

**TIPO DE NORMATIVO:
TECNOLÓGICA**

POLÍTICA DE USO DA INFRAESTRUTURA

**CONFEDERAÇÃO
BRASILEIRA DO DESPORTO
ESCOLAR – CBDE**



ÁREA:
Tecnologia da
Informação (TI)

CÓDIGO:
POL-003

GERÊNCIA:
Administrativa

VERSÃO:
V04

PÚBLICO:
(x) Interno () Externo

**DATA DE
PUBLICAÇÃO:**
01/06/2021

POLÍTICA DE USO DA INFRAESTRUTURA TECNOLÓGICA

SINOPSE

A política descrita nesse documento aplica-se a conduta dos funcionários e demais colaboradores na utilização da infraestrutura de tecnologia da Confederação Brasileira do Desporto Escolar (CBDE), especialmente, mas não exclusivamente, relativas a: propriedade intelectual, confidencialidade, divulgação de informações da empresa, padrões de conduta, mau uso dos recursos da empresa, antiassédio, e informações e segurança de dados.

ÍNDICE

SINOPSE	2
ÍNDICE	2
CONTROLE DE REVISÕES	3
1. OBJETIVO	4
2. ABRANGÊNCIA	4
3. TERMOS E DEFINIÇÕES	4
4. RESPONSABILIDADES	5
5. DIRETRIZES	6
6. CONSIDERAÇÕES FINAIS	10
7. VIGÊNCIA	10
8. LEGISLAÇÃO RELACIONADA	Erro! Indicador não definido.
9 ANEXOS	10

CONTROLE DE REVISÕES

Versão	Descrição sucinta das alterações:	Etapa	Nome /Cargo:	Data de Aprovação:
V04	Aprovação	Aprovação	Conselho de Administração	01/06/2021
V04	Emissão de Parecer	Análise Jurídica	Karina Rodrigues/Jurídico	27/05/2021
V04	Alteração/revisão/atualização e/ou inclusão de texto aos itens: 3. Conceitos; 4. Referências; 5. Responsabilidade; 7. Diretrizes; 8. Responsabilidades da equipe de TI; 12. Aprovação	Revisão	Anne Affiune/Coordenadora de Governança e Processos	29/04/2021
V03	Aprovação da alteração	Aprovação	Luiz Carlos Delphino/Diretor Geral (CEO)	25/09/2020
V03	Revisão do documento: incluída a previsão de entrega de cópia desse documento e assinatura no Termo de Recebimento e Anuência da Política de Uso de Infraestrutura Tecnológica, pelos funcionários	Revisão	Anne Affiune/Coordenadora de Governança e Processos	24/09/2020
V02	Revisão de texto	Revisão	Anne Affiune/Coordenadora de Governança e Processos	05/02/2020
V0	Criação do documento	Elaboração	Helbert Costa/Consultor	17/06/2019

1. OBJETIVO

Estabelecer as diretrizes gerais, as atribuições e os princípios básicos a serem observados quanto a utilização da infraestrutura de tecnologia da CBDE.

2. ABRANGÊNCIA

As diretrizes desta política devem ser aplicadas a todos os colaboradores da CBDE.

3. CONCEITOS

Área de TI/CBDE: Departamento/Setor da CBDE responsável pelas atividades de planejamento, monitoramento e suporte das atividades de tecnologia da informação e de segurança da informação da CBDE.

Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física ou por um determinado sistema;

Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física ou sistema não autorizado ou credenciado;

Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema;

Firewall institucional: conjunto de equipamentos e tecnologias que visam implementar e monitorar a política de comunicação da rede de dados da CBDE com a Internet.

Incidente de Segurança: violação de requisito de segurança estabelecido pela área de TI ou violação de legislação ou norma vigente.

Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

Recursos de Tecnologia da Informação: consideram-se recursos de tecnologia da informação o conjunto formado pelos bens e serviços de TI que constituem a infraestrutura tecnológica de suporte automatizado ao ciclo da informação, que envolve as atividades de produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação. Exemplos de recursos de TI são computadores desktops, terminais de acesso, servidores, equipamentos de rede como comutadores (switches) e roteadores, equipamentos de suporte com acesso a rede como nobreaks e geradores, equipamentos de comunicação como telefones, e todos os softwares, aplicações e informações que estejam armazenados em quaisquer destes dispositivos, entre outros.

Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

Sítio ou Aplicação Web: Documento, aplicação ou sistema de informação hospedado em recurso de TI, acessível através da rede de dados, identificado por uma URL. O sítio eletrônico da CBDE é acesso pelo endereço: www.cbde.org.br.

TI: Tecnologia da Informação

Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

Usuário: São os usuários internos, externos, colaboradores da CBDE que utilizam os recursos de TI no desempenho de suas funções.

4. REFERÊNCIAS

- Lei nº: 12.965/2014;
- Lei nº 13.709/2018;
- Estatuto Social;
- Planejamento Estratégico;
- Código de Conduta Ética;
- POL14 Política de Gestão de Pessoas;
- PO19 Manual de Procedimentos de Organização e Gestão de Documentos Digitais;
- PO23 Manual para Procedimentos de Assinatura Eletrônica.

5. RESPONSABILIDADES

Área ou Cargo	Responsável por:
Colaborador	Cumprir com as normas vigente nesta política
Gestores imediatos (Coordenadores, Gerentes e Diretorias)	Assegurar que a diretrizes desta política estão sendo cumpridas

6. PRINCÍPIOS

A concepção, desenvolvimento e operação dos recursos de TI da CBDE deverão atender aos seguintes princípios:

- **Vedação ao anonimato:** os recursos de TI da CBDE não podem ser utilizados de forma anônima, sendo responsabilidade área de TI da entidade a instalação de controles que garantam a identificação dos usuários de cada recurso.
- **Privacidade:** os recursos de TI e suas configurações de uso sempre respeitarão a privacidade dos usuários, salvo os casos previstos nesta **POL 03 - Política de Uso da Infraestrutura Tecnológica** e necessários à segurança da informação da CBDE.
- **Segurança:** os recursos ou serviços de TI somente poderão ser disponibilizados caso atendam à legislação em vigor, aos procedimentos de segurança da informação da CBDE, e à esta **POL 03 - Política de Uso da Infraestrutura**, sem colocar em risco o patrimônio material e intelectual da CBDE.

- Investimento em recursos compartilhados: sempre que possível, os investimentos em TI devem ser feitos de forma a atender o maior número de usuários possível, dando prioridade para infraestruturas compartilhadas.

7. DIRETRIZES

A política descrita nesse documento aplica-se a conduta dos funcionários e colaboradores na utilização da infraestrutura de tecnologia da CBDE, especialmente, mas não exclusivamente, relativas a: propriedade intelectual, confidencialidade, divulgação de informação da empresa, padrões de conduta, mau uso dos recursos da empresa, antiassédio, e informações e segurança de dados.

Ao violar essa política, o funcionário/colaborador pode estar sujeito a medidas disciplinares, até e inclusive a demissão. Além disso, o funcionário poderá responder civil e criminalmente pelos atos que violaram os direitos ou prejudicaram a CBDE e/ou outros indivíduos e empresas.

Todas as redes de dados da CBDE, acessos à Internet a partir de qualquer dispositivo de TI e sistemas e aplicações de software deverão seguir os padrões mínimos operacionais e de segurança definidos pelos procedimentos de segurança da informação da CBDE e por esta **POL 03 - Política de Uso da Infraestrutura Tecnológica**.

Todos os usuários dos recursos de TI da CBDE deverão atender à legislação vigente, às normativas específicas da CBDE, a esta **POL 03 - Política de Uso da Infraestrutura Tecnológica** e aos procedimentos de segurança da informação da CBDE, bem como a quaisquer requisitos de segurança da informação definidos pelos gestores da entidade e pela equipe de TI da CBDE.

Os usuários devem comunicar ao responsável à equipe de TI sempre que houver suspeita de incidente de segurança ou violação de normativos ou legislação em vigor.

As credenciais de acesso (conta e senha) a recursos de TI de uso individual são intransferíveis e não devem ser compartilhadas com terceiros.

Quaisquer privilégios sobre recursos de TI e sistemas de informação que um usuário final receber são intransferíveis, exceto quando previsto.

Os recursos de TI devem ser utilizados de forma a não prejudicar ou interferir nas atividades dos demais usuários ou na operacionalidade dos serviços e infraestrutura de rede.

É dever dos usuários dos recursos de TI o respeito à propriedade intelectual e direitos autorais, sendo considerado violação desta Política o compartilhamento de arquivos de áudio, vídeo ou dados sem a autorização da entidade ou em desconformidade com os termos da licença de uso.

A rede interna da CBDE tem como características prover a comunicação confiável entre os setores da entidade, entre CBDE e stakeholders, melhorar o fluxo e o acesso às informações, resguardar as informações e agilizar a tomada de decisões administrativas facilitando a comunicação entre seus usuários. Dessa forma, todas as informações institucionais deverão ser armazenadas nos servidores de dados da CBDE. Para tanto, todos os funcionários devem desenvolver suas atividades utilizando-se do acesso à rede interna da Entidade.

O acesso interno à rede interna da CBDE é concedido aos funcionários ativos durante a existência do vínculo, solicitada pela área de RH e executada pela área de TI.

Todos os equipamentos conectados à rede interna terão seus acessos monitorados por questões de segurança e para fins de auditoria.

7.1 Declaração de política

O uso da infraestrutura tecnológica da CBDE, incluindo computadores, impressoras, copiadoras, telefone e todas as formas de acesso à Internet/Intranet, é para uso dos negócios da entidade. O uso pessoal breve e ocasional do sistema de correio eletrônico ou da Internet é aceitável, desde que não seja feita de forma excessiva ou inadequada e ocorra durante o tempo pessoal (almoço ou outros intervalos), e não resulte em despesas para a CBDE.

Utilização é definida como "excessiva" se ela interfere com as funções normais de trabalho, a capacidade de resposta do profissional, ou a capacidade de realizar as atividades diárias de trabalho.

A comunicação eletrônica não deve ser usada para solicitar ou vender produtos ou serviços que não estão relacionados aos negócios da CBDE; distrair, intimidar ou assediar colegas de trabalho ou de terceiros; ou interromper o trabalho.

O uso de computadores da CBDE, redes e acesso à Internet é um privilégio concedido pela administração e pode ser revogada a qualquer momento por conduta inadequada realizada em tais sistemas, incluindo, mas não limitados a:

1. O envio de corrente ou participação de alguma forma na criação ou transmissão de correio eletrônico não solicitado ("*spam*");
2. Compartilhar com outra pessoa, funcionário ou não da CBDE, a senha ou usuário de acesso ao qualquer sistema da organização;
3. Engajar-se em atividades de negócios privados ou pessoais;
4. Uso excessivo de salas e aplicativos de mensagens instantâneas, sites de redes sociais;
5. Usar a infraestrutura da CBDE para violar ou tentar violar as leis e regulamentos Brasileiros ou de qualquer outra jurisdição;
6. Engajar-se em atividades maliciosas ou ilícitas;
7. Deliberadamente propagar qualquer vírus, *worm*, cavalo de tróia, código de programa malicioso, ou outro código ou arquivo projetado para interromper, desativar, prejudicar redes ou sistemas da CBDE ou de qualquer outro indivíduo ou entidade;
8. Criar, visualizar, transmitir ou receber matérias com uma ou mais das seguintes características: abusivo, profano, ameaçador, racista, sexista ou censurável;
9. Enviar, receber ou acessar material pornográfico;
10. Se envolver na política partidária;

11. Causar congestionamento, interrupção, invalidez, alteração ou deterioração de redes ou sistemas da CBDE;
12. Deixar de fazer *logoff* em qualquer computador ou sistema de acesso controlado que solicite autenticação com usuário e senha;
13. Violar ou tentar violar restrições de segurança em sistemas e aplicações da CBDE;
14. Navegar em sites pertencentes às categorias abaixo, ou fazer armazenamento, a distribuição, a edição, a gravação usando estrutura da CBDE:
 - Material sexualmente explícito e ainda material contrário a moral ou aos bons costumes;
 - Material de conteúdo impróprio, ofensivo, preconceituoso ou discriminatório;
 - Apologia à violência ou ao terrorismo;
 - Apologia às drogas;
 - Violação de direito autoral (pirataria).
15. Transferir qualquer tipo de programa, jogo e similares para a rede interna da empresa ou para os computadores sem autorização específica do superior hierárquico;
16. Fazer downloads de arquivos de extensões tipo: exe, .mp3, .wav, .bat, .com, .sys, .scr, , .mpeg, .avi, .rmvb, .dll, e de programas de entretenimento ou jogos, exceto os estritamente relacionados aos serviços inerentes à função do colaborador com vistas às atividades da empresa;
17. Acessar programas de TV na Internet ou qualquer conteúdo sob demanda (*streaming*);
18. Utilizar a computadores ou a rede da CBDE para jogar, jogos eletrônicos, inclusive os da Internet (*onlines*);
19. Revelar, fora do âmbito da CBDE, fato ou informação de qualquer natureza de que tenha tido conhecimento por força de suas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial.

7.2 Tratamento de Incidentes de Segurança

Fica instituído o processo de tratamento de incidentes de segurança da CBDE, com detalhamento definido em procedimento específico aprovado conforme definido na Matriz de Alçadas para aprovação da CBDE. O mesmo, deverá estar alinhado à política de gestão de riscos da entidade e normatizará o processo de trabalho da TI, relativo ao tratamento de incidentes de segurança.

Violações desta **POL 03 - Política de Uso da Infraestrutura Tecnológica**, bem como da legislação vigente, além de outras violações relacionadas à segurança da informação, são incidentes de segurança contemplados pelo processo de tratamento de incidentes definidos pela Entidade.

Cabe à área de TI da CBDE definir o processo de tratamento de incidentes de segurança da CBDE.

7.3 Propriedade e Acesso de Correio Eletrônico, Acesso à Internet, e arquivos de computador

A CBDE detém os direitos de todos os dados e arquivos armazenados em qualquer computador, rede ou sistema de informação utilizados na entidade. A CBDE também se reserva do direito de monitorar as mensagens eletrônicas via *e-mail* institucional e seu conteúdo. Os funcionários devem estar cientes de que as mensagens de correio eletrônico institucional enviadas e recebidas usando equipamentos e dados da CBDE não são privados e estão sujeitas a visualização, download, inspeção e arquivamento por funcionários da CBDE em todos os momentos. A CBDE tem o direito de inspecionar qualquer arquivo armazenado em áreas da rede ou em computadores ou mídia de armazenamento, a fim de garantir a conformidade com políticas e leis estaduais e federais.

A CBDE licenciou o uso de certos programas, aplicativos e software comerciais. Nenhum funcionário pode criar, usar ou distribuir cópias de tal software para as máquinas pessoais ou de terceiros.

7.4 Confidencialidade do correio eletrônico

Como observado acima, o correio eletrônico é usado em todos os momentos para monitoramento e divulgação de informação específica e está sujeita às leis estaduais e federais aplicáveis e normas da CBDE.

É considerada uma violação da política da empresa qualquer funcionário ou colaborador, incluindo os administradores de sistema, acessar arquivos de correio e sistemas de computadores eletrônicos para satisfazer a curiosidade sobre os assuntos dos outros.

NOTA: Os colaboradores da CBDE devem evitar utilizar o seu endereço com domínio “cbde.org.br” para comunicações de caráter pessoal.

7.5 Alteração de conteúdo de e-mail

Mensagens de correio eletrônico recebidas não devem ser alteradas e/ou encaminhadas para outro usuário sem autorização do remetente.

7.5.1 Declaração de Política para o navegador Internet/Intranet (s):

A Internet é para ser usada para promover a missão da CBDE e apoiar outros fins relacionados aos trabalhos diretos.

Os funcionários são individualmente responsáveis por todos e quaisquer danos sofridos como resultado de violar a política de segurança da Entidade, direitos autorais e acordos de licenciamento.

7.6 Equipamento eletrônico pessoal

A CBDE proíbe o uso ou posse no local de trabalho de qualquer dispositivo de armazenamento removível, sem a permissão expressa da entidade. Funcionários com esses dispositivos devem informar aos seus superiores, a fim de obter autorização expressa para esse uso (a autorização pode ser dada por e-mail, copiada à área de TI da CBDE).

Os funcionários não devem trazer computadores pessoais para o local de trabalho ou conectá-los aos sistemas eletrônicos da empresa a menos que expressamente autorizado. Qualquer funcionário ao trazer

um dispositivo de computação pessoal ou dispositivo de gravação de imagem estará automaticamente dando permissão para a CBDE inspecionar o conteúdo de tais dispositivos a qualquer momento.

8 SÃO RESPONSABILIDADES DA ÁREA DE TI

São atribuições inerentes à área de TI da CBDE, inclusive, mas não somente:

1. Planejar, executar e monitorar o uso de instalação e configuração de software e serviços de TI da CBDE;
2. Planejar, executar e monitorar as atividades relativas à infraestrutura física e de rede da CBDE;
3. Planejar, executar e monitorar incidentes de segurança da informação e prevenção dos mesmos;
4. Suporte à rede e dispositivos de rede da CBDE, configuração e manutenção de servidores, computadores e outros dispositivos de TI da CBDE;
5. Suporte à configuração, instalação e uso dos sistemas e softwares em operação na CBDE;
6. Orientar os usuários quanto aos procedimentos de segurança da informação da CBDE e a esta **POL 03 - Política de Uso da Infraestrutura Tecnológica**;
7. Orientar os usuários quanto ao uso da infraestrutura de TI da CBDE;
8. Gerenciar os usuários, as políticas de segurança e de acesso a recursos da rede.

9 CONSIDERAÇÕES FINAIS

1. Todos os funcionários, no ato da admissão, deverão receber cópia desta política e assinar o **Termo de Recebimento e Anuência da Política de Uso de Infraestrutura Tecnológica**.
2. A violação desta política pode levar a medidas disciplinares, até e inclusive a demissão.
3. Os funcionários que não desejarem que tais inspeções sejam feitas em seus dispositivos não devem conectá-los à rede, a internet, aos computadores ou quaisquer outros dispositivos da CBDE.

10 VIGÊNCIA

Esta política permanecerá em vigor por dois anos a contar da data de sua publicação.

11 ANEXOS

- N/D

12 APROVAÇÃO

Esta política foi aprovada pelo Conselho de Administração, em 01/06/2021, conforme registro em ata. Devendo ser assinada pelo Diretor Geral (CEO), utilizando assinatura digital.

Assinado por Luiz Carlos Delphino de Azevedo Junior

Luiz Delphino
Diretor Geral

POL.03 Política Uso da Infraestrutura Tecnológica V.04 APROVADA PELO CA EM 01 06 2021.pdf

Hash do Documento Original: (SHA1) 85481855b05d508fde1320b2db3044173d74818d
SID: 179CcAc292B-17CcBFfb52b-1A6bd6B012B-1add74fdD2B-1Dc4A4BA92B



Datas e horários baseados em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON)
Certificado de assinaturas gerado em 2 de junho de 2021



Assinaturas - Manuscrito Digital



Luiz Carlos Delphino de Azevedo Junior
luiz@cbde.org.br
Assinado em: 2021/06/02 13:54:31
Assinou como: parte

Assinado por Luiz Carlos Delphino de Azevedo Junior

