pessoa ou Instituição.

SEÇÃO II - PLATAFORMA DE MENSAGENS INSTANTÂNEAS

Art.57°. As plataformas de mensagens instantâneas desempenham um papel crucial na comunicação rápida e eficiente entre equipes dentro da instituição. No entanto, para garantir a segurança das informações corporativas e a conformidade com as boas práticas, é fundamental que o uso destas sejam monitorados e acompanhados.

Art.58°. É dever do colaborador:

I. Utilizar a plataforma homologada pela instituição;

II. Garantir que todas as comunicações realizadas na plataforma homologada seja feita de forma cautelosa para proteger a informação;

III. Não compartilhar dados sensíveis ou críticos em chats ou grupos sem a devida segurança e autorização;

IV. Informar imediatamente à equipe de TI ou ao departamento responsável sobre qualquer problema ou incidente relacionado à plataforma.

Art.59°. É vedado ao colaborador:

I. O uso de plataformas de mensagens instantâneas em dispositivos e/ou números não corporativos, para qualquer tipo de comunicação relacionada à Instituição;

II. A criação de grupos em plataformas de mensagens instantâneas em dispositivos e/ou números não corporativos, para compartilhamento de dados Institucionais ou tratamento de dados pessoais.

SEÇÃO III - VÍDEO CHAMADAS E CONFERÊNCIAS VIRTUAIS

Art.60°. As vídeo chamadas e conferências virtuais são essenciais para a comunicação eficaz e a colaboração entre equipes e com clientes. Elas permitem interações em tempo real, facilitando reuniões, apresentações e treinamentos, independentemente da localização dos participantes.

Art.61°. É permitido participar de reuniões em outras plataformas apenas como convidados, sem criar ou gerenciar salas.

Art.62°. É dever do colaborador:

I. Usar Google Meet para todas as vídeo chamadas e conferências virtuais relacionadas ao trabalho.

II. Os colaboradores devem garantir que, mesmo ao usar plataformas não homologadas, as informações corporativas sejam tratadas com cuidado e sigilo.

Art.63°. É vedado ao colaborador:

I. Criação de salas em plataformas não homologadas.

II. Uso de plataformas não autorizadas para reuniões corporativas.

III. Compartilhamento de Informações Sensíveis sem a devida autorização ou anonimização.

Centro de Estudos e Pesquisas "Dr. João Amorim"
Rua Dr. Lund, 41 - Liberdade
São Paulo-SP - CEP: 01513-020
11 3469-1818
cejam@cejam.org.br
cejam.org.br

CAPÍTULO VII - DO ACESSO À REDE CORPORATIVA (CABEADA/WIRELESS)

SEÇÃO I - REDE CORPORATIVA CABEADA

Art.64°. A rede corporativa de dados é utilizada por todos os colaboradores, estagiários e terceirizados autorizados pela área competente. Os pontos de rede estão mapeados conforme as estações de trabalho disponíveis.

Parágrafo único. Para inclusão de novos pontos de rede, é necessário abertura de chamados para avaliação da possibilidade de aumento da infraestrutura junto às áreas de engenharia e tecnologia.

Art.65°. Qualquer manutenção na estrutura da rede, somente é realizada pela equipe de TI ou por empresa contratada.

Art.66°. É dever do usuário:

I. Zelar pelo bom funcionamento da estrutura da rede cabeada da Instituição;
II. Informar a TI se observar alguma ação atente contra o bom funcionamento desta infraestrutura.

Art.67°. É vedado ao usuário:

I. Conectar um novo equipamento (computadores, notebooks, *switches*, roteadores ou outros) na estrutura da rede da Instituição, ficando restrito apenas a equipe de TI a inclusão de novos equipamentos;
II. Instalar ou executar no seu computador sistemas que fazem escaneamento no tráfego de pacotes da rede;
III. Instalar ou executar *softwares* que fazem a descoberta de ativos de rede;
IV. Utilizar computadores ou notebooks pessoais na rede da Instituição;
V. Alterar as configurações de rede dos computadores/notebooks ou outros dispositivos;
VI. Desligar ou danificar intencionalmente qualquer equipamento ou cabeamento da rede;
VII. Fraudar ou sabotar de qualquer forma a rede de dados corporativos.

SEÇÃO II - REDE CORPORATIVA WIRELESS

Art.68°. A Rede Corporativa *Wireless* pode ser disponibilizada pela Instituição para uso nas atividades dos colaboradores e prestadores de serviço devidamente autorizados, quando da sua atribuição houver a necessidade explícita de utilização desta rede, e esse acesso deve ser sempre realizado através de um equipamento corporativo.

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

§1º. Para inclusão de qualquer equipamento na rede *wireless,* deve ser aberto um chamado para a área de TI.

§2º. A configuração de um novo dispositivo deve ser realizada pela equipe de TI. Estes, mesmo sendo equipamentos de prestadores de serviço, devem respeitar as diretrizes deste regulamento durante sua conexão com a rede *wireless*.

Art.69°. Quando houver necessidade de criação de redes para pacientes ou visitantes essas devem ser segmentadas da rede corporativa, não sendo possível que as mesmas se comuniquem.

Art.70°. Qualquer manutenção na estrutura da rede é realizada pela equipe de TI, restritamente, não sendo permitido a outras áreas ou colaboradores realizá-la.

Art.71°. É dever do usuário informar a equipe da TI se observar alguma ação que atente contra o bom funcionamento desta infraestrutura.

Art.72°. É vedado ao usuário:

I. Conectar dispositivos não autorizados na rede *wireless*;
II. Utilização de *softwares* que tentem quebrar a senha da rede *wireless*;
III. Desligar ou danificar intencionalmente qualquer equipamento da rede;
IV. Instalar roteadores *wireless* ou amplificadores de sinais;
V. Promover ou facilitar ataques à rede de dados corporativos.

SEÇÃO II - ACESSO REMOTO À REDE CORPORATIVA

Art.73°. O CEJAM libera o acesso remoto aos seus colaboradores sob as seguintes condições:

I. O acesso remoto à rede corporativa da Instituição deve ser solicitado sempre através do sistemas de chamados;
II. Cabe ao gestor imediato solicitar ou revogar o acesso remoto dos colaboradores sob sua gestão;
III. O acesso quando autorizado não será vitalício, tendo de ser revalidado a cada 3 (três) meses desta forma seguindo por até 1 (um) ano, posterior a isso será necessário refazer o processo de solicitação;
IV. Deve ser implementado controles de liberação de horário para esses acessos, não sendo possível conexões fora do horário de trabalho, havendo necessidade de liberação fora desse horário o mesmo deve ser solicitado pelo gestor imediato através de abertura de chamado;

V. Não é permitido o acesso remoto à rede corporativa através de equipamentos pessoais.

Art.74°. É dever do usuário:

I. Responder por qualquer operação realizada sob suas credenciais de acesso;
II. Comunicar imediatamente a área de TI qualquer situação que coloque em risco o acesso ao ambiente da rede de dados;
III. Informar seu gestor quando forem identificados direitos de acesso remoto desnecessários à execução de suas atividades;
IV. Quando não tiver mais necessidade do acesso solicitar cancelamento deste;
V. Não conectar na VPN corporativa através de redes de *Wi-fi* públicas.

Art.75°. É vedado ao usuário:

I. Ceder seu acesso a outras pessoas;
II. Tentar ou criar mecanismos para acesso remoto à rede corporativa;
III. Executar ou instalar programas que habilitem conexão remota na sua estação como *Anydesk*, *Team Viewer* ou similares, sem autorização do Departamento de Inovação e Tecnologia;
IV. Fraudar as medidas de segurança da rede corporativa quando necessário acesso externo.

CAPÍTULO VIII - DA GESTÃO DE SISTEMAS, *SOFTWARES* E LICENÇAS

Art.76°. A segurança da informação deve ser incorporada em todas as etapas do desenvolvimento de sistemas internos e customizados, desde a concepção até a implantação e manutenção, com o objetivo de prevenir vulnerabilidades que possam comprometer a segurança e a continuidade das operações da instituição.

Art.77°. Todas as alterações ou atualizações em sistemas existentes, incluindo novas funcionalidades, correções de bugs ou mudanças na configuração, devem seguir um processo formal de gestão de mudanças, seguindo o capítulo XIX.

Art.78°. Todo software ou sistema web utilizado no âmbito corporativo deverá ser acessado exclusivamente através de contas de e-mail corporativas fornecidas pela instituição. É expressamente proibido o uso de contas de e-mail pessoais para acessar qualquer sistema ou serviço relacionado ao trabalho.

Art.79°. As manutenções e atualizações em sistemas devem ser planejadas e executadas de forma a minimizar o impacto nas operações e garantir a continuidade do negócio, preferencialmente em horários de menor demanda ou durante janelas de manutenção pré-definidas.

Art.80°. Todo software e/ou licença a ser adquirido ou utilizado pela instituição deve ser solicitado através do sistema interno de chamados, com o acompanhamento do departamento de TI, para que se tenha um controle e verifique os parâmetros adequados para utilização.

Art.81°. O departamento de TI é responsável pela instalação e gestão de *softwares* e de licenças de uso, adquiridas pela Instituição.

Art.82°. É dever do usuário utilizar o sistema de chamados para solicitar a renovação da licença de uso.

Art.83°. Não é permitido ao usuário utilizar licença pessoal para validação ou ativação de qualquer *software* comprado ou não pela Instituição.

Art.84°. Não é permitido a utilização de *softwares* mesmo que não necessite de ativação ou licenciamento inicial, sem prévia autorização do Departamento de Inovação e Tecnologia, devido a limitações de termos de uso para utilização em ambientes corporativos.

SEÇÃO I - DA UTILIZAÇÃO DE SISTEMAS CORPORATIVOS

Art.85°. O CEJAM disponibiliza alguns sistemas de maneira global, ou seja, destinado a todos os colaboradores, ou de maneira restrita, destinado à pessoas ou áreas específicas. Caso haja necessidade de o colaborador ter acesso a algum sistema, o gestor imediato do mesmo deve gerar um chamado com a solicitação, seguindo as instruções do sistema de chamados.

Parágrafo único. Caso o colaborador observe alguma ação contra o bom funcionamento do sistema, a orientação é que informe ao seu gestor imediato.

Art.86°. É de responsabilidade do colaborador manter a sua senha segura, e seguir as recomendações de segurança de senhas, denotadas no **CAPÍTULO IV**, **Seção II**.

Art.87°. O CEJAM reserva-se o direito de auditar, a qualquer momento e sem aviso prévio, o acesso aos sistemas corporativos.

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

Art.88°. É dever do usuário:

I. Não utilizar outro acesso que não seja o seu usuário;
II. Sempre que não estiver utilizando o sistema, desconectar o seu acesso;
III. Informar seu gestor imediato caso observe que tenha acesso a informações que não sejam pertinentes ao seu perfil;
IV. Tratar informações pessoais de forma segura, e informar possíveis vazamentos ou informações que agem contra a segurança do Sistema;
V. Não utilizar seu acesso para disponibilizar informações a terceiros sem prévia autorização.

Art.89°. É vedado ao usuário:

I. Fornecer para qualquer pessoa informações confidenciais ou restritas sobre fornecedores, pacientes, familiares, colaboradores ou voluntários;
II. Violar medidas de segurança ou de autenticação dos sistemas;
III. Utilizar do seu acesso ao sistema para executar atividades visando o benefício próprio ou de terceiros;
IV. Disponibilizar informações coletadas nos sistemas sem a devida autorização da Instituição;
V. Disponibilizar seu usuário e senha para que outro utilize;
VI. Obter acesso não autorizado, ou acessar indevidamente dados e sistemas, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades em sistemas;
VII. Monitorar ou interceptar o tráfego de dados nos sistemas.

SEÇÃO II - DA UTILIZAÇÃO PRONTUÁRIO ELETRÔNICO

Art.90°. Os prontuários eletrônicos disponíveis nas unidades CEJAM são ferramentas que visão facilidades no processo de atendimento e apoio na parte administrativa que, além dos cuidados e deveres já citados na **SEÇÃO I - DA UTILIZAÇÃO DE SISTEMAS**, acrescentamos o que é ser de responsabilidade e comprometimento do colaborador:

I. Utilizar os dados do sistema de prontuário eletrônico de acesso restrito e manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;
II. Não se ausentar da estação de trabalho sem encerrar a sessão de uso do sistema, garantindo assim a impossibilidade de acesso indevido por terceiros;

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

III. Restringir a utilização do prontuário eletrônico, apenas no local e horário de trabalho e para fins de assistência ao paciente, salvo o médico que está tratando do paciente;
a. Quando do acesso remoto, Telemedicina, entre outras, ao prontuário eletrônico é solicitado que os colaboradores tenham os mesmo cuidados exigidos no ambiente remoto e que o equipamento utilize de VPN para a rede da unidade;

IV. Cuidar da integridade, confidencialidade e disponibilidade dos dados, informações contidas no prontuário eletrônico, devendo comunicar o Setor de Segurança da Informação através do e-mail (seg.infor@cejam.org.br) e minha chefia imediata quaisquer indícios ou possibilidades de irregularidades, de desvios ou falhas identificadas no sistema, sendo proibida a exploração de falhas ou vulnerabilidades porventura existentes;

V. Não revelar a senha de acesso ao sistema a ninguém e tomar o máximo de cuidado para que ela permaneça somente seu conhecimento, tendo ciência que a senha é de cunho pessoal e intransferível;

VI. Responder, em todas as instâncias, pelas consequências das ações ou omissões que possam pôr em risco ou comprometer a exclusividade de conhecimento da senha, ou das transações a que se tem acesso.

VII. Ter o entendimento claro de que constitui descumprimento de normas legais, regulamentares e quebra de sigilo funcional divulgar dados obtidos do sistema, aos quais se tem acesso, para outros trabalhadores ou terceiros não envolvidos nos trabalhos executados;

VIII. Respeitar as normas de segurança e restrições do sistema impostas pelos métodos de segurança presentes em qualquer sistema (tais como privilégio e direitos de acesso);

IX. Ter ciência de que constitui falta de zelo e dedicação às atribuições do cargo e descumprimento de normas legais e regulamentares, não proceder com cuidado na guarda e utilização de senha ou emprestá-la a terceiros, ainda que habilitados;

X. Ter ciência de que constitui infração penal, funcional, bem como responsabilização por crime contra a Administração Pública, tipificado no art. 313-A e 313-B tratar dados ou facilitar o tratamento, tais como, a inserção de dados falsos, alteração ou exclusão indevida de dados do sistema ou bancos de dados, com o fim de obter vantagem indevida para si, ou para outrem, ou para causar dano; bem como modificar o sistema de informações ou programa de informática sem autorização, sendo esse um rol exemplificativo.

XI. Ciência de que todos estes itens estão em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018, LGPD), que visa proteger a privacidade e garantir a

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

segurança dos dados pessoais coletados, armazenados e tratados no âmbito de suas atividades.

SEÇÃO III - CERTIFICADO DIGITAL

Art.91°. O certificado digital é a identidade digital da pessoa física e jurídica no meio eletrônico, o colaborador que fizer uso deste tipo de tecnologia de forma direta deve seguir o que está descrito neste regulamento.

Art.92°. Existem dois tipos de certificado digital:

I. Certificado A1 que é armazenado no computador ou no dispositivo móvel;
II. Certificado A3 que é armazenado em mídia criptográfica (cartão, token ou nuvem).

Parágrafo único. Para instalação desses certificados é necessário abertura de chamado pelo sistema interno solicitando ao setor de TI o apoio para instalação em seu computador.

Art.93°. Quando o certificado da Instituição tiver seu vencimento, e o novo contrato for realizado é dever da área que realiza as tratativas, cadastrar a nova senha e disponibilizá-la junto ao certificado tipo A1 para o setor de TI realizar a instalação nos computadores indicados. Caso fique algum computador pendente após este processo, será necessário abertura de chamados individuais.

Art.94°. Cada contrato possui seu certificado utilizado nas tarefas dos setores internos como Recurso Humanos, as Regionais recebem seu certificado referente ao seu CNPJ e esses devem ser instalados pela TI local nas estações de trabalho indicadas, sempre registrando essa ação através de chamados.

Art.95°. Quando houver necessidade de instalação do certificado da Matriz em alguma unidade, o mesmo é solicitado pelo Departamento de Gestão de Pessoas da Sede Administrativa, sempre registrando a solicitação através de chamado para a TI.

Art.96°. É dever do usuário:

I. Armazenar o certificado e senha em local seguro sempre que usar o certificado digital individual.

Art.97°. É vedado ao usuário:

I. Instalar ou utilizar o certificado digital Institucional em equipamentos pessoais, sob qualquer pretexto;

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

II. Disponibilizar a senha do certificado digital para terceiros, mesmo que este seja colaborador;

III. utilizar o certificado digital instalado na sua estação de trabalho para outros fins que não sejam os estabelecidos.

CAPÍTULO IX - DA SEGURANÇA FÍSICA E DO AMBIENTE

Art.98°. Assegurar a proteção dos ativos, incluindo equipamentos, instalações e pessoas, contra ameaças físicas que possam comprometer a segurança da informação, a continuidade dos negócios e a integridade das operações da instituição.

Art.99°. O acesso às instalações deve ser restrito apenas a pessoas autorizadas, medidas de controle de acesso físico podem ser implementadas, como:

I. Cartões de Acesso: Utilização de crachás ou cartões de acesso personalizados para autorizar a entrada em áreas restritas;

II. Biometria: Implementação de sistemas biométricos (impressão digital, reconhecimento facial, etc.) em áreas de alta segurança;

III. Registro de Visitantes: Todos os visitantes devem ser registrados e acompanhados por um colaborador autorizado enquanto estiverem nas instalações;

IV. Monitoramento de Acesso: Manter logs de acesso e realizar revisões periódicas para detectar atividades suspeitas ou não autorizadas.

Art.100°. As áreas que abrigam ativos críticos, como *data centers*, salas de servidores, locais que armazenam dados sensíveis, devem ser protegidas com medidas de segurança adicionais.

Art.101°. Medidas de segurança visando a continuidade do negócio devem ser implementadas para proteger as instalações contra riscos ambientais, como incêndios, inundações, e falhas de energia.

SEÇÃO I - DO ACESSO ÀS CÂMERAS DE SEGURANÇA

Art.102°. A Instituição possui monitoramento por câmera nas áreas internas e externas, com intuito de zelar pelo seu patrimônio e garantir a segurança dos seus colaboradores e pacientes.

Art.103°. A Instituição se reserva o direito de auditar o conteúdo das câmeras sempre que achar necessário sem prévio aviso.

Art.104°. O acesso externo às câmeras de segurança é restrito aos gestores, com a devida validação do gestor do TI.

Art.105°. O acesso do conteúdo gravado pelas câmeras só é disponibilizado através da solicitação no sistema interno de chamados, com a autorização do gestor imediato e validação do gestor da área de TI.

Parágrafo único. A manutenção das câmeras, deve ser realizada pela equipe de TI ou empresa responsável, sendo estritamente proibido que colaboradores não autorizados realizem qualquer tipo de ação.

Art.106°. É vedado ao usuário:

I. Usar seu acesso às câmeras para proveito próprio;
II. Realizar gravações e divulgar estas sem as devidas autorizações;
III. Disponibilizar seu acesso de *login* e senha para terceiros;
IV. Movimentar ou remanejar as câmeras de lugar;
V. Vandalizar ou atentar contra o bom funcionamento dos equipamentos e/ou sua infraestrutura;
VI. Obstruir total ou parcialmente o campo de visão da câmera.

CAPÍTULO X - DAS MÍDIAS SOCIAIS

Art.107°. As contas corporativas de acesso para administração das mídias sociais oficiais da Instituição devem ser criadas e gerenciadas pelo Departamento de Comunicação, *Marketing* e Relacionamento Institucional. Já as senhas devem ser compartilhadas com o Departamento de Inovação e Tecnologia Institucional, exclusivamente, para o caso de necessidade de recuperação senha ou para realizar alguma auditoria.

Art.108°. Caso o colaborador identifique alguma reportagem ou postagem que denigra ou não faça parte dos canais oficiais da Instituição, o mesmo deve informar o conteúdo à área de comunicação (comunicacao@cejam.org.br).

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

CAPÍTULO XI - DA GESTÃO DE *BACKUP*

Art.109°. Estabelecer diretrizes e procedimentos para a realização de *backups* regulares e seguros dos dados da instituição, garantindo a disponibilidade e a integridade das informações em caso de falhas, desastres ou incidentes de segurança.

Art.110°. Cada Gestor Regional deve preparar o plano para atender as demandas específicas para continuidade do serviço que está sob sua gestão.

Art.111°. Este plano aplica-se a todos os sistemas, servidores, bases de dados, e dispositivos de armazenamento que contenham dados sensíveis da instituição.

Art.112°. A frequência dos *backups* deve ser estabelecida com base na criticidade dos dados e nos requisitos de recuperação.

Art.113°. Os *backups* devem ser agendados em horários que minimizem a interrupção das operações, preferencialmente fora de horários críticos.

Art.114°. Os *backups* devem ser armazenados de forma segura, tanto localmente quanto em sistema em nuvem, para garantir redundância e proteção contra desastres locais.

Art.115°. Os dados de *backup* devem ser protegidos contra acessos não autorizados e violações de segurança.

Art.116°. Necessário criação de procedimentos claros para a recuperação de dados que devem estar documentados e testados regularmente.

Art.117°. Os dados de *backup* devem ser retidos por períodos específicos, de acordo com as necessidades operacionais, regulamentações legais e políticas internas. Após o período de retenção, os *backups* devem ser descartados de forma segura.

CAPÍTULO XII - DA GESTÃO DE MUDANÇA

Art.118°. Uma mudança é qualquer implantação, atualização, modificação ou remoção de componentes de TI ou processos de negócio que possa afetar os serviços, segurança ou operação da instituição.

Art.119°. O Gestor Regional é responsável pelo planejamento, registro, acompanhamento e conclusão da mudança, envolvendo as partes interessadas, alinhado ao time de Segurança da Informação.

Art.120°. A mudança deve ser realizada preferencialmente fora de horários críticos.

Art.121°. Atualizações em sistemas devem ser testadas antes em ambientes de homologação, para então serem aplicadas em produção.

Art.122°. O processo de gestão de mudanças deve seguir um ciclo estruturado para garantir que todas as mudanças sejam avaliadas, aprovadas, implementadas e revisadas adequadamente e que contemple um plano para reverter as mudanças aplicadas.

CAPÍTULO XIII - DA GESTÃO DE INCIDENTES

Art.123°. Estabelecer diretrizes e procedimentos para a identificação, resposta, gestão e recuperação de incidentes de segurança da informação, visando minimizar os impactos sobre os ativos da instituição e assegurar a continuidade das operações.

Art.124°. Um incidente de segurança da informação é qualquer evento que comprometa ou tenha o potencial de comprometer a integridade, confidencialidade, ou disponibilidade das informações, sistemas ou ativos da instituição.

Art.125°. Todos os colaboradores ou terceiros devem notificar um incidente de segurança da informação de imediato para a equipe de segurança da informação através do *e-mail* seg.infor@cejam.org.br.

Art.126°. Após a identificação de um incidente, o comitê de resposta a incidentes deve ser acionado, esse é composto pelo Gestor de Inovação e Tecnologia, equipe de Segurança da Informação Institucional, Gestor Regional e a TI local.

Art.127°. Todos os incidentes devem ser documentados de forma detalhada para análise futura e para assegurar a conformidade com as políticas de segurança.

Art.128°. Realizar uma revisão detalhada para identificar lições aprendidas e ajustar políticas e procedimentos conforme necessário.

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

SEÇÃO I - PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS

Art.129°. Em alinhamento com as metodologias de Qualidade adotadas pela instituição, como as normas ISO 27001 e os padrões da Organização Nacional de Acreditação (ONA), implementamos um conjunto robusto de medidas preventivas e processos internos para garantir a segurança contra ameaças cibernéticas.

Art.130°. As principais medidas adotadas incluem:

I. Sistema de Gestão de Incidentes é uma plataforma centralizada que permite o registro, rastreamento e resolução de incidentes de segurança da informação de forma eficiente. Ele garante que todos os incidentes sejam documentados desde a detecção até a resolução, proporcionando uma visão clara do ciclo de vida dos incidentes.

II. O Monitoramento Contínuo envolve a supervisão ininterrupta de toda a infraestrutura de TI, utilizando ferramentas avançadas para identificar e responder a atividades suspeitas em tempo real. Essa vigilância constante sobre redes, servidores, aplicações e dispositivos, permitindo a detecção precoce de comportamentos anômalos ou tentativas de invasão.

III. Controle de Acessos é fundamental para informações sensíveis e sistemas críticos, seguindo a Política de Gerenciamento de Usuários que define quem tem permissão para acessar recursos específicos, baseado em seu papel dentro da instituição.

IV. Plano de Resposta a Incidentes é o documento estratégico que detalha as etapas a serem seguidas em caso de um incidente de segurança, como um ataque cibernético. Eles incluem protocolos para a identificação, contenção, erradicação e recuperação de incidentes, bem como comunicação com partes interessadas internas e externas. Seguidos pelo documento de Lições Aprendidas em Incidentes.

CAPÍTULO XIV - DO PLANO DE CONTINGÊNCIA

Art.131°. Definir diretrizes e responsabilidades para o desenvolvimento, implementação e manutenção de um Plano de Contingência, garantindo que a instituição possa continuar exercendo suas atividades em caso de incidentes, desastres ou interrupções significativas.

Art.132°. Cada Gestor Regional deve preparar o plano para atender as demandas específicas para continuidade do serviço que está sob sua gestão.

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

Art.133°. O plano deve ser um documento abrangente que inclua os seguintes componentes principais:

I. Análise de Impacto do Negócio: Identificação e avaliação dos impactos potenciais de diferentes tipos de interrupções nos processos de negócios e nos ativos críticos;

II. Avaliação de Riscos: Identificação e análise dos riscos que podem comprometer a continuidade dos negócios, como falhas de tecnologia, desastres naturais, ciberataques, e outras ameaças;

III. Estratégias de Continuidade: Desenvolvimento de estratégias específicas para mitigar riscos identificados e garantir a continuidade das operações, incluindo redundância, diversificação de fornecedores, e soluções de recuperação.

Art.134°. Este plano se aplica a todas as unidades de negócio, sistemas críticos, processos operacionais, e infraestrutura da instituição, abrangendo medidas para assegurar a continuidade e a recuperação de operações em situações de emergência.

Art.135°. A implementação do plano de contingência envolve a preparação de todos os recursos e a disseminação das responsabilidades.

Art.136°. O plano deve:

I. Ser um documento vivo, sujeito a revisões regulares e atualizações contínuas.

II. Incluir estratégias detalhadas para a recuperação de operações após a contenção de um incidente, garantindo a restauração completa das atividades normais.

III. Estar em conformidade com todas as regulamentações legais e normas aplicáveis à continuidade de negócios, incluindo requisitos específicos da indústria e normas de segurança da informação.

IV. Ser devidamente documentado e armazenado em locais acessíveis para todos os colaboradores chaves, garantindo que o plano esteja disponível em formato físico e digital durante emergências.

CAPÍTULO XV - DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Art.137°. O comitê de segurança da informação deve:

I. Ser constituído por um representante das áreas abaixo:

A. Gestão da Tecnologia;e
B. Gestão Jurídica.

II. Reunir-se, formalmente, uma vez a cada três meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum, incidente grave ou definição relevante;

III. Assegurar, disseminar e aprovar ações sobre a segurança da informação em toda Instituição;

IV. Utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico;

V. Propor investimentos relacionados à segurança da informação com objetivo de reduzir os riscos;

VI. Propor alterações nas versões deste documento.

Art.138°. O comitê possui autonomia para aprovar e sequenciar decisões relacionadas à segurança da informação, de forma a assegurar a agilidade nas operações necessárias para o andamento de projetos.

Parágrafo único. As reuniões do comitê serão registradas em atas ou pró-memórias.

CAPÍTULO XVI - DA DISCIPLINA NA PROTEÇÃO DE DADOS – LGPD

Art.139°. Para fins de melhor compreensão das disposições acerca da proteção de dados pessoais, considera-se:

I. Tratamento de Dados: Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

II. Titular: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

III. Banco de Dados: Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico. Frequentemente abreviado pelas letras "B.D";

IV. Controlador: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados. No caso do presente

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

Regulamento o CEJAM é o controlador dos dados que recebe e faz o tratamento necessário;

V. Operador: Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Como exemplo ilustrativo, o operador pode ser um funcionário que opera ou manipula os dados conforme a finalidade. Isso também pode ser feito por uma empresa terceirizada;

VI. Encarregado: Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

VII. Agentes de Tratamento: Controlador e Operador;

VIII. Anonimização: Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

IX. Consentimento: Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Art.140°. O tratamento de dados pessoais por colaboradores do CEJAM, fornecedores e demais interessados, é disciplinado através das políticas e manuais que compõe o Programa de Conformidade LGPD, acessíveis através do link: https://cejam.org.br/governanca aba "Programa de Conformidade LGPD", em conjunto com este regulamento.

Art.141°. Através de acesso aos bancos de dados do CEJAM ou qualquer outro meio, o tratamento de dados pessoais realizado por colaboradores deve ser baseado na Lei Geral de Proteção de Dados (LGPD), Constituição Federal e demais diplomas legais que normatizam o tema em Direito Digital.

Art.142°. Somente é autorizado o tratamento de dados pessoais pelos colaboradores para a execução da atividade profissional com finalidade de executar tarefas que atendam as demandas solicitadas exclusivamente pelo CEJAM, enquanto empregador, e devidamente supervisionada por sua gestão hierárquica departamental.

Art.143°. Nas atividades que demonstrem necessidade de tratamento de dados pessoais, o colaborador deve se pautar nas disposições contidas neste regulamento e nos instrumentos de governança em proteção de dados mencionados no **Art. 131º**.

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

SEÇÃO I - ORIENTAÇÃO PARA O TRATAMENTO DE DADOS PESSOAIS

Art.144°. No tratamento de dados pessoais, os colaboradores devem agir orientados pelos seguintes fundamentos:

I. Respeito à privacidade: O tratamento de dados pessoais deve ser sempre limitado à finalidade para a qual foram captados, sendo terminantemente proibido o seu uso para invasão à privacidade de seus titulares;

II. Autodeterminação informativa: É o poder que o titular tem sobre suas próprias informações, não podendo o colaborador alterar seus dados sem ter sido autorizado pelo próprio titular;

III. Liberdade de expressão, de informação, de comunicação e de opinião: São direitos constitucionais constantes também na LGPD. O tratamento dos dados não pode ser usado para fins de atrapalhar o exercício do titular sobre estes direitos;

IV. Inviolabilidade da intimidade, da honra e da imagem: Dados pessoais são informações privadas e não públicas, devendo o tratamento respectivo ser efetuado de forma a preservar essas informações de acessos não autorizados;

V. Desenvolvimento econômico, tecnológico e inovação: A atividade do CEJAM é de alta relevância social. Dentre diversas tarefas administrativas, o tratamento de dados pela entidade é um dos instrumentos utilizados para que sua finalidade seja alcançada, colaborando assim com estes fundamentos;

VI. Livre iniciativa, a livre concorrência e a defesa do consumidor: Na prestação de serviços da entidade, o tratamento de dados pessoais deve ser realizado com a observância legal adequada para auxiliar à sociedade em seu desenvolvimento regular;

VII. Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Art.145°. Na captação de dados pessoais, seja de outros colaboradores ou do público externo, a solicitação dos dados deve ser revestida das seguintes características:

I. Finalidade: Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível;

II. Adequação: Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

III. Necessidade: Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV. Livre acesso: Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V. Transparência: Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VI. Qualidade dos dados: Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VII. Segurança: Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII. Prevenção: Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX. Não discriminação: Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X. Responsabilização e prestação de contas: Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Art.146°. Havendo a necessidade de obter dados pessoais de titulares, tal situação deve ser revestida das seguintes características:

I. O colaborador deverá informar ao titular a finalidade para qual os seus dados pessoais estão sendo solicitados, de modo explícito e não resumido;

II. Além do disposto no item acima, o colaborador deverá obter o consentimento do titular de forma a demonstrar que foi esclarecido acerca da finalidade e que o titular autoriza o tratamento de seus dados;

III. Deve ser demonstrado ao titular a possibilidade de revogação de seu consentimento e esclarecido que há hipóteses em que o controlador está obrigado pela lei a manter os dados, situação que impossibilita a finalização imediata do tratamento.

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

Art.147°. O compartilhamento de dados pessoais apenas é autorizado nos casos em que seja estritamente necessário, para o regular desempenho das tarefas departamentais em rotinas administrativas.

Parágrafo Único: Entende-se por necessidade regular ao desempenho de tarefas, eventos nos quais, sem o compartilhamento dos dados, não seria possível a regular execução da atividade, tais como: compartilhamento de dados para Instituição bancária na gestão salarial de empregado, com empresas gestoras de benefícios alimentícios, com a administração pública para recolhimento previdenciários, entre outros casos, não se limitando a estes exemplos.

Art.148°. Ressalvadas as rotinas administrativas nas quais o compartilhamento de dados com outros controladores seja necessário para o regular desempenho das tarefas, os colaboradores do CEJAM não estão autorizados a compartilhar dados pessoais em posse da entidade com terceiros.

Parágrafo único: Durante a execução de sua atividade profissional, caso o colaborador se depare com necessidades diferentes das dispostas neste regulamento para fins de compartilhamento de dados pessoais, deverá consultar o Comitê de Segurança da Informação ou departamento jurídico para obter a orientação ideal sobre como proceder.

SEÇÃO II - TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

Art.149°. Considera-se dado pessoal sensível: Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a instituição de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Art.150°. O tratamento de dados pessoais sensíveis deve ser realizado com observância rigorosa às disposições contidas neste regulamento e demais políticas, somente sendo autorizado quando o titular ou seu responsável legal consentir, de forma destacada e para finalidades específicas.

Art.151°. Os casos em que o tratamento de dados sensíveis pode ser executado sem o consentimento do titular são aqueles indispensáveis para as seguintes finalidades:

I. Cumprimento de obrigação legal ou regulatória pela entidade;
II. Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

III. Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

IV. Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

V. Proteção da vida ou da incolumidade física do titular ou de terceiro;

VI. Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

VII. Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no Art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Parágrafo Único: As disposições contidas neste artigo são excepcionais, devendo o consentimento ser a regra básica e inicial no tratamento de dados pessoais conforme disposições do **Art. 132º**.

CAPÍTULO XVII – REVISÃO

Art.152°. O presente regulamento deve ser analisado a cada cinco anos e/ou a qualquer momento para realização de alterações relevantes, devendo ser revisado pela própria equipe e aprovado pelos responsáveis.

Parágrafo Único: Posteriormente, a versão aprovada deverá ser divulgada à Instituição e mantida em arquivo digital de fácil acesso aos colaboradores.

São Paulo, 14 de Agosto de 2024

JOÃO FRANCISCO ROMANO

Gerente Executivo

FLORIZA MENDES

Gerente Administrativa

Centro de Estudos e Pesquisas "Dr. João Amorim"
Rua Dr. Lund, 41 - Liberdade
São Paulo-SP - CEP: 01513-020
11 3469-1818
cejam@cejam.org.br
cejam.org.br

ANEXO I - TERMO DE CONFIDENCIALIDADE

Eu,_____, nacionalidade _____, estado civil _____, com residência na _____ CEP _____, portador (a) do RG nº _____ e inscrito no CPF/MF sob o nº _____, exercendo a função de _____, por meio do presente

Termo, comprometo-me:

1. A manter absoluto sigilo acerca de todas as informações administrativas, técnicas contábeis, fiscais e cadastrais da empresa contratante, dos clientes internos e externos e usuários dos serviços de saúde desta, bem como de dados, documentos, procedimentos e informações a que tenha acesso ou que venha a ter conhecimento por qualquer meio, ainda que não pertinentes ou diretamente vinculados às minhas atividades, compromisso esse que se estende mesmo após o término do contrato de trabalho;

2. Seguir as diretrizes, políticas, treinamentos e instruções ministrados pelo empregador quanto às normas de Governança Corporativa, Programa de Integridade e Programa de Conformidade LGPD, principalmente em assuntos relacionados à confidencialidade de informações e sigilo profissional que vier a ter acesso em virtude de seu vínculo empregatício.

3. A reconhecer que pertence exclusivamente à Instituição contratante, clientes e fornecedores desta os programas de computador disponibilizados, bem como os direitos de autoria e de propriedade, incluindo códigos-fontes, bases de dados, derivativos, rotinas ou aplicativos desenvolvidos a partir dos programas, documentação, desenhos, informações técnicas, patentes, marcas, material de propaganda, análises de marketing, lista de clientes e usuários dos serviços de saúde, sendo que todos têm caráter de informação confidencial e sigilosa, obrigando-se, assim, a não divulgá-los, copiá-los, cedê-los, transferi-los ou torná-los disponíveis a terceiros, sob qualquer hipótese, tampouco utilizá-los, em benefício próprio ou de terceiros, mesmo após o término do contrato de trabalho;

4. Reconhecendo que estou autorizado a utilizar a rede interna de computadores da Instituição ou de onde estiver desenvolvendo minhas atividades, tendo acesso ao correio eletrônico e à

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

internet, me obrigo a fazer uso comedido de tais recursos e estritamente no limite das necessidades de serviço, sendo expressamente vedada a utilização de tais meios de comunicação e informação para finalidades pessoais ou estranhas às atividades a serem desenvolvidas internamente. Comprometo-me, ainda, a não veicular dados, informações ou mensagens injuriosas da Instituição, seus colaboradores, fornecedores e/ou demais clientes internos e externos.

5. A reconhecer que todos os atos e atividades desenvolvidos no CEJAM devem estar em consonância com as disposições da Lei Federal nº.13.709/2018 (LGPD), sobretudo para o tratamento e uso adequado dos dados pessoais dos usuários e terceiros.

Estou ciente que a infração a estas normas constitui falta funcional punível administrativamente, sem prejuízo da responsabilidade penal e civil de acordo com a Lei vigente, responsabilizando-me, inclusive, pelos danos que vier causar à Instituição ou a terceiros, em decorrência do uso indevido das informações por mim acessadas.

Data: _____ Ciente e de acordo _____

Colaborador(a)

_____

Coordenação de Gestão de Pessoas

Centro de Estudos e Pesquisas "Dr. João Amorim"
Rua Dr. Lund, 41 - Liberdade
São Paulo-SP - CEP: 01513-020
11 3469-1818
cejam@cejam.org.br
cejam.org.br

ANEXO II - TERMO DE RESPONSABILIDADE DA GUARDA E USO DE CELULAR CORPORATIVO

O **CENTRO DE ESTUDOS E PESQUISAS "DR. JOÃO AMORIM",** inscrita no **CNPJ** sob o nº_____, entrega neste ato, o aparelho celular modelo:_____ IMEI:_____, linha:_____*, ao(a) colaborador(a) _____, portador do RG sob o nº_____, doravante denominado simplesmente "USUÁRIO" sob as seguintes condições:

1. O equipamento deverá ser utilizado ÚNICA e EXCLUSIVAMENTE a serviço da empresa tendo em vista a atividade a ser exercida pelo USUÁRIO;

2. É vedado o uso do equipamento para armazenamento, compartilhamento edição indevida ou outro tipo de tratamento de dados pessoais para finalidades estranhas ou não autorizadas na atividade profissional do colaborador;

3. Ficará o USUÁRIO responsável pelo uso e conservação do equipamento;

4. O USUÁRIO tem somente a DETENÇÃO, tendo em vista o uso exclusivo para prestação de serviços profissionais e NÃO a PROPRIEDADE do equipamento, sendo terminantemente proibidos o empréstimo, aluguel ou cessão deste a terceiros;

5. Ao término da prestação de serviço ou do contrato individual de trabalho, o USUÁRIO compromete-se a devolver o equipamento em perfeito estado no mesmo dia em que for comunicado ou comunique seu desligamento, considerando o desgaste natural pelo uso normal do equipamento.

linha habilitada para originar ligações para qualquer operadora de telefonia, considerando linhas móveis e fixas. Para chamadas interurbanas (DDD) deve ser utilizado o código de operadora 41 (TIM). Pacote de Internet 5 Gb.

Data: _____ Ciente e de acordo _____

Colaborador(a)

Centro de Estudos e Pesquisas "Dr. João Amorim" Rua Dr. Lund, 41 - Liberdade São Paulo-SP - CEP: 01513-020 11 3469-1818 cejam@cejam.org.br cejam.org.br

RIN.INST.TI.IS.001.004___REGULAMENTO_DE_SEGURANCA_DA_INFORMACAO_(1).pdf

Documento número #994dc8b2-a70a-48ac-81f3-6bee4ac3ca37

Hash do documento original (SHA256): 3f34cb3d4c8c00683e09619ccacd0f9ded2502e033658c33035522e4471aaab0

Assinaturas

Bryan Valdez Nakasato
CPF: 418.957.578-00
Assinou em 28 ago 2024 às 17:56:10

Rodrigo Silva Santa Rita
CPF: 223.901.108-43
Assinou em 28 ago 2024 às 17:55:42

Vinicius Gomes Silva
CPF: 433.979.698-08
Assinou em 29 ago 2024 às 08:38:45

João Francisco Romano
CPF: 125.109.338-84
Assinou em 02 set 2024 às 11:16:58

Floriza de Jesus Mendes Santana
CPF: 359.994.975-15
Assinou em 30 ago 2024 às 13:17:13

Rodrigo Lima Miranda
CPF: 330.481.918-52
Assinou em 28 ago 2024 às 17:48:51

Alexandre Garcia D'Aurea
CPF: 274.134.058-73
Assinou em 29 ago 2024 às 08:55:40

Log

28 ago 2024, 17:45:53	Operador com email danilo.santos@cejam.org.br na Conta 1397fc5c-a13f-44bf-a6e1-975f0f21d497 criou este documento número 994dc8b2-a70a-48ac-81f3-6bee4ac3ca37. Data limite para assinatura do documento: 06 de setembro de 2024 (18:00). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
28 ago 2024, 17:45:54	Operador com email danilo.santos@cejam.org.br na Conta 1397fc5c-a13f-44bf-a6e1-975f0f21d497 adicionou à Lista de Assinatura: bryan.nakasato@cejam.org.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Bryan Valdez Nakasato.
28 ago 2024, 17:45:54	Operador com email danilo.santos@cejam.org.br na Conta 1397fc5c-a13f-44bf-a6e1-975f0f21d497 adicionou à Lista de Assinatura: rodrigo.silva@cejam.org.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Rodrigo Silva Santa Rita.
28 ago 2024, 17:45:54	Operador com email danilo.santos@cejam.org.br na Conta 1397fc5c-a13f-44bf-a6e1-975f0f21d497 adicionou à Lista de Assinatura: vinicius.gomes@cejam.org.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Vinicius Gomes Silva.
28 ago 2024, 17:45:54	Operador com email danilo.santos@cejam.org.br na Conta 1397fc5c-a13f-44bf-a6e1-975f0f21d497 adicionou à Lista de Assinatura: alexandre.daurea@cejam.org.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Alexandre Garcia D'Aurea.
28 ago 2024, 17:45:54	Operador com email danilo.santos@cejam.org.br na Conta 1397fc5c-a13f-44bf-a6e1-975f0f21d497 adicionou à Lista de Assinatura: joao.romano@cejam.org.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo João Francisco Romano.
28 ago 2024, 17:45:54	Operador com email danilo.santos@cejam.org.br na Conta 1397fc5c-a13f-44bf-a6e1-975f0f21d497 adicionou à Lista de Assinatura: floriza.mendes@cejam.org.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Floriza de Jesus Mendes Santana.
28 ago 2024, 17:45:54	Operador com email danilo.santos@cejam.org.br na Conta 1397fc5c-a13f-44bf-a6e1-975f0f21d497 adicionou à Lista de Assinatura: rodrigo.miranda@cejam.org.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Rodrigo Lima Miranda e CPF 330.481.918-52.
28 ago 2024, 17:45:54	Operador com email danilo.santos@cejam.org.br na Conta 1397fc5c-a13f-44bf-a6e1-975f0f21d497 adicionou à Lista de Assinatura: alexandre.daurea@cejam.org.br para assinar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Alexandre Garcia D'Aurea.
28 ago 2024, 17:45:54	Operador com email danilo.santos@cejam.org.br na Conta 1397fc5c-a13f-44bf-a6e1-975f0f21d497 adicionou o signatário bryan.nakasato@cejam.org.br para assinar e rubricar todas as páginas.
28 ago 2024, 17:45:54	Operador com email danilo.santos@cejam.org.br na Conta 1397fc5c-a13f-44bf-a6e1-975f0f21d497 adicionou o signatário rodrigo.silva@cejam.org.br para assinar e rubricar todas as páginas.

28 ago 2024, 17:45:54	Operador com email danilo.santos@cejam.org.br na Conta 1397fc5c-a13f-44bf-a6e1-975f0f21d497 adicionou o signatário vinicius.gomes@cejam.org.br para assinar e rubricar todas as páginas.
28 ago 2024, 17:45:54	Operador com email danilo.santos@cejam.org.br na Conta 1397fc5c-a13f-44bf-a6e1-975f0f21d497 adicionou o signatário alexandre.daurea@cejam.org.br para assinar e rubricar todas as páginas.
28 ago 2024, 17:45:54	Operador com email danilo.santos@cejam.org.br na Conta 1397fc5c-a13f-44bf-a6e1-975f0f21d497 adicionou o signatário joao.romano@cejam.org.br para assinar e rubricar todas as páginas.
28 ago 2024, 17:45:54	Operador com email danilo.santos@cejam.org.br na Conta 1397fc5c-a13f-44bf-a6e1-975f0f21d497 adicionou o signatário floriza.mendes@cejam.org.br para assinar e rubricar todas as páginas.
28 ago 2024, 17:45:54	Operador com email danilo.santos@cejam.org.br na Conta 1397fc5c-a13f-44bf-a6e1-975f0f21d497 adicionou o signatário rodrigo.miranda@cejam.org.br para assinar e rubricar todas as páginas.
28 ago 2024, 17:45:54	Operador com email danilo.santos@cejam.org.br na Conta 1397fc5c-a13f-44bf-a6e1-975f0f21d497 adicionou o signatário alexandre.daurea@cejam.org.br para assinar e rubricar todas as páginas.
28 ago 2024, 17:48:51	Rodrigo Lima Miranda assinou. Pontos de autenticação: Token via E-mail rodrigo.miranda@cejam.org.br. CPF informado: 330.481.918-52. Rubricou todas as páginas. IP: 187.88.22.16. Localização compartilhada pelo dispositivo eletrônico: latitude -23.480129383671635 e longitude -46.57670402204329. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.970.0 disponibilizado em https://app.clicksign.com.
28 ago 2024, 17:55:42	Rodrigo Silva Santa Rita assinou. Pontos de autenticação: Token via E-mail rodrigo.silva@cejam.org.br. CPF informado: 223.901.108-43. Rubricou todas as páginas. IP: 187.10.71.33. Componente de assinatura versão 1.970.0 disponibilizado em https://app.clicksign.com.
28 ago 2024, 17:56:10	Bryan Valdez Nakasato assinou. Pontos de autenticação: Token via E-mail bryan.nakasato@cejam.org.br. CPF informado: 418.957.578-00. Rubricou todas as páginas. IP: 200.229.239.10. Componente de assinatura versão 1.970.0 disponibilizado em https://app.clicksign.com.
29 ago 2024, 08:38:45	Vinicius Gomes Silva assinou. Pontos de autenticação: Token via E-mail vinicius.gomes@cejam.org.br. CPF informado: 433.979.698-08. Rubricou todas as páginas. IP: 200.155.175.94. Componente de assinatura versão 1.970.1 disponibilizado em https://app.clicksign.com.
29 ago 2024, 08:55:40	Alexandre Garcia D'Aurea assinou. Pontos de autenticação: Token via E-mail alexandre.daurea@cejam.org.br. CPF informado: 274.134.058-73. Rubricou todas as páginas. IP: 200.229.239.10. Componente de assinatura versão 1.970.2 disponibilizado em https://app.clicksign.com.
29 ago 2024, 09:26:46	Operador com email danilo.santos@cejam.org.br na Conta 1397fc5c-a13f-44bf-a6e1-975f0f21d497 removeu da Lista de Assinatura: alexandre.daurea@cejam.org.br para assinar.
30 ago 2024, 13:17:13	Floriza de Jesus Mendes Santana assinou. Pontos de autenticação: Token via E-mail floriza.mendes@cejam.org.br. CPF informado: 359.994.975-15. Rubricou todas as páginas. IP: 200.155.175.94. Localização compartilhada pelo dispositivo eletrônico: latitude -23.5535051 e longitude -46.6126353. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.972.0 disponibilizado em https://app.clicksign.com.

02 set 2024, 11:16:58	João Francisco Romano assinou. Pontos de autenticação: Token via E-mail joao.romano@cejam.org.br. CPF informado: 125.109.338-84. Rubricou todas as páginas. IP: 200.229.239.10. Localização compartilhada pelo dispositivo eletrônico: latitude -23.5567187 e longitude -46.632872. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.972.0 disponibilizado em https://app.clicksign.com.
02 set 2024, 11:16:59	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 994dc8b2-a70a-48ac-81f3-6bee4ac3ca37.

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 994dc8b2-a70a-48ac-81f3-6bee4ac3ca37, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.