# Política de Segurança da Informação

**Cenpec - 2023**

# Apresentação

A Política de segurança da informação, no Cenpec, adiante denominada somente como "Instituição", aplica-se a todas(os) as(os) administradoras(es), funcionárias(os), prestadoras(es) de serviços, sistemas e serviços, incluindo no caso de trabalhos e projetos executados externamente ou por terceiros, que utilizem o ambiente de processamento da instituição, ou acesso a informações pertencentes à instituição.

**Todo e qualquer usuário de recursos computadorizados ou de telecomunicações da instituição tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.** A violação desta política de segurança é qualquer ato que:

1. Exponha a instituição a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados e/ou de informações ou ainda da perda de equipamento.
2. Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.
3. Englobe o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

**A quem se aplica:**

A todas(os) as(os) integrantes do Cenpec, como associadas(os), conselheiras(os), colaboradoras(es) (equipe interna), e a todas(os) aquelas(es) que se relacionam direta ou indiretamente com a organização (terceiros), como fornecedoras(es), prestadoras(es) de serviço, consultoras(es), voluntárias(os), investidoras(es), doadoras(es), organizações apoiadas e quaisquer outras partes interessadas.

A Política de Segurança da Informação se baseia na norma ISO 27002, que deverá orientar as normas internas.

# Glossário

| SIGLA/TERMO | SIGNIFICADO |
|---|---|
| TI | Setor de Tecnologia da Informação |
| DPO | Encarregada(o) de Dados do Cenpec |
| CTD | Coordenação de Tecnologias Digitais |
| RMM | Software de Gerenciamento e Monitoramento Remoto<br>(Remote Monitoring and Management) |
| CPD | Central de Processamento de Dados |
| HD | Unidade de disco rígido |
| LGPD | Lei Geral de Proteção de Dados (Lei nº 13.709/2018) |
| Dado pessoal | Informação relacionada a pessoa natural identificada ou identificável. |
| Dado pessoal sensível | Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. |
| Fishing | Forma de invasão para capturar os dados. |
| Ransomware | Sequestro de dados. |

| | |
|---|---|
| Comissão LGPD | É composto pelo DPO e representantes da área de Programas e Projetos, TI e administrativo, com o objetivo de fazer a gestão dos dados da instituição junto ao DPO. |
| Comitê de Crise | O Comitê de Crise consiste em uma equipe reativa que irá lidar diretamente de forma organizada em uma situação de incidente.<br><br>Ele deve contar com pessoas de diferentes áreas e expertises, como Segurança da Informação, Tecnologia da Informação (TI), Jurídico, Proteção de Dados, Comunicação etc., para garantir a multidisciplinaridade de atuação, quando de uma ocorrência de um incidente.<br><br>Essa equipe avaliará o impacto do incidente e as medidas a serem adotadas para mitigar os efeitos da ocorrência. Um comitê de crise deve ser formado não apenas em situações que envolvam dados pessoais, de forma geral, mas também em acontecimentos que possam ter repercussões graves para os direitos de titulares e a imagem do Cenpec. |
| Comitê LGPD | É composto por colaboradoras(es) de diferentes áreas da instituição, com reuniões mensais com o apoio da consultoria jurídica, para atualização das diretrizes da LGPD e discussão/encaminhamentos de possíveis casos. |

## 1. OBJETIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização do negócio da instituição. Estabelecer a segurança e proteger as informações da instituição, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

## 2. RESPONSABILIDADE PARA COM A INFORMAÇÃO

**Considerar a informação como um bem da instituição, um dos recursos críticos para a realização do negócio, que detém grande valor para a instituição e deve sempre ser tratada profissionalmente.**

## 3. CLASSIFICAÇÃO DA INFORMAÇÃO

**É de responsabilidade do administrador de cada área estabelecer critérios relativos ao nível de confidencialidade da informação** (e-mails, documentos, relatórios e/ou mídias digitais, áreas administrativas dos sistemas dos projetos) gerada por sua área de acordo com os itens abaixo:

Nível 1 - Informação pública: Acessível por qualquer pessoa.

Nível 2 - Informação de uso interno: Acesso apenas pelos colaboradores do Cenpec.

Nível 3 - Informação confidencial: Acesso apenas por equipes pré-definidas internamente.

Nível 4 - Informação restrita: Acesso apenas por pessoas autorizadas.

Medidas de segurança

Nível 3 e 4: Adoção de senha individual, robusta e específica para acesso ao documento/pasta.

Nível 2: Acesso ao banco de dados deve ser individualizado e com senha de acesso ao software de armazenamento.

Nesta classificação, as bases de dados serão organizadas de acordo com o nível de confidencialidade do conteúdo. Podendo ocorrer, inclusive, de um dado/documento ser classificado em duas categorias. Alguns exemplos práticos:

- Registro admissional de empregado: nível 3 e 4. Ou seja, quem tem acesso às informações é o setor de Recursos Humanos, mas nem todas as pessoas da equipe devem ter acesso, apenas aquelas que tratam as informações na execução de suas atividades.
- Folha de pagamento/holerite: nível 3.
- Informações públicas pessoais + dados de origem étnica/racial (dados sensíveis): nível 3. Neste caso temos a reunião de informações que seriam de nível 1 e nível 3. Desta

forma, deve-se aplicar ao banco de dados as medidas de segurança do nível 3 que garante maior segurança.

**Toda(o) gestora(or) deve orientar sua equipe a não circular informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito "mesa limpa", ou seja, ao terminar o trabalho não deixar a máquina aberta (sempre bloquear seu login) e nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas, seja no trabalho presencial ou remoto (home office).**

Arquivos sensíveis deverão ser criptografados com senha de acesso.

As informações podem ser reclassificadas ao longo do tempo, em função de novos fatos ou de divulgação.

### 3.1. Limitação de acesso

Assim, com a classificação das informações, **os dados pessoais devem ser acessados apenas pelas pessoas que, para a execução da sua atividade, precisam ter acesso à informação.** Essa limitação de acesso consiste em um processo elaborado pela administração do Cenpec e o setor de tecnologia que evita a disseminação desnecessária de informações e possíveis lesões aos titulares de dados tratados pelo Cenpec.

Com essa implementação, o colaborador terá acesso apenas aos dados pessoais necessários para realizar o seu trabalho, devendo adotar medidas de salvaguarda em seu tratamento:

a. Quando precisar se ausentar de sua estação de trabalho ou da vista da sua máquina, bloqueie o computador para que os dados não fiquem expostos.
b. Quando encerrar o dia de trabalho, desligue o computador do Cenpec. Não deixe o log-in automático nesses sistemas, devendo inserir sua credencial de identificação e senha sempre que iniciar o dia ou quando precisar se ausentar por muito tempo do seu local de trabalho.
c. Não utilize informações pessoais na criação/alteração de suas senhas ou padrões comuns e fracos. Caso tenha dúvidas sobre a criação de senhas fortes, consulte a(o) encarregada(o) de dados do Cenpec.

**No contexto de trabalho remoto, a(o) colaboradora(or) que usa um equipamento do Cenpec é responsável pelo seu uso. Se quaisquer pessoas que não pertencem à organização acessarem o computador, a responsabilidade será da(o) colaboradora(or) responsável por aquela máquina. Por isso, casos de perda ou roubo do maquinário devem ser comunicados imediatamente ao superior imediato, ao RH, à TI e ao DPO.**

**Em caso de necessidade de acesso às informações que não estejam disponíveis,** seja pelo nível de confidencialidade ou porque a(o) funcionária(o) não está envolvida(o) na atividade para qual o dado foi coletado, a(o) funcionária(o) deverá solicitar acesso específico às informações necessárias enviando junto o motivo da necessidade e por quanto tempo vai precisar do acesso à(ao) gestor a(or) do processo/atividade em que a informação está sendo tratada.

**Quando se tratar de informações confidenciais:** A(O) gestora(or) realizará consulta à(ao) encarregada(o) de dados referente à disponibilização das informações. Havendo a liberação da(o) encarregada(o) de dados, a(o) gestora(or) disponibilizará apenas os dados especificados como necessários. Será criada uma pasta de acesso em que constará apenas o dado/documento necessário com acesso apenas pela(o) gestora(or) e pela(o) colaboradora(or) que solicitou a informação. A(O) colaboradora(or) não deve armazenar em local diverso a informação.

Caberá à comissão LGPD (com auxílio do Comitê de LGPD) registrar a atividade de tratamento em questão. Após a finalização da utilização dos dados, a(o) gestora(or) inicial deve finalizar a atividade de tratamento com a eliminação da pasta e dos dados/documentos constantes nela.

## 4. DADOS DAS(OS) COLABORADORAS(ES)

**A instituição se compromete a não acumular ou manter intencionalmente Dados Pessoais de colaboradoras(es) além daqueles necessários para o cumprimento das finalidades para as quais foram coletados e/ou de acordo com as bases legais da LGPD (art. 16).** Todos os dados pessoais das(os) colaboradoras(es) serão considerados dados restritos. Dados Pessoais de colaboradores sob a responsabilidade da instituição não serão usados para fins diferentes daqueles para os quais foram coletados.

**Dados pessoais de colaboradoras(es) não serão transferidos para terceiros, exceto quando necessário para o cumprimento da finalidade, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, nesse caso, a lista de endereços eletrônicos (e-mails) usados pelos colaboradores da instituição. Por outro lado, as(os) colaboradoras(es) se comprometem a não armazenar dados pessoais nas instalações (máquinas locais em escritórios compartilhados) e equipamentos da instituição, sem prévia e expressa autorização da diretoria.**

Os computadores podem ser formatados (apagados) a qualquer momento pela equipe de TI do Cenpec, sendo sempre verificado e confirmado com a(o) gestora(or) e a(o) DPO se os dados

armazenados nas máquinas podem efetivamente ser eliminados das bases de dados do Cenpec.

## 5. ADMISSÃO E DEMISSÃO DE COLABORADORAS(ES)/ TEMPORÁRIAS(OS) / ESTAGIÁRIAS(OS)

A contratação de colaboradoras(es), estagiárias(os), temporárias(os) e prestadoras(es) de serviços é de aprovação exclusiva da diretoria da instituição.

O RH da instituição deverá informar à Tecnologia da Informação (TI) e à Coordenação de Tecnologias Digitais (CTD), toda e qualquer movimentação de temporárias(os) e/ou estagiárias(os), e admissão/demissão de funcionárias(os), para ser **cadastradas(os)** ou **excluídas(os)** em todo ambiente tecnológico da instituição (conta Google, sistemas dos projetos, ferramenta de disparo de e-mail etc.). Isto inclui o fornecimento de sua senha ("password") e registro do seu nome como usuário no ambiente pela TI e/ou pela CTD.

A comissão LGPD também deverá ser comunicada sobre admissões e demissões de funcionárias(os), devendo o RH encaminhar informações sobre:

No caso de admissão: o tipo de contratação, os dados pessoais coletados e para quais finalidades, local de armazenamento das informações, setores/pessoas com acesso às informações e, por fim, se o contrato em questão tem prazo para encerramento.

No caso de demissão: informações sobre o titular de dados em questão e seu contrato com o Cenpec.

Cabe ao departamento solicitante da contratação a comunicação a TI sobre as rotinas a que o novo contratado terá direito de acesso (matriz de acesso), encaminhando essas informações com cópia para a comissão LGPD. No caso de temporárias(os) e/ou estagiárias(os) deverá também ser informado o tempo em que o mesmo prestará serviço à instituição, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas ao direito de seu acesso ao sistema. No caso de demissão, o RH deverá comunicar o fato antecipadamente a TI e a CTD, para que a(o) funcionária(o) desligada(o) seja excluída(o) do ambiente tecnológico da instituição, garantindo a segurança da informação.

Quando ocorrer o desligamento de qualquer colaboradora(or) da instituição, todas as mensagens eletrônicas dessa(e) colaboradora(or) deverão ser redirecionadas para funcionárias(os) indicados pelo responsável de sua área.

Cabe ao RH dar conhecimento e obter as devidas assinaturas de concordância das(os) novas(os) contratadas(os) em relação à Política de Segurança da Informação da instituição e ao Termo de adesão à Política de Integridade. Nenhuma(um) colaboradora(or), estagiária(o) ou temporária(o) poderá ser contratada(o), sem ter expressamente concordado com esta política e com o termo de adesão à Política de Integridade.

## 6. TRANSFERÊNCIA DE COLABORADORAS(ES) / TEMPORÁRIAS(OS) / ESTAGIÁRIAS(OS)

Quando uma(um) colaboradora(or) for promovida(o) ou transferida(o) de seção ou gerência, o RH deverá comunicar o fato ao TI e à comissão LGPD do Cenpec, para que sejam feitas as adequações necessárias para o acesso da(o) referida(o) funcionária(o) ao sistema informatizado da instituição e para que a comissão LGPD atualize o registro interno das informações sobre tratamento de dados pessoais.

## 7. TREINAMENTO E CONSCIENTIZAÇÃO EM SEGURANÇA

**Toda(o) colaboradora(or) ou parceira(o) nova(o) deverá realizar, nos dois primeiros dias de trabalho, a leitura desta Política de Segurança e assinar o Termo de Ciência da Política, que serão arquivados no RH.**

**Além disso, deverá passar por treinamento para conscientização e aculturamento sobre proteção de dados pessoais e LGPD.**

Será realizada, mensalmente, reunião de segurança envolvendo a TI, para discussão de problemas, providências e novas implantações de segurança na instituição.

Reuniões de Segurança extras serão convocadas pela diretoria em caso de eventos extraordinários ou urgentes.

As(Os) colaboradoras(es) não ligadas(os) à área de TI passarão, a cada 90 dias, por uma reciclagem de segurança, realizando a troca de senha de acesso ao ambiente tecnológico da instituição. O computador das(os) colaboradoras(es) será visitado remotamente e semanalmente pela equipe de TI para rotinas de atualizações do Windows e atualização de antivírus que rodam de forma automática nos computadores. Serão realizados treinamentos e

capacitações para todas(os) as(os) colaboradoras(es) ao longo do ano, sempre que necessário, para orientações, esclarecimentos e recomendações.

## 8. USO INDEVIDO DE PROGRAMAS DE COMPUTADOR

Os programas de computador são protegidos pela lei de direitos autorais, a Lei nº 9.610/98, e pela legislação específica de software, a Lei nº 9.609/98. Sendo assim, o uso dos programas de computador depende de contratos de licença ou de autorização do titular da propriedade intelectual, exceto quando se tratar de softwares disponibilizados por meio de licenças de uso livre e gratuito.

O Cenpec respeita os direitos de propriedade intelectual sobre os programas de computador que usa e reconhece que deve pagar o justo valor por eles, não autorizando o uso de programas não licenciados nos computadores da instituição. É terminantemente proibido o uso indevido de programas (sem licenciamento) na instituição.

**As(Os) usuárias(os) não podem, em hipótese alguma, instalar este tipo de software nos equipamentos da instituição, mesmo porque somente o pessoal da TI tem autorização para instalação de programas previamente autorizados dentro da política de segurança da instituição. Por essa razão, as(os) usuárias(os) devem se assegurar de que não estão executando ações que possam infringir direitos sobre a propriedade intelectual de terceiros. Por isso, não é permitido instalar programas provenientes da Internet nos computadores da instituição, sem expressa anuência da TI.**

Periodicamente, a TI fará verificações nos dados dos servidores e/ou nos computadores da instituição, visando garantir a correta aplicação desta diretriz. Caso sejam encontrados programas de uso não autorizados, estes deverão ser removidos dos computadores. A TI deverá elaborar relatório sobre a ocorrência para formalizar e encaminhar à administração do Cenpec e ao(à) DPO. A administração do Cenpec analisará internamente as implicações para determinação de sanção e a(o) DPO fará a análise do caso para verificar possíveis ocorrências de incidentes de segurança. Caso seja confirmado um incidente, a(o) DPO deve fazer o registro interno da ocorrência e demais determinações do item 15 desta política.

Aquelas(es) que instalarem em seus computadores de trabalho tais programas de uso não autorizado se responsabilizarão perante a instituição e terceiros por quaisquer problemas ou prejuízos causados por essa ação.

## 9. PERMISSÕES E SENHAS

Para acessar sua estação de trabalho nos computadores da instituição, toda(o) usuária(o) deverá possuir login e senha previamente cadastrados pela TI, utilizando a dupla autenticação. O login e a senha de acesso ao ambiente administrativo dos sistemas dos projetos serão previamente cadastrados pela equipe CTD, também com dupla autenticação.

Somente a Diretoria e administradoras(es) de TI poderão ter acesso de administrador ao ambiente Google Workspace.

As(Os) usuárias(os) poderão receber outras senhas de acesso a subsistemas da Intranet (por exemplo, web sites internos) somente quando necessário e de acordo com as diretrizes do item 3.1 desta Política.

Quem deve fornecer os dados referentes aos direitos da(o) usuária(o) é a(o) responsável direta(o)pelo RH, que deve encaminhar um e-mail ao TI. Quando da necessidade de cadastramento de uma(um) nova(o) usuária(o) para utilização da "rede", sistemas ou equipamentos de informática da instituição, o RH deverá comunicar esta necessidade a TI, por meio de memorando ou e-mail, informando a que tipo de rotinas e programas a(o) nova(o) usuária(o) terá direito de acesso e quais serão restritos.

A área de TI fará o cadastramento e informará à(ao) nova(o) usuária(o) o seu login e sua senha. A TI deverá se atentar para gerar senhas sem utilizar dados pessoais da(o) nova(o) usuária(o).

**Todas(os) as(os) usuárias(os) responsáveis pela aprovação eletrônica de documentos (exemplo: pedidos de compra, solicitações e etc.) deverão comunicar a TI qual será sua(seu) substituta(o) quando de sua ausência da instituição, para que as permissões possam ser alteradas (delegação de poderes).** Quando houver necessidade de compartilhamento de dados e informações para usuários externos, é necessário primeiramente entender se no banco de dados em questão existem dados pessoais. Caso a resposta seja afirmativa, precisamos seguir o seguinte fluxo:

a. A(O) gestora(or) da atividade precisa ser comunicada(o) sobre a solicitação;

b. A(O) gestora(or) deverá contatar a(o) encarregada(o) de dados para auxiliar na demanda. O e-mail de comunicação interna com a(o) encarregada(o) de proteção de dados deve conter as seguintes informações:

i. Com quem os dados e por quanto tempo serão compartilhados (pessoa, consultor, outra organização ou empresa).

| |
|---|
| ii. Por qual motivo os dados pessoais serão compartilhados (por exemplo: execução de parte do projeto comandado pelo Cenpec, análise conjunta de uma mesma base de dados pessoais, prestação de contas sobre um projeto da entidade etc.) |
| iii. Quais são as finalidades para as quais a pessoa/organização, com quem os dados serão compartilhados, podem utilizar tais dados pessoais? |
| iv. Existência de cláusula contratual prevendo os cuidados que a pessoa ou organização deve ter com os dados pessoais transferidos pelo Cenpec. |

| | |
|---|---|
| 1. Estou compartilhando dados pessoais ou dados pessoais sensíveis?<br><br>2. Os dados pessoais que irei compartilhar já são acessados pelas pessoas para quem eles serão enviados?<br>3. Há risco/probabilidade da pessoa ou organização, com quem ocorreu o compartilhamento, utilizar os dados pessoais para objetivos diferentes daqueles que foram informados às(aos) titulares de dados pessoais ou ela tratará os dados justamente para que essa finalidade se realize? | A resposta à primeira pergunta, indicará o risco envolvido no compartilhamento de dados, uma vez que os dados pessoais sensíveis podem colocar a(o) titular de dados em situações de discriminação se usados incorretamente.<br><br>Já a resposta às perguntas 2 e 3 indica se pode existir o risco de acesso indevido ou desvio de finalidade por parte da pessoa ou organização para a qual os dados pessoais estão sendo transferidos. Isso é importante para evitar que os dados sejam utilizados de forma diferente do que foi informado para as(os) titulares de dados pessoais. |

c. Assim, existindo o compartilhamento, a(o) encarregada(o) de dados entenderá se este compartilhamento constitui uma nova finalidade que não foi informada anteriormente ao titular, verificando os riscos do compartilhamento e como coletar o consentimento da(o) titular de dados para essa nova atividade, dando a devida transparência sobre a atividade.

d. Assim, será preciso analisar se o contrato ou termo firmado com o terceiro traz disposições detalhadas sobre proteção de dados e o processamento de informações;

e. Na inexistência de cláusulas sobre proteção de dados, com a ajuda da(o) encarregada(o) de dados, será analisada a necessidade de estabelecer um acordo de processamento de dados entre o Cenpec e o terceiro;

f. Somente após estas análises e eventual assinatura de acordo que a atividade de compartilhamento poderá ser realizada.

Quando o compartilhamento não envolver dados pessoais, será gerada uma pasta com acesso apenas às informações que o terceiro necessita acessar. A permissão de acesso deverá ser bloqueada tão logo este tenha terminado o seu trabalho, e se houver no futuro nova necessidade de acesso, deverá então ser desbloqueada pela TI.

As senhas de administrador ("root") de todos os equipamentos da instituição, inclusive servidores, roteadores, estações de trabalho, máquinas virtuais, equipamentos de telecomunicações e outros, deverão ser conhecidas e armazenadas pelas(os) administradoras(es) de TI. Todos os equipamentos acima, que utilizarem de acesso por chaves criptográficas (como certificados SSH), deverão ter instalados os certificados da diretoria da instituição e do responsável de segurança, na conta de administrador ou "root" desses equipamentos.

É obrigatório que as(os) usuárias(os) criem um arquivo criptografado (por exemplo, criptografia Microsoft) ou protegido por senha para registrar logins e senhas em seu computador, bem como outras informações sensíveis da instituição (ver item 3. Acima).

## 10. COMPARTILHAMENTO DE DADOS E SEGURANÇA CONTRA INCIDENTES

Não é permitido o compartilhamento de arquivos da instituição com terceiros sem autorização. No caso de os arquivos conterem dados pessoais, a(o) encarregada(o) de dados deverá analisar os riscos envolvidos no compartilhamento ulterior para verificar se concederá autorização. Todos os dados deverão ser armazenados nas pastas em nuvem da instituição (Google Drive) com limitação de acesso interno e seguindo as determinações de classificação dos dados do item 3 desta política, e a autorização para acessá-los deverá ser administrada pela TI, baseada na matriz de acesso definida pelas lideranças das áreas (Diretoras(es)/Gerentes/Coordenadoras(es)). A TI está orientada a periodicamente verificar

remotamente todos os compartilhamentos existentes e garantir que dados considerados confidenciais e/ou restritos estejam armazenados adequadamente na nuvem, devendo o compartilhamento de informações com terceiros ser realizado com a abertura de pasta específica para o compartilhamento em questão.

Os compartilhamentos de impressoras devem estar sujeitos às autorizações de acesso da TI, baseado na matriz de acesso definida pelas lideranças das áreas.

Não é permitido na instituição o uso de dispositivos móveis ou qualquer outro meio de armazenamento externo para arquivos com dados pessoais, confidenciais e/ou restritos, tais como pen-drives, HD externo e outras nuvens (dropbox, etc), sem a devida autorização.

Deverão ser criados algumas(ns) usuárias(os) de controle por ambiente do projeto que funcionarão como alarmes no caso de vazamento de dados, garantindo que saberemos a origem do vazamento. Por exemplo, criar e cadastrar um usuário controle: emerson.emlioeof@gmail.com no projeto Escrevendo o Futuro. A equipe irá monitorar esta(e) usuária(o) e, caso seja verificado o recebimento de algum e-mail fora do projeto, o TI saberá a origem do vazamento, devendo sempre envolver a DPO e o Comitê de Dados em situações de incidente de segurança.

## 11. BACKUP (CÓPIA DE SEGURANÇA DOS DADOS)

Todos os dados da instituição deverão ser protegidos por meio de rotinas sistemáticas de Backup, para assegurar a continuidade de negócios em caso de sinistro nos ambientes (físico e nuvem) do Cenpec. Cópias de segurança das pastas em nuvem da instituição (Google Drive) e dos sistemas dos projetos são de responsabilidade da TI e da CTD, respectivamente, e deverão ser feitas diariamente e registradas na pasta de evidência.

Ao final de cada mês também deverá ser feita uma cópia de segurança com os dados de fechamento do mês, dos dados das pastas em nuvem da instituição (Google Drive).

Validação do Backup – Mensalmente o backup deverá ser testado pela TI, voltando-se parte ou todo o conteúdo do backup em um local previamente definido para este fim. Essa operação deverá ser acompanhada e registrada (na pasta de evidências) pelo administrador da instituição responsável por supervisionar a área de TI.

**Política de retenção da nuvem da instituição (Google Drive)**

Cópias diárias, semanais e mensais deverão ser realizadas.

**Política de retenção dos sistemas/ambientes dos projetos (AWS):**

● Backup da base de dados: a base de dados deve ser configurada com backup automático por 7 dias, possibilitando o retorno para qualquer segundo anterior por meio da análise de logs.

● Backups da aplicação: diariamente, durante a madrugada, devem ser realizados backups dos ambientes de produção.

● Manter os backups off-line, garantindo que os dados do backup não fiquem acessíveis em ambiente de produção.

## 12. INVENTÁRIO DE ATIVOS (computadores)

A TI é responsável por manter um sistema de inventário de ativos (hoje utilizamos o software de monitoramento RMM), que permite identificar o acervo de equipamentos e softwares.

No caso de softwares licenciados, o sistema deverá registrar licenças e documentação.

O administrativo deve controlar e informar à TI e à CTD a assinatura e uso de ferramentas digitais e serviço on-line para os projetos.

## 13 . CÓPIAS DE SEGURANÇA DE ARQUIVOS EM DESKTOPS

**Não é política da instituição o armazenamento de dados em desktops individuais, entretanto existem alguns programas fiscais que não permitem o armazenamento em nuvem. Nesses e em outros casos, a TI deverá alertar à(ao) usuária(o) que ela(e) deve fazer backup dos dados de sua máquina periodicamente.**

**É responsabilidade das(os) próprias(os) usuárias(os) a elaboração de cópias de segurança ("backups") de dados e outros arquivos ou documentos, desenvolvidos pelas(os) colaboradoras(es) em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da instituição.**

**No caso das informações consideradas de fundamental importância para a continuidade dos negócios da instituição (por exemplo, o Imposto de Renda Pessoa Jurídica do Cenpec), a TI analisará caso a caso e orientará onde cada usuário deverá manter estas informações. Estas informações serão incluídas na rotina diária de backup.**

## 14. SEGURANÇA E INTEGRIDADE DOS DADOS E SERVIDORES

O gerenciamento, a manutenção, a alteração e a atualização de equipamentos e programas de dados é responsabilidade exclusiva da TI.

Os servidores e equipamentos associados (como roteadores, switches, modems, nobreaks e refrigeração) estão mantidos em local de acesso restrito. A TI definirá quais funcionárias(os) e parceiras(os**)** poderão ter acesso físico e remoto aos servidores, com os devidos protocolos de registro de segurança.

A área dos servidores e equipamentos associados deverá ter recursos de segurança ambiental, como detectores de fumaça e extintores de incêndio.

É proibido comer, beber ou fumar na área dos servidores. Somente deverão ser portados equipamentos e ferramentas necessários à execução de atividades técnicas.

É proibida a remoção de servidores e equipamentos associados sem permissão da Diretoria ou do gestor de TI. É proibida a retirada de discos (HDs) na sala de servidores. É proibido o uso de *pen drives* ou equipamentos externos de armazenamento na sala de servidores, salvo permissão da Diretoria ou do gestor de TI.

Os servidores deverão estar permanentemente conectados aos equipamentos de “nobreak”. Os “nobreaks” deverão ser testados mensalmente, e enviados para manutenção quando necessário.

Nos próximos anos, a tendência é desativar todo o ambiente físico, ficando apenas como legado, sendo todos os arquivos da instituição migrados e armazenados em nuvem do Cenpec (Google Drive).

## 15. DIRETRIZES PARA A EVENTUALIDADE DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

### 15.1. Notificação Interna sobre o Incidente

Um incidente de segurança ocorrerá com a violação da segurança dos dados, ou seja, com acesso não autorizado a determinadas informações, acesso acidental ou qualquer outro ilícito

que venha a ensejar a **destruição, a alteração, a perda, o vazamento ou qualquer forma de tratamento de dados que possa ser considerada ilícita ou inadequada**. Assim, havendo a percepção da ocorrência de um incidente, deve-se contatar imediatamente o Comitê de Crise e o Encarregado pelo Tratamento de Dados Pessoais do Cenpec, notificando-lhes imediatamente sobre o ocorrido e apresentando-lhes o máximo de informações possível sobre o que foi percebido como Incidente.

Pode-se considerar como incidente de segurança:

- Falhas de sistemas de informações e perdas de serviços.
- Identificação de Código malicioso.
- Negação de serviço.
- Erros resultantes de dados incompletos ou inconsistentes.
- Violações de confidencialidade e integridade.
- Uso impróprio de sistemas de informação.
- Acesso indevido ou não autorizado, físico ou lógico, a servidores e equipamentos associados.
- Modificações não autorizadas em servidores e equipamentos associados, ou sistemas operacionais e softwares, ou componentes da rede
- Recebimento de e-mails suspeitos como em caso de *fishing* e/ou indicação de invasão dos sistemas via Ransomware.

A notificação da ocorrência deverá acontecer via e-mail comite.lgpd@cenpec.org.br que, por sua vez, deverá ser de conhecimento de todos do Cenpec. A comunicação sobre potencial Incidente com Dados Pessoais deve conter, no mínimo:

- Nome do Projeto ou área afetada;
- Qual a ocorrência (descrição mais detalhada possível sobre o que ocorreu);
- Data;
- Hora;
- Quais medidas foram adotadas (caso já tenha havido alguma).

No caso de **vazamento de dados**, acrescente-se às informações mencionadas acima:

(i) Quais dados foram vazados e onde ocorreu o vazamento (se já houver identificado);

(ii) Qual foi a comunicação que ocorreu com o titular de dados (se tiver havido);

(iii) Demais dados do incidente ou qualquer outra informação que tenha sido utilizada para identificar a atividade.

Uma vez recebida a notificação interna a respeito de um Incidente, seja real ou suspeito, é necessário, primeiramente a avaliação do DPO e Comitê LGPD do envolvimento efetivo de dados pessoais na ocorrência. Caso seja identificado que a situação não envolve dados pessoais, o DPO repassará aos administradores das áreas de TI a demanda, ficando a cargo desta equipe relatar o incidente à Diretoria da Instituição e agir em conjunto com o Comitê de Crise, avaliando os riscos atrelados ao Incidente para estipulação das medidas para a solução da ocorrência, segundo os seguintes princípios:

- Preservação do ambiente e armazenamento das evidências e circunstâncias
- Perícia do ambiente
- Análise e identificação da causa do incidente
- Planejamento e implantação das medidas corretivas ou preventivas
- Comunicação com aqueles afetados ou envolvidos
- Notificação para a autoridade apropriada.

Contudo, caso identificado que a ocorrência envolve dados pessoais, deve ser adotada as diretrizes do Protocolo LGPD - Incidente de Segurança.

## 16. ACESSO À INTERNET

Em caso de trabalho presencial, o acesso à Internet será autorizado pela diretoria da instituição para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na instituição. Sites que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados.

**O uso da Internet pelo computador da instituição é monitorado pela TI, através de "logs" (arquivos gerados no Google Workspace).**

Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- De conteúdo pornográfico ou relacionado a sexo;
- Que defendam atividades ilegais;

- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
- Que promovam a participação em salas de discussão, chats, *messaging*, conferências e videoconferências, em assuntos não relacionados aos negócios da instituição;
- Que promovam discussão pública sobre os negócios da instituição, a menos que autorizado pela Diretoria;
- Que possibilitem a distribuição de informações de nível “Interno, Confidencial ou Restrito”.
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.
- Que permitam o armazenamento externo de quaisquer dados pessoais e/ou confidenciais/restritos da instituição (como "*cloud-drives*" e semelhantes), sem a devida autorização.

## 17. ACESSO REMOTO

O acesso remoto aos servidores físicos da instituição será autorizado nas seguintes condições:

- Para execução de tarefas de administração, manutenção, programação ou solução de problemas.
- Mediante uso de VPN previamente autorizada.
- Os certificados instalados nos servidores deverão ser previamente autorizados pela Diretoria ou pelo gestor de TI da instituição.
- Mediante liberação do IP do ponto de origem do acesso (projetos/rede/máquinas)

Sempre que o acesso for previamente programado, deverá ser informado à Diretoria ou pela gestão de TI da instituição por e-mail, com descrição da atividade a ser realizada.

Se o acesso for emergencial, a atividade deverá ser registrada posteriormente em e-mail enviado à Diretoria ou pela gestão de TI da instituição.

Nos próximos anos, a tendência é desativar todo o ambiente físico, ficando apenas com o legado, sendo todos os arquivos da instituição migrados e armazenados em nuvem do Cenpec (Google Drive).

O acesso ao ambiente administrativo dos projetos para colaboradoras(es) e consultoras(es) deverá ser definido em matriz de acesso pela liderança da área/projetos e liberado pela CTD apenas durante o período pela necessidade de utilização e deverá ser bloqueado assim que não tiver mais finalidade.

## 18. REGISTRO DOS LOGS

Os servidores físicos da instituição deverão manter o log dos servidores na pasta de evidências.

Para o ambiente de nuvem da instituição (Google Drive), deverão manter o log de acesso às pastas.

A gestão da TI recomenda também que o controle de acessos da área autenticada de ambientes dos projetos possua registro (logs) dos acessos e das ações realizadas (ex.: editar, atualizar e excluir dados pessoais) de forma que seja possível rastrear as(os) responsáveis (e-mail ou CPF) pelas ações, resultado das ações (antes e depois), data/hora, com respectivo IP de origem.

## 19. USO DO CORREIO ELETRÔNICO (E-MAIL)

**O correio eletrônico fornecido pela instituição é um instrumento de comunicação interna e externa para a realização do negócio da instituição. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da instituição, não podem ser contrárias à legislação vigente e nem aos princípios éticos da instituição.**

**O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço, sendo proibida a utilização compartilhada de senhas de acesso.**

É terminantemente proibido o envio de mensagens que:

- contenham declarações difamatórias e linguagem ofensiva;
- possam trazer prejuízos a outras pessoas;
- sejam hostis ou inadequadas;
- sejam relativas a “correntes e pirâmides”, de conteúdos pornográficos ou equivalentes;
- possam prejudicar a imagem da instituição;
- possam prejudicar a imagem de outras instituições ou indivíduos;
- sejam incoerentes com as políticas da instituição;
- contenham conteúdo ilegal.

Para incluir uma(um) nova(o) usuária(o) no correio eletrônico, o RH deverá fazer um pedido formal à TI, que providenciará a inclusão desta(e) e dos recursos necessários. A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado. Em caso de congestionamento no Sistema de correio eletrônico, a TI fará auditorias no servidor de correio

e/ou nas estações de trabalho das(os) usuárias(os), visando identificar o motivo que ocasionou o problema.

As mensagens classificadas como “Interno, Confidencial ou Restrito” deverão conter uma clara identificação dessa classificação.

As(Os) usuárias(os) devem organizar as mensagens enviadas e recebidas em pastas apropriadas no seu cliente de correio.

O sistema de correio da instituição obrigatoriamente processará todas as mensagens através de filtros AntiSpam e antivírus.

Com a finalidade de evitar Spam, não disparar mensagem via e-mail institucional para grupos maiores que 100 pessoas. Para disparos em massa, deve ser utilizada a ferramenta de disparo de mailing do Cenpec, com gestão e acompanhamento da CTD.

Por fim, todos os dados pessoais e/ou documentos que contiverem dados pessoais devem conter a confidencialidade como padrão (modo confidencial do Google). Após o encerramento da troca de e-mails com dados pessoais, quando a troca de e-mails estiver finalizada, o colaborador deve armazenar os documentos, dados pessoais e até mesmo as cópias dos e-mails diretamente na nuvem do Cenpec (Google Drive). Isso evitará o armazenamento inseguro das informações no sistema de e-mails, acessos indevidos por pessoas não autorizadas e a perda de informações no caso de desligamento do colaborador.

Após o salvamento das informações no sistema, deve-se aguardar um período de até 30 (trinta) dias e realizar a exclusão dos dados pessoais e documentos armazenados no sistema do e-mail.

## 20. USO DE MÍDIAS SOCIAIS (ferramentas de mensagem instantânea, redes sociais etc.)

**As mídias sociais com finalidade institucional não devem ser utilizadas para compartilhamento de dados pessoais e/ou confidenciais/restritos.**

As trocas de mensagens instantâneas referentes às ações do Cenpec devem ser realizadas via ferramentas (chat e espaços) do Google Cenpec. Caso a área ou projeto precise utilizar outros aplicativos de mensagem instantânea como o WhatsApp, não deve compartilhar dados confidenciais por meio dessa ferramenta e deve seguir as orientações de uso seguro das ferramentas de mensagem instantânea, consultar o Guia de Ferramentas de Comunicação Instantânea.

## 21. NECESSIDADE DE NOVOS SISTEMAS, APLICATIVOS E EQUIPAMENTOS

A TI é responsável pela aplicação da Política da instituição em relação à definição de compra e substituição de “software” e “hardware”. Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardware) deverá ser discutida com o responsável pela TI. Não é permitida a compra ou o desenvolvimento de "softwares" ou "hardwares" diretamente pelos usuários.

Após a análise pela TI e tomada de decisão positiva pela compra, o responsável pelo TI deverá contatar o(a) DPO e Comitê LGPD para avaliação de questões de proteção de dados e privacidade da ferramenta. Com o aval do(a) DPO, o Cenpec poderá proceder com a aquisição da ferramenta.

Todo novo equipamento ou software adquirido pela instituição deverá ser cadastrado no sistema de controle de ativos, antes de sua ativação para uso pela pessoa ou departamento interessado.

Os novos servidores deverão seguir as Normas de Configuração de Servidores.

No caso de assinatura e uso de ferramentas digitais e serviços on-line para uso específico dos projetos, o administrativo deve controlar e informar à TI e à CTD.

## 22. MODIFICAÇÕES DE EQUIPAMENTO E SISTEMAS

Alterações de sistemas ou substituição de equipamentos deverão ser executados dentro de um projeto que envolva etapas de planejamento, testes preliminares, implantação, testes e documentação (de programas e dados), registrando-se as alterações no sistema de controle de ativos.

Em especial, a equipe de TI deverá confirmar os aspectos de segurança do novo ambiente, mediante a checagem da conformidade às normas de instalação de servidores e mediante testes (como *scans* de segurança).

## 23. DESCARTE DE EQUIPAMENTOS, MÍDIAS E DOCUMENTOS

As mídias fora de uso, pifadas ou danificadas deverão ser tratadas da seguinte maneira:

- Discos rígidos (HDs) e discos sólidos (SSDs ou *flash*): Se os dispositivos ainda permitirem acesso, deverão ser utilizadas ferramentas de software de apagamento total de dados, não apenas formatação simples. Em seguida, esses discos deverão ser entregues ao administrador de TI, para identificação. Caso seja necessário enviar tais dispositivos para manutenção ou descarte definitivo, o conteúdo deverá ser destruído pelos meios técnicos apropriados (como desmagnetização de HDs ou destruição física de SSDs).
- Dispositivos de armazenamento móvel como *pen drives*, memórias SD, CF e equivalentes: mesmo procedimento acima.
- Mídias descartáveis (como disquetes, CDs e DVDs): essas mídias devem ser destruídas no picotador próprio da instituição.
- Documentos físicos:

**(i)** Para **documentos com dados de alto risco**, seja porque constam dados considerados sensíveis, confidenciais, sigilosos ou por seu teor trazer riscos ao **Cenpec**, recomenda-se a utilização de caneta/carimbo selador de dados confidenciais, ideal para esconder/omitir informações dificultando ou tornando impossível a identificação dos dados.

**(ii)** **Utilização de fragmentadoras de papel particulada**, devendo-se priorizar os equipamentos que permitem deixar o papel mais triturado, pois quanto menores os pedaços, mais difícil a recuperação e associação das informações neles constantes.

**(iii)** **Após a trituração do documento**, caso exista um alto volume de documentos físicos, deve-se prezar pela separação do material triturado em recipientes diferentes (como sacos de lixo difusos), misturando os conteúdos para dificultar a associação dos papéis e identificação das informações.

**(iv)** Outra conduta que pode ser incluída nesse processo é o **descarte progressivo dos recipientes em datas diversas**.

**(v)** Para os **documentos classificados com alto grau de confidencialidade e sigilo, ou seja, que têm alto risco de impacto negativo ao Cenpec no caso de vazamento de informações,** recomenda-se a incineração das informações.

No momento do descarte final, os equipamentos devem passar pelos seguintes procedimentos:

- Retirada de partes e peças que possam ser aproveitadas (como placas de rede, placas de vídeo, HDs, monitores, teclados e demais itens).
- Caso ainda seja funcional, o equipamento deverá sofrer a retirada de informações contidas em HDs, chips de memória, dispositivos de armazenamento (ou tais componentes devem ser apagados, destruídos ou inutilizados).
- Deve ser providenciada a retirada por instituição especializada em descarte ou reaproveitamento ecológico ou social.

## 24. USO DE COMPUTADORES e EQUIPAMENTOS MÓVEIS DO CENPEC

As(Os) usuárias(os) que tiverem direito ao uso de computadores pessoais (*notebooks*, *tablets*, celulares e semelhantes), ou qualquer outro equipamento computacional ou de telecomunicações, de propriedade do Cenpec, devem estar cientes das condições de uso e assinar o "Termo de Responsabilidade pela guarda e uso de aparelho tecnológico".

**No contexto do trabalho remoto (home office), as colaboradoras(es) devem sempre utilizar os computadores fornecidos pela instituição para realização do seu trabalho.**

A(O) usuária(o) não deve alterar a configuração do equipamento recebido, podendo existir exceções a serem aprovadas pela gestão da TI.

Os computadores da instituição utilizam o bitlocker da Microsoft para criptografia do HD.

Alguns cuidados que devem ser observados:

Fora do trabalho:

- Mantenha o equipamento sempre com você.
- Atenção em hall de hotéis, aeroportos, aviões, táxi etc.
- Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível.
- Atenção ao transportar o equipamento na rua.

Em caso de perda, roubo ou furto:

- Registre a ocorrência em uma delegacia de polícia.
- Comunique imediatamente ao seu superior imediato, o RH, a TI e a(o) DPO.
- Envie uma cópia da ocorrência para o RH/TI.

## 25. USO DE COMPUTADORES OU EQUIPAMENTOS MÓVEIS, DISPOSITIVOS E ACESSÓRIOS PESSOAIS

Somente poderá ser utilizado equipamento de propriedade de colaboradores e parceiros para trabalhos da instituição mediante autorização prévia da Diretoria e cadastramento prévio na TI.

As(Os) usuárias(os) que tiverem direito ao uso de computadores pessoais de sua propriedade (notebooks, *tablets*, celulares, *pen drives*, dispositivos de armazenamento e semelhantes), ou qualquer outro equipamento computacional ou de telecomunicações, devem estar cientes de que:

- Os recursos de tecnologia da informação têm como objetivo a realização de atividades profissionais.
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.
- Todas as normas de segurança contidas neste documento deverão ser observadas.
- As informações classificadas como “Interno, Confidencial ou Restrito” não poderão ser copiadas para esses equipamentos e dispositivos de propriedade pessoal do funcionário ou parceiro.
- Toda e qualquer manutenção nestes equipamentos particulares não será feita pela gestão de TI.

## 26. USO DE SISTEMAS E RECURSOS COMPUTACIONAIS EXTERNOS

A contratação de prestadores externos como provedores de hospedagem, datacenters, provedores de links e *backbones* só poderá ser feita após checagem das certificações de segurança desses prestadores, e o termo de confidencialidade e privacidade dos serviços.

As(Os) colaboradora(os) deverão estar atentos às condições dos prestadores por ocasião de visitas e instalações, bem como a eventuais problemas de segurança.

## 27. RESPONSABILIDADE DAS(OS) DIRETORAS(ES)/GERENTES/COORDENADORAS(ES)

As(Os) diretoras(es), gerentes e coordenadoras(es) são responsáveis pelas definições dos direitos de acesso de suas(seus) colaboradoras(es) aos sistemas e às informações da instituição, cabendo àquelas(es) profissionais verificarem se estas(es) estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, orientando a equipe a manter cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política. Serão responsáveis também em manter sempre atualizada a Matriz de acesso, documento que define os direitos de acesso dos funcionários aos sistemas e informações da instituição.

A TI fará auditorias periódicas do acesso dos usuários às informações, verificando:

- que tipo de informação o usuário pode acessar;
- quem está autorizado a acessar determinada rotina e/ou informação;
- quem acessou determinada rotina e informação;
- quem deu à(ao) usuária(o) permissão de acesso a determinada rotina ou informação;
- que informação ou rotina determinada(o) usuária(o) acessou;
- quem tentou acessar qualquer rotina ou informação sem estar autorizada(o).

## 28. SISTEMAS DE TELECOMUNICAÇÕES

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da instituição, assim como o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade da TI, de acordo com as definições da Diretoria da instituição. Para controle, poderão ser enviados relatórios gerados pelo serviço voip Net2phone Brasil informando a cada gerência quanto foi gasto por ramal.

## 29. USO DE ANTIVÍRUS

Todo arquivo em mídia proveniente de unidade externa deverá ser verificado por programa antivírus. Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus. Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pela TI, via rede. A(O) usuária(o) não pode, em nenhuma hipótese, desabilitar o programa antivírus instalado nas estações de trabalho.

## 30. SOLICITAÇÃO DE ATENDIMENTO TÉCNICO

As solicitações de atendimento técnico deverão ser registradas no sistema de atendimento, por telefone ou e-mail.

As solicitações técnicas serão classificadas de acordo com nível de criticidade e ordem de abertura, com exceção de usuários ou atividades prioritárias.

**Canais de comunicação**
Portal do cliente da Blocktime
Telefone: 11 3087-3400 nos dias úteis, de segundas às sextas-feiras das 8h às 18h.
WhatsApp: 11 3087-3400 nos dias úteis, de segundas às sextas-feiras das 8h às 18h.
SLA (tempo de resposta acordado) de até 4 horas úteis para atendimento e/ou encaminhamento de uma solução.

## 31. PENALIDADES

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.