POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

DA PROCURADORIA-GERAL DO ESTADO DO CEARÁ

NR01 - CONTROLE DE ACESSO

Setembro/2022

CEARÁ
GOVERNO DO ESTADO
PROCURADORIA-GERAL DO ESTADO

CONTROLE DE VERSÕES

Versão	Data	Responsável	Alteração principal
00	07/11/2022	Coordenadoria de TI	Versão inicial publicada

SUMÁRIO

1. INTRODUÇÃO

O controle de acesso ao ambiente tecnológico da PGE-CE, se refere aos mecanismos de autenticação necessários para que os usuários tenham acesso à rede através de credenciais (login e senha), que permita um acesso identificado e com autorização que permita acesso aos recursos necessários.

2. OBJETIVO

Definir padrões mínimos de controle no acesso aos recursos tecnológicos da PGE-CE, garantindo o acesso apenas a pessoas autorizadas.

3. ABRANGÊNCIA

Estes controles se aplicam a todos os usuários, internos ou externos, que utilizam os recursos tecnológicos da PGE-CE.

4. CONTROLE DE ACESSO

4.1. O colaborador poderá utilizar a rede e os sistemas da PGE-CE, única e exclusivamente, após identificação por meio de uma credencial de acesso (login e senha);

4.2. O login dos usuários será formado pelo seu nome e sobrenome, sendo assegurado a livre escolha do sobrenome, bem como do nome social, para fins de utilização no login de rede e na utilização do e-mail, contudo, permanecendo proibida a criação fora dos padrões determinados pela Instituição;

4.3. As autorizações devem ser definidas de acordo com a necessidade de desempenho das funções (acesso motivado) e considerando o princípio do privilégio mínimos (ter acesso apenas aos recursos ou sistemas necessários para a execução de tarefas);

4.4. Caberá a Coordenação de TI a análise periódica dos perfis de acesso utilizados por usuários internos e externos da PGE-CE;

4.5. A Coordenação de TI deverá manter bloqueado o login de acesso de todos os servidores, terceirizados, comissionados e estagiários durante o período de gozo de férias ou de qualquer afastamento das atividades laborais, mediante comunicação mensal da área de Recursos Humanos. Em situações onde se faça necessária a ativação do login neste período, o gestor da área ou superior deverá solicitar a ativação à Coordenação de TI através da Central de Serviços, informando o período em que o login ficará ativado;

4.6. Não será concedido o direito de administrador para os usuários de computador;

4.7. O acesso dos colaboradores e prestadores de serviços possuirá um prazo de validade, de acordo com o prazo do contrato firmado entre este e a PGE-CE;

4.8. Não será permitido o compartilhamento de recursos, salvo nos seguintes casos:

I. arquivos ou pastas que possuam cunho reservado ou secreto, restrito a pessoas autorizadas, de forma temporária, relacionados ao desempenho das atividades ou em conformidade com os interesses da PGE-CE; e

II. utilização de impressoras.

4.9. O uso de pasta pública nos servidores corporativos deve ser realizado de forma consciente e cautelosa, de modo a não incorrer em mal uso, como alocação indevida de espaço, armazenamento de arquivos indevidos, eliminação de arquivos, etc.

4.10. As contas de usuários serão distribuídas em três grupos:

I. Contas de usuários: utilizadas por todos os colaboradores, com acesso único à rede corporativa, com permissões exclusivas para o acesso às suas atividades.

II. Contas de administrador: utilizadas para administrar o ambiente computacional da rede.

III. Contas de serviço: utilizadas para automatizar procedimentos entre sistemas, aplicações, serviço de rede, sem qualquer intervenção humana no seu uso.

4.11. As contas de usuário serão bloqueadas após 5 (cinco) tentativas inválidas, sendo necessário entrar em contato com a CTI para reativá-las.

4.12. Na situação de esquecimento da senha, a mesma deverá ser resetada, uma vez que o conteúdo é armazenado de forma

criptografada, de modo que não seja possível reverter ou identificar o conteúdo da senha armazenada.

4.1. Controle de Acesso Lógico

Acesso lógico de contas de usuários/sistemas:

Entende-se que um acesso lógico é o acesso aos sistemas, local ou remoto, onde é necessário o uso de credenciais (login/senha).

4.1.1. Não será permitido o acesso lógico à rede por qualquer colaborador ou visitante, sem que este possua uma credencial que lhe dê o acesso com as devidas restrições aplicadas;

4.1.2. A credencial de usuário será válida pelo período de vínculo de trabalho com a PGE-CE, e não deve ser reaproveitada para outros usuários, mesmo após o término da necessidade de uso inicial;

4.1.3. As atividades realizadas por meio de determinada credencial de acesso são de responsabilidade do respectivo usuário;

4.1.4. É proibido aos usuários o compartilhamento de suas credenciais de acesso, bem como de realizarem qualquer ação utilizando a credencial de acesso individual ou de grupo para a qual não tenham sido autorizados;

4.1.5. Os usuários deverão manter bloqueada a sua estação de trabalho sempre que se ausentar do equipamento e/ou do seu ambiente de trabalho;

4.1.6. Todos os computadores e notebooks deverão estar protegidos por proteção de tela com ativação e bloqueio automático estabelecido para 10 (dez) minutos de inatividade, com o objetivo de proteger o sistema na ausência do usuário ao equipamento;

4.1.7. O gestor da área ou superior deverá abrir um chamado junto à Central de Serviços solicitando o bloqueio das credenciais de acesso do(s) respectivo(s) usuários afastados ou desligados e o ajuste das permissões quando da mudança de setor/área;

4.1.8. A área de Recursos Humanos deverá comunicar, imediatamente, à Coordenação de TI sobre qualquer demissão, exoneração ou mudança de setor de servidor, comissionado, terceirizado ou

estagiário, para que sejam realizados os procedimentos de desligamento dos acessos aos recursos e sistemas da PGE-CE;

4.1.9. Para sistemas externos, caberá ao gestor da respectiva área informar, no menor tempo possível, o desligamento do(s) usuário(s) aos Órgãos responsáveis onde o usuário possua acesso, solicitando que o acesso seja revogado;

4.1.10. As pessoas que acessam fisicamente as instalações, mas que não possuírem vínculo de trabalho com a PGE-CE, serão consideradas visitantes. Neste caso, elas terão acesso lógico a um ambiente tecnológico separado, controlado e monitorado, seja em meio físico (cabeado) ou móvel (wifi);

4.1.11. O usuário não deverá executar atividades que sejam ilegais, classificadas como crime ou contravenção, perante as leis locais, estaduais, federais ou internacionais, enquanto utilizar os recursos computacionais sob o domínio da PGE-CE;

4.1.12. Os recursos computacionais da PGE-CE não deverão ser utilizados para obter ou transmitir materiais políticos, pornográficos, de pedofilia, ofensivos, raciais, discriminatórios e que violem leis de trabalho, entre outros;

4.1.13. O usuário não deverá promover ou manter um negócio pessoal ou privado com oferta de produtos e/ou serviços, utilizando-se dos recursos computacionais e informações da PGE-CE como base de operação e/ou de divulgação para ganhos pessoais;

4.1.14. O acesso lógico aos recursos de TI deve ser gerenciado por meio de sistema de controle de acesso, concedido e mantido pela administração da rede, de acordo com as responsabilidades e atividades de cada usuário;

Acesso lógico de contas de administradores:

4.1.15. As credenciais de acesso privilegiado, que correspondem ao acesso a atividades de administrador de sistemas e/ou ativos físicos do ambiente de TI, devem ser atribuídos conforme aprovação do Coordenador de TI ou superior, com base na sua respectiva função e na necessidade de conhecimento da informação para as atividades do trabalho;

4.1.16. O compartilhamento do uso de credenciais de acesso privilegiado deve ser individual e restrito. Contudo, quando essas credenciais

precisarem ser compartilhadas por questões técnicas, estas devem ser apenas para equipe habilitada, autorizadas pelo Coordenador de Tecnologia da Informação ou superior;

4.1.17. As credenciais de acesso privilegiado devem ser necessariamente trocadas quando houver desligamento ou substituição de qualquer membro da equipe;

4.1.18. Todos os usuários que utilizam credenciais de acesso privilegiadas para execução de atividades específicas para este fim devem também possuir credenciais não privilegiadas para atividades do dia a dia, de modo que a utilização de credenciais de acesso privilegiado só ocorra quando for estritamente necessário;

Acesso lógico de contas de serviço:

4.1.19. As Contas de Serviço devem ter individualmente um responsável pela sua manutenção, bem como pela alteração de sua senha. O responsável não deve utilizar a Conta do Serviço para outros fins que não seja para o qual foi criado, conforme sua definição;

4.1.20. Sistemas e dispositivos devem ser configurados, quando tecnicamente possível, de modo a prevenir o acesso remoto por meio de Contas de Serviço;

4.1.21. Contas de Acesso privilegiado que não se enquadram em Contas de Serviço terão suas senhas expiradas em observância ao mesmo processo adotado para contas de acesso não privilegiado.

4.2. Controle de Acesso Físico

4.2.1. O acesso ao Datacenter deverá ser feito por pessoal devidamente autorizado e cadastrado no sistema de autenticação biométrica, quando existente, devendo o acesso ser registrado em software para esta finalidade, contendo no mínimo as informações de nome do usuário, data e hora do acesso;

4.2.2. O acesso de visitantes ou terceiros somente poderá ser realizado com o acompanhamento de um colaborador autorizado;

4.2.3. Não será permitido a entrada de nenhum tipo de alimento, bebida, produto que produza fumaça ou inflamável;

4.2.4. No caso de desligamento de colaboradores que possuam acesso ao Datacenter, deverá ser providenciada a sua exclusão do sistema de autenticação imediatamente.