usuário, de acordo com o estabelecido nesta norma.
Art. 5º São atribuições da Secretaria de Gestão de Pessoas (SEGP):
I - Manter atualizado o Sistema de Gestão de Pessoas, no que concerne aos seguintes eventos:
1. Nomeação de membro e servidor;
2. Exoneração de servidor;
3. Aposentadoria de membro e servidor;
4. Falecimento de membro e servidor;
5. Devolução de servidor cedido de outra instituição;
6. Início e término de Termo de Compromisso de Estágio;
7. Cessão e retorno de servidor efetivo do Tribunal;
8. Licença sem vencimento de servidor;
9. Mudança de lotação de servidor;
10. Mudança de cargo comissionado e/ou função gratificada de servidor;
11. Substituição de cargo comissionado e/ou função gratificada de servidor;
12. Suspensão de servidor em decorrência de processo administrativo.
Art. 6º É atribuição do fiscal do contrato que envolva terceirização de mão de obra comunicar, por meio da Central de Serviços de TI, as situações de afastamento ou mudança de lotação, sempre que o funcionário terceirizado utilizar serviços de TI para o cumprimento de suas atividades.
Art. 7º É atribuição da chefia imediata das unidades do TCE-PA, solicitar a concessão e/ou atualização de permissões de acesso aos sistemas e serviços de TI para usuários sob a sua subordinação, seguindo o princípio do privilégio mínimo.
Art. 8º São responsabilidades dos usuários dos serviços de TI:
I - Manter o sigilo de suas senhas;
II - Realizar o bloqueio da sua estação de trabalho sempre que se ausentar de sua - unidade;
III - Finalizar a sessão de uso dos serviços de TI, sempre que concluir suas atividades;
IV - Realizar as alterações de senhas, de acordo com o estabelecido nessa norma.

CAPÍTULO III
CRIAÇÃO DE CREDENCIAIS E GERENCIAMENTO DO ACESSO

Art. 9º. O acesso aos serviços de TI poderá ser solicitado pela chefia imediata para os usuários lotados em sua unidade, de acordo com a necessidade trabalho, seguindo o princípio do privilégio mínimo.
Art. 10. A solicitação de credenciais de acesso ou ajustes dessas autorizações deverá ser realizada por meio da Central de Serviços de TI, pela chefia imediata, devendo constar, no mínimo, as seguintes informações:
I - Nome completo do usuário;
II - Matrícula;
III - Lotação do usuário;
IV - Serviços e/ou soluções de TI que serão utilizados;
V - Permissões de acesso necessárias.
Parágrafo único. Informações adicionais para a concessão do acesso poderão ser solicitadas de acordo com as necessidades pertinentes a cada solução de TI.
Art. 11. A solicitação de credenciais de acesso também poderá ser realizada por meio de autocadastro, caso o serviço de TI disponibilize tal funcionalidade, cabendo ao responsável pelo serviço o gerenciamento do acesso.
Art. 12. As permissões de acesso aos serviços de TI poderão ser modificadas a qualquer tempo por solicitação da chefia imediata ou do superior hierárquico, de acordo com a necessidade do serviço.
Art. 13. Em caso de mudança de lotação, o servidor terá suas permissões de acesso revogadas, e novas permissões deverão ser solicitadas pela chefia da lotação atual.

CAPÍTULO IV
UTILIZAÇÃO DE CONTAS E SENHAS

Art. 14. O usuário é o único responsável pelo uso de sua credencial de acesso, sendo a conta de uso pessoal e intransferível, devendo obrigatoriamente ser mantida em sigilo pelo mesmo.
Parágrafo único. O compartilhamento, a divulgação e demais violações ao sigilo das senhas implica responsabilidade disciplinar, sem prejuízo das medidas cíveis e criminais cabíveis.
Art. 15. As senhas não devem ser encaminhadas em mensagens de e-mail, chamados da Central de Serviços, aplicativos de mensagens instantâneas, nem anotadas e ou armazenadas em dispositivos móveis, salvo em aplicativo específico para tal funcionalidade que disponham de criptografia forte.
Art. 16. Para o acesso aos serviços de TI do TCE-PA será requisitada identificação da credencial de acesso.
Art. 17. Os acessos bem-sucedidos e as falhas nas tentativas de autenticação poderão ser registrados para fins de auditoria.
Art. 18. Os sistemas e aplicações deverão possuir mecanismos que impeçam a exibição, na tela de acesso, da senha digitada pelo usuário, devendo exibir caracteres tais como asteriscos ou similares.
Art. 19. As estações de trabalho deverão possuir mecanismos para bloquear a sessão do usuário, após 10 (dez) minutos de inatividade.
Art. 20. As soluções de TI deverão possuir mecanismo para encerrar a sessão do usuário após um determinado período de inatividade, de acordo com as especificidades operacionais de cada sistema ou serviço de TI.
Art. 21. As senhas de acesso aos serviços de TI poderão ser alteradas a qualquer tempo pelo próprio usuário, utilizando os mecanismos disponíveis nos sistemas de autenticação.
Art. 22. Caso o usuário suspeite do comprometimento de sua senha, esta deverá ser modificada imediatamente, situação em que o usuário também deverá comunicar imediatamente, por meio da Central de Serviços de TI, para que sejam aplicados os procedimentos cabíveis relacionados à segurança da informação.
Art. 23. Nas situações de esquecimento da conta de usuário (usuário e/ou senha), caso o serviço de TI não disponibilize procedimentos para redefinição das credenciais, a mesma deverá ser reinicializada por solicitação do próprio usuário por meio da Central de Serviços de TI, podendo, para o atendimento, ser solicitada a apresentação de documentos para comprovar sua identidade.

CAPÍTULO V
UTILIZAÇÃO DE CONTAS PRIVILEGIADAS

Art. 24. Os acessos privilegiados, por questões de segurança, devem ser realizados por quantidade limitada de usuários, que terão perfis de administradores e autorização de acesso para essas funcionalidades.
Art. 25. As contas de administrador, root, superusuário ou análogas, utilizadas em sistemas e soluções de segurança e/ou infraestrutura de TI, não devem ser mantidas sob a gestão de apenas um servidor da equipe técnica de TI, devendo ser geradas e armazenadas em solução conhecida como "cofre de senhas".
Art. 26. Caso as contas privilegiadas não possam ter as senhas alteradas, serão desabilitadas e consideradas "contas de serviço", não sendo utilizadas para qualquer tipo de acesso.
Art. 27. Todas as senhas que precisarem ser trafegadas pela rede deverão estar criptografadas.

CAPÍTULO VI
DEFINIÇÃO DE SENHAS

Art. 28. As senhas não poderão conter o nome completo da conta do usuário ou mais de dois caracteres consecutivos de partes desse nome.
Art. 29. As senhas para contas de usuário deverão conter, no mínimo, 8 (oito) caracteres, e, para contas privilegiadas, no mínimo 14 (quatorze) caracteres.
Art. 30. As senhas de contas de usuário deverão conter caracteres de três destas quatro categorias:
I - Letra maiúscula;
II - Letra minúscula;
III - Número (0 a 9);
IV - Caractere especial (por exemplo: !, @, #, $, %, ^, &, *, entre outros).
Art. 31. As senhas de contas privilegiadas deverão conter as quatro categorias especificadas no artigo anterior e utilizar, sempre que viável, múltiplo fator de autenticação.
Art. 32. Os sistemas e aplicações deverão prover mecanismos que garantam que somente sejam aceitas senhas com os critérios estabelecidos nesta norma, armazenando-as de forma criptografada.

CAPÍTULO VII
VALIDADE DE SENHAS

Art. 33. As senhas deverão ser alteradas, no mínimo, a cada 180 (cento e oitenta) dias.
Art. 34. Os sistemas de autenticação de usuário guardarão um histórico de senhas, composto pelas 3 (três) últimas senhas usadas, a fim de evitar suas reutilizações.
Art. 35. Após 5 (cinco) tentativas erradas de digitação de uma senha, a conta do usuário será bloqueada automaticamente. As solicitações de desbloqueio deverão ser realizadas por meio da Central de Serviços de TI, mediante a confirmação, pela equipe de TI, da veracidade dos dados do usuário.

CAPÍTULO VIII
BLOQUEIO E EXCLUSÃO DE CONTAS DE USUÁRIO

Art. 36. As contas de usuário deverão ser bloqueadas nas seguintes situações:
I - Cessão para outra instituição;
II - Licença sem vencimento;
III - Por ausência de acesso em período superior a 60 (sessenta) dias.
Art. 37. As contas bloqueadas por ausência de acesso poderão ser reativadas a pedido do próprio usuário, por meio da Central de Serviços de TI.
Art. 38. As contas de usuário bloqueadas em decorrência de cessão ou licença sem vencimento serão reativadas, a pedido da chefia imediata, quando do retorno do servidor ao Tribunal.
Art. 39. Caso a área de TI detecte o comprometimento da conta de usuário, esta poderá ser bloqueada para que ocorram os procedimentos cabíveis relacionados à segurança da informação.
Art. 40. A exclusão da conta de usuário ocorrerá nas seguintes situações:
I - Exoneração;
II - Aposentadoria;
III - Falecimento;
IV - Devolução de servidor cedido de outra instituição;
V - Término de Termo de Compromisso de Estágio;
VI - Término do contrato de prestação de serviço.
Art. 41. Antes de efetuar a exclusão das contas de usuário em decorrência de exoneração, estas ficarão bloqueadas por 15 (quinze) dias.
CAPÍTULO IX
DISPOSIÇÕES FINAIS
Art. 42. As situações não previstas nesta norma serão submetidas ao Comitê de Segurança da Informação (CSIN).
Art. 43. As dúvidas referentes à aplicação dos procedimentos estabelecidos nesta norma poderão ser encaminhadas por meio da Central de Serviços de TI.
Art. 44. Esta PORTARIA entra em vigor na data de sua publicação.
MARIA DE LOURDES LIMA DE OLIVEIRA
Presidente do Tribunal de Contas do Estado do Pará

Protocolo: 899834

CONTRATO

EXTRATO DE CONTRATO
CONTRATO Nº 06/2023 - ORGANIZAÇÃO SOCIAL PARÁ 2000
DATA DA ASSINATURA: 27/01/2023
OBJETO: Locação de espaço no Complexo Turístico da Estação das Docas, discriminado(s) na CLÁUSULA 25ª, sendo que seu uso se destina exclusivamente à realização do evento denominado "CERIMÔNIA DO TCE".
VIGÊNCIA: 30/01/2023 até 31/01/2023
ORIGEM: Dispensa de Licitação n° 02/2023
VALOR: R$ 434.716,43 (Quatrocentos e trinta e quatro mil e setecentos e dezesseis reais e quarenta e três centavos)
DOTAÇÃO ORÇAMENTÁRIA:
Unidade Gestora: