RESOLUÇÃO DO CONSELHO DE ADMINISTRAÇÃO DO CEBRASPE
N.º 000005/2025

Aprova a Política de Segurança da Informação (PSI) do Cebraspe.

O **CONSELHO DE ADMINISTRAÇÃO DO CENTRO BRASILEIRO DE PESQUISA EM AVALIAÇÃO E SELEÇÃO E DE PROMOÇÃO DE EVENTOS (CEBRASPE)**, no uso de suas atribuições estatutárias e regimentais, em sua 92.ª Reunião, Ordinária e Presencial, realizada em 13 de agosto de 2025,

RESOLVE:

Aprovar, por unanimidade, a **Política de Segurança da Informação (PSI) do Cebraspe**, proposta pela Diretoria-Geral, conforme apresentada nesta reunião, que passa a fazer parte desta resolução.

Brasília, 13 de agosto de 2025.

Carmenísia Jacobina Aires
Presidente do Conselho de Administração

Política de
Segurança da Informação

Controle de Versão

- **Versão do Documento:**
- **Data de Aprovação:**
- **Data da Próxima Revisão:**
- **Status:**

---

1. Apresentação

A informação é um dos ativos mais valiosos do Cebraspe. Ela sustenta a credibilidade da instituição, influencia decisões estratégicas e garante o correto funcionamento dos processos internos e externos. Esta Política de Segurança da Informação (PSI) estabelece as diretrizes para proteger esses ativos contra acessos não autorizados, alterações indevidas, destruição acidental, vazamentos e indisponibilidades.

2. Objetivo

A PSI tem como objetivo principal garantir a proteção da informação contra ameaças internas e externas, deliberadas ou acidentais. Busca assegurar os pilares da segurança: Confidencialidade (restrição de acesso), Integridade (precisão e confiabilidade dos dados) e Disponibilidade (acesso garantido a quem de direito). A política ainda promove conformidade com a legislação vigente, como a LGPD (Lei Geral de Proteção de Dados), além de normas técnicas como a ISO/IEC 27001.

3. Âmbito de Aplicação

Aplica-se a todos os usuários (empregados, prestadores de serviço, consultores, estagiários, parceiros e qualquer pessoa) com acesso a sistemas, redes, dados ou informações da instituição. Inclui também fornecedores terceirizados e usuários externos que interagem com os sistemas institucionais.

4. Princípios Fundamentais

- **Confidencialidade:** Assegura que informações sensíveis não sejam acessadas por pessoas não autorizadas.
- **Integridade:** Garante que a informação se mantenha completa e precisa, sem alterações indevidas.
- **Disponibilidade:** A informação deve estar acessível sempre que necessária, garantindo continuidade operacional.
- **Legalidade:** Observância à legislação aplicável, especialmente LGPD e normas específicas.
- **Responsabilidade:** Cada usuário é corresponsável pela proteção da informação que manipula ou acessa.

5. Estrutura de Governança

Define os agentes responsáveis por zelar pela segurança da informação:

- **Comitê de Segurança da Informação (CSI):** Órgão estratégico e consultivo responsável por supervisionar a PSI, propor melhorias e deliberar em situações críticas.
- **Coordenação de Tecnologia da Informação e Comunicação (CTIC):** Executa os controles técnicos.

- **Gestores:** Responsáveis por disseminar a política em suas unidades e garantir que as práticas sejam seguidas.
- **Usuários:** Devem adotar comportamentos éticos e seguros, conforme diretrizes da PSI.

6. Classificação da Informação

Para definir os cuidados necessários, conforme deliberação do CSI, as informações são divididas em:

- **Pública:** Pode ser divulgada livremente.
- **Restrita:** Acesso limitado a determinados grupos de trabalho.
- **Pessoal:** Dados relativos a indivíduos identificáveis.
- **Sigilosa:** Informações críticas cuja divulgação pode causar prejuízos institucionais.

6.1. Requisitos Mínimos de Manuseio

- **Informação Pública:** Pode ser compartilhada sem restrições.
- **Informação Restrita:** Deve ser armazenada em repositórios institucionais autorizados e seu compartilhamento externo deve ser justificado e aprovado pelo gestor da área.
- **Informação Pessoal e Sigilosa:** Exige os mais altos níveis de controle. Deve ser armazenada em ambientes com criptografia, acessada apenas por pessoal autorizado e seu compartilhamento é proibido, a menos que haja base legal ou consentimento explícito, seguindo os procedimentos definidos pela CTIC e pelo Encarregado de Proteção de Dados (DPO).
- O uso de DLP (Data Loss Prevention) poderá ser adotado para prevenção de vazamento de dados.

7. Segurança Física

Prevê controles para proteção contra acesso físico não autorizado:

- Portar crachá visível.
- Controle de acesso a todas as áreas.
- Visitantes devem ser registrados e acompanhados.
- Dispositivos e mídias sensíveis devem ser armazenados em locais seguros.

8. Acesso e Identidade

Estabelece regras para criação, modificação e revogação de acessos:

8.1. Concessão de Acesso

- Todo acesso a sistemas e informações deve ser formalmente solicitado pelo gestor direto do usuário, através dos canais designados pela CTIC.
- A solicitação deve justificar a necessidade do acesso com base na função profissional do usuário.
- A concessão de acesso deve seguir o Princípio do Menor Privilégio, outorgando apenas as permissões estritamente necessárias para a execução das atividades do cargo.
- Contas de usuário são pessoais e intransferíveis. A criação de contas genéricas é proibida, exceto em casos excepcionais e documentados, com aprovação do Comitê de Segurança da Informação (CSI).

8.2. Revisão de Acesso

- Os gestores de cada área são responsáveis por revisar os acessos de suas equipes em um intervalo máximo de **um ano**.
- A Área de TIC fornecerá relatórios para apoiar o processo de revisão, quando solicitado.
- Acessos que não são mais necessários devem ser imediatamente comunicados à CTIC para revogação.

8.3. Alteração de Acesso

- Em caso de mudança de função, cargo ou unidade de um empregado, seu gestor deve solicitar a revisão completa de seus acessos para adequá-los à nova realidade funcional.

8.4. Revogação de Acesso

- É de responsabilidade da CTIC a revogação dos acessos dos usuários.
- O acesso de um usuário deve ser imediatamente revogado em caso de desligamento, término de contrato ou término de projeto.
- O acesso de um usuário deve ser temporariamente revogado em caso de férias ou afastamento médico.
- É responsabilidade do gestor direto e da área de Gestão de Pessoas (COGEP) comunicar o desligamento ou o afastamento temporário à CTIC com a máxima antecedência possível para garantir a revogação tempestiva.

8.5 Gestão de Senhas

8.5.1. Complexidade

- As senhas devem ter um comprimento mínimo de 8 caracteres.
- Devem conter uma combinação de letras maiúsculas, letras minúsculas, números e caracteres especiais.
- É proibido o uso de informações pessoais óbvias (nome, data de nascimento), nomes da empresa ou palavras comuns e sequências de teclado (ex: "123456", "qwerty", "senha123").

8.5.2. Troca e Expiração

- Há obrigatoriedade de troca periódica forçada de senhas, a cada 90 dias.
- O usuário deverá alterar sua senha imediatamente caso suspeite ou seja notificado de um comprometimento de sua conta.
- As senhas iniciais ou redefinidas pela CTIC devem ser obrigatoriamente alteradas pelo usuário no primeiro acesso.

8.5.3. Armazenamento e Proteção

- É expressamente proibido compartilhar a senha com qualquer outra pessoa, incluindo colegas de equipe ou a equipe de suporte da CTIC.
- É proibido anotar senhas em locais visíveis (ex: post-its, agendas abertas). Se for necessário anotar, deve ser em local seguro e de acesso restrito.
- A reutilização de senhas entre sistemas críticos do Cebraspe e serviços externos (redes sociais, e-mails pessoais) é proibida.

8.5.4. Bloqueio de Conta

- A conta de usuário será bloqueada automaticamente após **3 (três) tentativas de acesso** malsucedidas. O desbloqueio deverá ser solicitado à CTIC.

8.6. Autenticação Multifator (MFA)

8.6.1. Obrigatoriedade

O uso de MFA é **mandatório** para:

- Todo e qualquer tipo de acesso remoto à rede interna do Cebraspe (ex: VPN).
- Todo e qualquer sistema que o recurso de MFA esteja disponível.
- Contas com privilégios administrativos ou de serviço em qualquer sistema.

8.7. Gerenciamento de Contas Privilegiadas

- Contas com privilégios de administrador (ex: administrator, root, contas de domínio) devem ser utilizadas apenas para tarefas que exijam tais privilégios. Para atividades rotineiras, deve-se usar uma conta de usuário padrão.
- O uso de contas privilegiadas deve ser registrado (log) e monitorado continuamente pela CTIC.
- O compartilhamento de credenciais de contas privilegiadas é estritamente proibido.

8.8. Responsabilidades

- **Usuários:** Zelar pela confidencialidade de suas credenciais; reportar imediatamente qualquer incidente ou suspeita de comprometimento.
- **Gestores:** Solicitar, revisar, justificar e aprovar os acessos de sua equipe; comunicar desligamentos e transferências.
- **Área de TIC:** Implementar e administrar os controles descritos nesta norma; automatizar o provisionamento e a revogação de acessos sempre que possível; monitorar o cumprimento das regras.
- **Comitê de Segurança da Informação (CSI):** Revisar e aprovar esta norma e suas futuras atualizações.
- É responsabilidade da **Coordenação de Tecnologia da Informação e Comunicação (CTIC)** cumprir, fazer cumprir e manter atualizados as normas e procedimentos de segurança, revisando continuamente os riscos e controles.
- É também responsabilidade da **CTIC** desenvolver e manter um plano de investimento contínuo, com identificação de necessidades de softwares, equipamentos informáticos e soluções de segurança, a fim de preservar a integridade, disponibilidade e confidencialidade das informações do Cebraspe.
- Cabe à **alta direção** assegurar os recursos necessários para a aquisição e manutenção contínua de softwares, equipamentos e soluções de segurança da informação e tecnologia, a fim de garantir a efetiva aplicação desta Política.

9. Segurança de Redes e Sistemas

Protege a infraestrutura tecnológica:

- Acesso remoto somente via VPN corporativa ou outra tecnologia segura aprovada pela CTIC.
- Monitoramento por meio de sistemas automatizados deve ser contínuo para detectar comportamentos suspeitos.

- Haverá segmentação da rede para limitar impactos de incidentes.
- Aplicação de atualizações e correções de segurança regularmente.

10. Uso da Internet

Regras para o uso responsável e seguro da Internet:

- Proibido acessar conteúdo ilegal, ofensivo ou prejudicial à imagem institucional.
- Não é permitido o uso de programas de compartilhamento de arquivos (P2P), como BitTorrent, uTorrent e eMule, exceto aqueles autorizados pela CTIC, como o WhatsApp, Microsoft Teams e Google Drive (contas coorporativas).
- O tráfego pode ser monitorado para garantir segurança e desempenho.

11. Correio Eletrônico

Estabelece conduta para o uso do e-mail institucional:

- Deve ser utilizado para fins profissionais.
- É proibido enviar mensagens ofensivas, spam, ou utilizar e-mail para fins comerciais, exceto quando utilizando contas corporativas e sistemas autorizados de envio de mensagens de e-mail marketing.
- Mensagens suspeitas devem ser encaminhadas à CTIC.
- O Cebraspe nunca solicita senhas por e-mail.

12. Dispositivos de Acesso

Trata dos equipamentos usados para acessar os sistemas e redes internas da organização:

- Devem estar atualizados, com antivírus ativo e configurações seguras.
- Inclui notebooks, celulares, tablets e dispositivos pessoais autorizados.
- Em caso de perda ou roubo, o fato deve ser reportado imediatamente.

13. Alterações de Configuração

Estabelece que somente a CTIC pode alterar configurações de:

- Equipamentos de rede.
- Servidores e estações de trabalho institucionais.
- Software instalado em máquinas institucionais.

14. Backup e Recuperação

Garante a continuidade dos serviços em caso de falhas ou ataques cibernéticos, contemplados na Política de Backup e Recuperação de dados:

- Backups periódicos devem ser realizados para os sistemas e documentos críticos.
- Devem ser armazenados em ambientes protegidos contra perdas, roubos e desastres.
- Testes de restauração devem ser executados regularmente.

15. Retenção e Descarte Seguro de Dados

- As informações e dados devem ser mantidos pelo tempo necessário para cumprir sua finalidade ou por exigência legal/regulatória.
- Ao final do ciclo de vida, mídias físicas e digitais que contenham informações Restritas, Pessoais ou Sigilosas devem ser descartadas de forma segura e irreversível, utilizando métodos como sanitização de dados ou destruição física, conforme procedimento da CTIC.

16. Instalação de Software

Define que:

- Somente softwares licenciados e homologados podem ser instalados.
- Downloads devem ser realizados somente de fontes confiáveis.

17. Dispositivos Móveis

Cuidados com notebooks, celulares e tablets:

- Devem possuir criptografia, antivírus e, se possível, rastreamento remoto.
- Em caso de perda, roubo ou comprometimento, comunicar imediatamente a CTIC.
- Evitar armazenar informações sensíveis localmente sem proteção adequada.

18. Arquivos e Mensageria

18.1. Armazenamento de Arquivos

- Dados institucionais devem ser armazenados nos servidores de arquivos locais corporativos, controlados pela CTIC (ex: \\arquivos, pastas institucionais).

18.2. Mensageria e Compartilhamento de Arquivos

- O uso de aplicativos como Microsoft Teams é autorizado exclusivamente para fins institucionais.
- Apenas aplicativos homologados pela CTIC podem ser utilizados para comunicação e troca de arquivos.
- O conteúdo transmitido nesses canais está sujeito a monitoramento.
- O Compartilhamento de Arquivos deve ser feito por repositórios com controle de acesso, como o Servidor de Arquivos institucional.
- Informações restritas devem ser protegidas e compartilhadas com permissões adequadas.
- O envio para fora da instituição exige autorização do gestor.

19. Segurança na Cadeia de Suprimentos (Fornecedores)

- Fornecedores e parceiros que manuseiam dados do Cebraspe devem assinar um Acordo de Confidencialidade antes da prospecção.
- Contratos com terceiros devem incluir cláusulas específicas de segurança da informação, privacidade e confidencialidade.
- O acesso de terceiros aos sistemas do Cebraspe deve seguir o princípio do menor privilégio e ser monitorado continuamente.

20. Segurança no Desenvolvimento de Sistemas

- A segurança deve ser integrada em todas as fases do ciclo de vida de desenvolvimento de software (DevSecOps).
- Práticas de codificação segura devem ser seguidas, e os desenvolvedores devem receber treinamento contínuo.
- Sistemas desenvolvidos ou adquiridos devem passar por análise de vulnerabilidade (SAST/DAST) antes de entrarem em produção.

21. Boas Práticas Pessoais

Cada usuário deve:

- Criar senhas fortes, não as compartilhar e seguir esta Política.
- Desconfiar de e-mails e links suspeitos.
- Bloquear a estação de trabalho ao se ausentar.
- Nunca compartilhar dados pessoais de terceiros sem autorização.

22. Tratamento de Incidentes

- Qualquer anomalia ou incidente de segurança da informação deve ser reportado imediatamente à CTIC.
- A equipe de segurança da informação ativará o Plano de Resposta a Incidentes de Segurança da Informação, com medidas corretivas e preventivas.
- Incidentes de devem ser registrados e avaliados para evitar reincidências.

23. Gestão de Riscos

- Os riscos relacionados à segurança da informação devem ser identificados, classificados, tratados e monitorados regularmente, utilizando uma metodologia formal.

24. Auditoria e Conformidade

- Auditorias internas e externas devem avaliar o cumprimento da PSI.
- Conformidade com a LGPD, ISO/IEC 27001 e outras normas devem ser mantidas.
- Não conformidades devem gerar planos de ação corretiva e serem monitoradas até a resolução.

25. Treinamento e Conscientização

- Todos os empregados devem participar de treinamentos sobre segurança da informação.
- Campanhas periódicas de conscientização deverão ser realizadas.
- A cultura de segurança deve ser parte do cotidiano da instituição.

26. Responsabilidade dos Gestores

- Garantir o cumprimento desta política dentro de suas unidades.
- Zelar pela segregação de acessos conforme as funções dos empregados.
- Comunicar imediatamente as contas de usuários desligados ou transferidos.
- Cooperar com a CTIC na apuração de incidentes ou violações de segurança da informação.

27. Sanções

- Violações à PSI podem resultar em advertência, suspensão, desligamento e, conforme o caso, medidas administrativas, cíveis ou penais.
- A natureza da sanção dependerá da gravidade da infração e da responsabilidade envolvida.

28. Disposições Finais

- Esta Política e suas normas devem ser revisadas periodicamente, em intervalo mínimo de um ano, para garantir a melhoria contínua.
- As diretrizes desta Política devem ser amplamente divulgadas pela Coordenação de Gestão de Pessoas (COGEP) e pela Assessoria de Comunicação a todos os empregados, desde o seu ingresso e sempre que houver atualizações.
- O documento deve estar disponível para todos os usuários na Intranet institucional.
- Versões atualizadas devem ser validadas pelo Comitê de Segurança da Informação e homologadas pela alta direção e aprovadas pelo Conselho de Administração.

29. APROVAÇÕES

Adriana Rigon Weska

Diretora-Geral

Claudia Maffini Griboski

Diretora Executiva

xxxxxxxxx

Presidente do Comitê de Segurança da Informação

Vinicius Gomes Duarte

Supervisor de Segurança de TIC

ASSINATURA(S) ELETRÔNICA(S)

A autenticidade do documento pode ser conferida no site:
https://ged.cebraspe.org.br/ValidarDocumentoGedex.aspx
informando o código CRC: 485957766B63427A5773513D / Página 11 de 11

Assinado eletronicamente por: Vinicius Gomes Duarte, Supervisor de Segurança de TIC

Data da Assinatura: 08/08/2025 17:59:02

Assinado eletronicamente por: ADRIANA RIGON WESKA, DIRETOR GERAL
Data da Assinatura: 08/08/2025 18:00:39

ASSINATURA(S) ELETRÔNICA(S)