



**CONTROLADORIA E OUVIDORIA
GERAL DO ESTADO**
Governo do Estado do Ceará

Procedimento: CONTROLE DE ACESSO	Código: P.COTIC.004	Folha: 1/13
Processo: TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Primeira Edição: 01/12/14	
Área: COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Edição: 2ª	Data: 30/09/2019

CONTROLE DE APROVAÇÃO

ELABORAÇÃO	REVISÃO	APROVAÇÃO
Daniel da Silva Monteiro	Marcus Antônio da Silva	Paulo Roberto de Carvalho Nunes
	Tiago Monteiro da Silva	Cassia Matos
		Anastácia da Silva Santos
		Marcos Henrique de Carvalho Almeida

HISTÓRICO DE MODIFICAÇÕES

EDIÇÃO	DATA	ALTERAÇÕES EM RELAÇÃO À REVISÃO ANTERIOR
01	01/12/2014	Edição inicial.
02	30/09/2019	Inclusão de autenticação de acesso, controles de acesso à <i>internet</i> , físico, lógico e de dispositivos pessoais. Revisão de diretrizes.



Procedimento: CONTROLE DE ACESSO	Código: P.COTIC.004	Folha: 2/13
Processo: TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Primeira Edição: 01/12/14	
Área: COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Edição: 2ª	Data: 30/09/2019

ÍNDICE

1. OBJETIVO	3
2. ABRANGÊNCIA	3
3. COMPETÊNCIAS	3
4. SIGLAS E CONCEITUAÇÕES	3
5. DIRETRIZES GERAIS	5
6. DIRETRIZES ESPECÍFICAS	5
7. DEVERES E RESPONSABILIDADES DO USUÁRIO E DA CGE	10
8. SANÇÕES LEGAIS	11
9. REVISÃO	11
10. APROVAÇÃO	12
11. REFERÊNCIAS BIBLIOGRÁFICAS	12
12. CONTROLE DE REGISTRO DA QUALIDADE	13



Procedimento: CONTROLE DE ACESSO	Código: P.COTIC.004	Folha: 3/13
Processo: TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Primeira Edição: 01/12/14	
Área: COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Edição: 2ª	Data: 30/09/2019

1. OBJETIVO

Estabelecer os procedimentos adequados para o acesso a ativos de Tecnologia da Informação e Comunicação (TIC) e da correta utilização das contas de usuários de rede e de recursos a fim de evitar a quebra de segurança da informação e comunicações no âmbito da Controladoria e Ouvidoria Geral do Estado do Ceará (CGE), observado o disposto no Decreto Estadual nº 29.227/2008.

2. ABRANGÊNCIA

Este procedimento abrange todos os agentes públicos que possuem ou são responsáveis por uma conta ou qualquer forma de acesso no ambiente de Tecnologia da Informação e Comunicação da Controladoria e Ouvidoria Geral do Estado do Ceará.

3. COMPETÊNCIAS

- 3.1. Compete à Direção Superior da CGE zelar pelo fiel cumprimento ao estabelecido neste procedimento;
- 3.2. Compete à Coordenadoria de Tecnologia da Informação e Comunicação (COTIC) implantar, administrar e efetuar a atualização periódica deste procedimento;
- 3.3. Competem aos agentes públicos cumprirem as determinações constantes neste procedimento, independentemente do nível hierárquico ou função, bem como do vínculo empregatício.

4. SIGLAS E CONCEITUAÇÕES

- 4.1. Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade. (Norma Complementar nº 07/IN01/DSIC/GSIPR);
- 4.2. Acesso remoto do tipo VPN: Acesso corporativo através de uma rede privada sobre a internet;
- 4.3. Controles de Acesso Físico: conjunto de procedimentos que visam restringir o acesso aos Datacenters, onde estão os equipamentos que hospedam as informações da CGE, permitindo apenas às pessoas autorizadas;
- 4.4. Controles de Acesso Lógico: conjunto de procedimentos, recursos e meios utilizados com a finalidade de prevenir e/ou obstruir ações de qualquer natureza que possam comprometer recursos computacionais, redes corporativas, aplicações e sistemas de informação;
- 4.5. Administrador: Contas administrativas que permitem acesso total e irrestrito a quaisquer recursos do sistema em que estão configuradas;



Procedimento: CONTROLE DE ACESSO	Código: P.COTIC.004	Folha: 4/13
Processo: TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Primeira Edição: 01/12/14	
Área: COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Edição: 2ª	Data: 30/09/2019

- 4.6.** Ativos: os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e os recursos humanos que a eles têm acesso. (Norma Complementar nº 10/IN01/DSIC/GSIPR);
- 4.7.** Agente público: todo aquele que exerce cargo, emprego ou função na CGE, ainda que transitoriamente ou sem remuneração, por nomeação, designação, contratação ou qualquer outra forma de vínculo (servidores públicos, militares, servidores temporários regidos pela Lei nº 8.745/1993, empregados públicos regidos pela Lei nº 9.962/2000 e colaboradores);
- 4.8.** CGE: Controladoria e Ouvidoria Geral do Estado do Ceará;
- 4.9.** COTIC: Coordenadoria de Tecnologia da Informação e Comunicação;
- 4.10.** COAFI: Coordenadoria Administrativo-Financeira;
- 4.11.** Dispositivos Pessoais: são tipicamente laptops, tablets, *Personal Digital Assistants* (PDAs), palmtops, celulares, smartphones, câmeras digitais, memorandos digitais, impressoras etc., além dos meios de armazenamento portáteis associados, tais como como *pen drive*, cartões de memória, discos rígidos portáteis, DVDs, CDs, disquetes etc.
- 4.12.** Nuvem: modelo computacional que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços (Norma Complementar nº 14/IN01/DSIC/GSIPR);
- 4.13.** Ofício Circular: Meio de comunicação formal entre órgãos e secretarias do Governo do Estado do Ceará;
- 4.14.** Rede de computadores: Conjunto de dois ou mais dispositivos (também chamados de computadores/servidores) que usam um conjunto de regras (protocolo) em comum para compartilhar recursos (aplicações, repositório de arquivos, mensagens, impressoras etc.) entre si, interligados por um subsistema de comunicação;
- 4.15.** SACC: Sistema de Acompanhamento de Contratos e Convênios;
- 4.16.** TIC: Tecnologia da Informação e Comunicação;
- 4.17.** Usuários: O usuário é quem irá usufruir do serviço prestado;
- 4.18.** VIPROC: Sistema de Virtualização de Processos do Governo do Estado do Ceará.



Procedimento: CONTROLE DE ACESSO	Código: P.COTIC.004	Folha: 5/13
Processo: TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Primeira Edição: 01/12/14	
Área: COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Edição: 2ª	Data: 30/09/2019

5. DIRETRIZES GERAIS

- 5.1. A solicitação de concessão e remoção de acesso aos ativos de TIC deve ser comunicada diretamente pela área demandante para a COAFI. A COTIC atenderá essas demandas relacionadas a acessos apenas mediante abertura de chamado realizado exclusivamente pela COAFI (categoria INFRAESTRUTURA e subcategoria SUPORTE TÉCNICO). O chamado deve conter informações a respeito dos dados pessoais (nome completo e CPF), setor da estrutura organizacional da CGE e recursos (rede interna, e-mail, sistemas etc.) da demanda. A comunicação do desligamento ao agente público deve ser realizada apenas após articulação e ciência da COTIC por questões de segurança da informação;
- 5.2. A COTIC, mediante análise criteriosa, pode bloquear, remover ou negar a concessão dos acessos aos ativos de TIC da CGE para que se evitem ameaças à integridade e sigilo das informações;
- 5.3. Todo Agente Público que necessita de acesso a recursos de TIC deverá possuir uma credencial única que o identifica, protegida por autenticação seguindo os padrões estabelecidos neste procedimento;
- 5.4. Os sistemas e aplicações, quando necessária a restrição de acesso, deverão prover um mecanismo autenticação que garanta que só sejam acessados através de usuários previamente estabelecidos;
- 5.5. Usuários e sua autenticação são individuais, secretos, intransferíveis e protegidas com o grau de segurança compatível com a informação;
- 5.6. Restrições específicas para cada ambiente, aplicação ou plataforma poderão ser adotadas;
- 5.7. Não serão concedidos mais privilégios que o necessário para execução de uma tarefa ou trabalho.

6. DIRETRIZES ESPECÍFICAS

6.1. Autenticação de acesso

- 6.1.1. As senhas de acesso à rede corporativa da CGE deverão ser trocadas periodicamente, em um prazo não superior a 90 dias, via solicitação automática quando expirar o prazo mencionado;
- 6.1.2. Os seguintes requisitos deverão ser observados por todos os usuários no momento da definição de suas senhas:
 - a) Deverá conter pelo menos 3 (três) das 4 (quatro) classes de caracteres:
 - I. Alfabético minúsculo (a, b, c ...);
 - II. Alfabético maiúsculo (A, B, C ...);



Procedimento: CONTROLE DE ACESSO	Código: P.COTIC.004	Folha: 6/13
Processo: TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Primeira Edição: 01/12/14	
Área: COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Edição: 2ª	Data: 30/09/2019

- III. Numéricos (0, 1, 2 ...);
- IV. Caracteres especiais - sinais de pontuação e/ou símbolos (@, %, !, :, { }, [], <, >, ;, ` " ? , |, / etc.).

b) Não deverá conter:

- I. O nome de usuário, nome real, ou o nome do órgão/organização/área;
- II. Uma palavra completa do dicionário;
- III. Informação significativamente igual as 6 (seis) últimas senhas.

6.1.3. O tamanho mínimo estipulado é de 7 (sete) caracteres;

6.1.4. O acesso do usuário será bloqueado após 3 (três) tentativas consecutivas de acesso incorreto;

6.1.5. Os sistemas de controle de acesso não permitem ao usuário alterar uma senha bloqueada, sendo necessário solicitar o desbloqueio através do sistema de abertura de chamados da CGE, e só será executado o desbloqueio e troca da senha depois de identificação positiva do usuário.

6.2. Controles de acesso à internet

6.2.1. O acesso à internet dar-se-á, exclusivamente, pelos meios autorizados pela COTIC;

6.2.2. O acesso à internet é disponibilizado pela CGE para uso nas atividades relacionadas ao trabalho, observado o disposto neste procedimento;

6.2.3. Constitui acesso indevido à internet e será bloqueada qualquer das seguintes ações:

a) Utilizar programas e/ou acessar páginas de troca de mensagens em tempo real (bate-papo), exceto os autorizados pelo gestor de cada área e autorizados tecnicamente pela COTIC;

b) Acessar páginas de conteúdo considerado ofensivo, ilegal, impróprio ou incompatível com as atividades funcionais ou com a política de segurança da informação, tais como pornografia, pedofilia, racismo, jogos, acesso remoto e páginas de distribuição e de compartilhamento de software;

c) Utilizar programas e/ou acessar páginas para troca de conteúdo via rede ponto-a-ponto (*peer-to-peer*);

d) Utilizar programas e/ou acessar páginas de áudio e vídeo em tempo real, ou sob demanda, exceto os autorizados pelo Coordenador de cada área ou cargo superior e autorizados tecnicamente pela COTIC;



Procedimento: CONTROLE DE ACESSO	Código: P.COTIC.004	Folha: 7/13
Processo: TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Primeira Edição: 01/12/14	
Área: COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Edição: 2ª	Data: 30/09/2019

e) Utilizar programas e/ou acessar páginas para armazenamento de conteúdo em Nuvem exceto os autorizados pelo Coordenador de cada área e autorizados tecnicamente pela COTIC;

f) Acessar Sites que representem ameaça de segurança ou que possam comprometer de alguma forma a segurança das informações da CGE;

g) Acessar ou fazer download de arquivos não relacionados ao trabalho, em especial músicas, imagens, vídeos, jogos e programas de qualquer tipo.

6.2.4. Todo tráfego de internet será controlado e inspecionado, de forma automática, pela ferramenta de filtro de conteúdo de internet, configurada de acordo com os limites estabelecidos por este procedimento;

6.2.5. A liberação de acesso a sítios e serviços bloqueados necessários ao desempenho das atribuições funcionais do agente público dependerá de solicitação devidamente justificada através do sistema de abertura de chamados à COTIC, que a submeterá quando necessário à coordenação do solicitante ou cargo superior;

6.2.6. A responsabilidade a respeito do uso adequado do recurso de internet é compartilhada por todos os agentes públicos da CGE, conforme as regras estabelecidas neste procedimento, devendo ser reportada à COTIC o seu descumprimento;

6.2.7. Todo acesso à internet deverá ser registrado, e os registros serão mantidos pela COTIC;

6.2.8. Em caso de indícios de descumprimento das diretrizes previstas neste procedimento a chefia imediata ou superior poderá solicitar, justificadamente, à COTIC auditoria dos registros de acesso à Internet;

6.2.9. As diretrizes para o controle de acesso à internet devem ser cumpridas quando utilizados equipamentos fornecidos pela CGE fora de suas dependências físicas;

6.2.10. As diretrizes para o controle de acesso à internet devem também ser cumpridas mesmo quando utilizados dispositivos pessoais conectados à rede da CGE.

6.3. Controles de acesso físico

6.3.1. Todo e qualquer acesso aos Datacenters da CGE deve ser formalizado através do sistema de abertura de chamados e conter, no mínimo, as seguintes



Procedimento: CONTROLE DE ACESSO	Código: P.COTIC.004	Folha: 8/13
Processo: TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Primeira Edição: 01/12/14	
Área: COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Edição: 2ª	Data: 30/09/2019

informações: Tempo estimado do acesso, justificativa para o acesso, nome completo e CPF de terceiros;

- 6.3.2.** Devem ser adotados pela COTIC controles que restrinjam a entrada e saída de pessoas aos Datacenters da CGE estabelecendo o acesso apenas de pessoal autorizado;
- 6.3.3.** Todo o pessoal envolvido em trabalhos de apoio aos Datacenters da CGE, tais como a manutenção das instalações físicas, deve ser orientado pela COTIC para adotar as medidas deste procedimento;
- 6.3.4.** O acesso aos Datacenters da CGE deve ser controlado e acompanhado por um técnico da COTIC. No caso de visitantes é imprescindível a autorização de um colaborador da CGE responsável pela visita;
- 6.3.5.** É proibida a utilização de equipamentos de gravação de imagem, som, vídeo ou qualquer outro que possa comprometer a segurança dos Datacenters da CGE dentro das dependências do Datacenter para fins não relacionados a manutenção do Datacenter e seus equipamentos;
- 6.3.6.** Os controles de acesso estabelecidos neste procedimento não se estendem aos Datacenters contratados como serviço de Nuvem, sendo estabelecidos para esses os definidos em contrato.

6.4. Controles de acesso lógico

- 6.4.1.** As credenciais de acesso à rede e recursos corporativos de da CGE só podem ser concedidas após a data de contratação ou de entrada em exercício do agente público;
- 6.4.2.** As credenciais de acesso à rede e recursos corporativos da CGE devem ser excluídas ou bloqueadas quando do desligamento do agente público ou em situações de riscos à segurança das informações da CGE;
- 6.4.3.** Os sistemas da CGE publicados na Internet devem ser protegidos com mecanismos para evitar a interceptação e/ou interferência de dados;
- 6.4.4.** Os computadores e sistemas que necessitam de acesso lógico restrito da CGE devem possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados, seguindo as regras da autenticação de acesso;
- 6.4.5.** Os computadores que necessitam de acesso lógico a rede interna corporativa da CGE devem ter instalado e em execução software cliente de antivírus corporativo devidamente atualizado, com verificação por vírus recentemente realizada;



Procedimento: CONTROLE DE ACESSO	Código: P.COTIC.004	Folha: 9/13
Processo: TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Primeira Edição: 01/12/14	
Área: COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Edição: 2ª	Data: 30/09/2019

6.4.6. Cada usuário deve manter suas credenciais de acesso em sigilo absoluto e não o fornecer a outra pessoa, garantindo assim, a impossibilidade de acesso indevido por pessoas não autorizadas.

6.5. Acesso de dispositivos pessoais

6.5.1. Agentes públicos que preferem, por questões diversas, utilizar dispositivos pessoais para fins de trabalho na CGE devem ser explicitamente autorizados a fazê-lo mediante solicitação no sistema de abertura de chamados;

6.5.2. A solicitação de utilização de dispositivos pessoais através do sistema de abertura de chamados deve conter, no mínimo, as seguintes informações: Tempo de validade do acesso, justificativa para o acesso, nome completo e CPF do solicitante;

6.5.3. Agentes públicos devem proteger os dados corporativos na mesma medida que protegem quando utilizam equipamentos de TIC corporativos e não devem introduzir riscos inaceitáveis (como vírus e vazamento de informações) para a rede corporativa;

6.5.4. A liberação do acesso de dispositivos pessoais só será efetivada após avaliação e aprovação pela COTIC, para que se evitem ameaças à integridade e sigilo das informações contidas na rede da CGE. Será feita uma análise criteriosa, podendo ser negado o acesso caso comprometa a segurança das informações da CGE;

6.5.5. Dispositivos pessoais devem se conectar a redes de convidados que fornecem conexões à Internet limitadas, mas não terão acesso à rede local corporativa. Eles não devem ser usados para criar, modificar, armazenar ou comunicar dados corporativos a não ser que estejam explicitamente autorizados a fazê-lo pela COTIC;

6.5.6. Recomenda-se que dados corporativos só podem ser criados, processados, armazenados e comunicados em dispositivos pessoais que executam software cliente de antivírus, o qual esteja devidamente atualizado, com verificação por vírus recentemente realizada e validado pela COTIC;

6.5.7. Aqueles dispositivos pessoais em que os proprietários se recusam a permitir que a COTIC instale o software cliente de antivírus com os direitos e privilégios necessários para operar corretamente e aqueles em que o software cliente de antivírus está desativado ou excluído após a instalação não podem ter qualquer tipo de acesso à rede da CGE;

6.5.8. Os dispositivos pessoais utilizados receberão suporte da COTIC limitado e apenas para fins corporativos;



Procedimento: CONTROLE DE ACESSO	Código: P.COTIC.004	Folha: 10/13
Processo: TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Primeira Edição: 01/12/14	
Área: COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Edição: 2ª	Data: 30/09/2019

- 6.5.9.** O acesso remoto do tipo VPN aos recursos computacionais deve ser realizado adotando os mecanismos de segurança definidos para evitar ameaças à integridade e sigilo do serviço;
- 6.5.10.** O acesso remoto do tipo VPN aos serviços corporativos somente deve ser autorizado aos agentes públicos que executem atividade vinculada à atuação institucional na CGE e que necessitam deste serviço para execução de suas atividades institucionais;
- 6.5.11.** A liberação de acesso remoto do tipo VPN, só será efetivada após avaliação e aprovação pela COTIC, para que se evitem ameaças à integridade e sigilo das informações contidas na rede da CGE. Será feita uma análise criteriosa, podendo ser negado o acesso remoto caso comprometa a segurança das informações da CGE;
- 6.5.12.** A solicitação do acesso remoto do tipo VPN deve ser realizada através do sistema de abertura de chamados e conter, no mínimo, as seguintes informações: Tempo de validade do acesso remoto, justificativa para o acesso, nome completo e CPF do solicitante;
- 6.5.13.** As informações que trafegam no acesso remoto do tipo VPN devem estar criptografadas;
- 6.5.14.** É vedada a utilização do acesso remoto do tipo VPN para fins não relacionados às atividades da instituição;
- 6.5.15.** A CGE não tem responsabilidade pelo licenciamento de software que qualquer dispositivo pessoal que tenha acesso à sua rede, sendo responsabilidade do proprietário do dispositivo.

7. DEVERES E RESPONSABILIDADES DO USUÁRIO E DA CGE

7.1. Deveres do Usuário:

- 7.1.1.** Alterar a senha quando houver suspeita de haver sido comprometida e comunicar à área de TIC;
- 7.1.2.** Não revelar o conteúdo das senhas, sob qualquer forma ou hipótese, mesmo que para o correspondente superior hierárquico, assistentes, secretárias ou colegas de trabalho.

7.2. Responsabilidades do Usuário:

- 7.2.1.** Ser responsável por todos os acessos realizados de sua propriedade;
- 7.2.2.** Zelar pelo fiel cumprimento ao estabelecido neste procedimento.



Procedimento: CONTROLE DE ACESSO	Código: P.COTIC.004	Folha: 11/13
Processo: TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Primeira Edição: 01/12/14	
Área: COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Edição: 2ª	Data: 30/09/2019

7.3. Responsabilidades da CGE:

- 7.3.1.** Criar e manter as contas de sistemas e serviços;
- 7.3.2.** Adotar mecanismos para bloquear a senha no caso de tentativas inválidas;
- 7.3.3.** Adotar mecanismos para forçar o usuário a trocar a senha no primeiro acesso;
- 7.3.4.** Instruir os usuários para a criação de senhas fortes e sobre sua importância para a segurança da informação;
- 7.3.5.** Manter o sistema de controle de acesso configurado com as especificações vigentes neste procedimento;
- 7.3.6.** Manter registros que permitam a contabilização do uso, auditoria e recuperação nas situações de falha, e possuir mecanismos que impeçam a geração de senhas fracas ou óbvias.

8. SANÇÕES LEGAIS

- 8.1.** Eventuais penalidades poderão incluir processos administrativos, criminais e cíveis, além daquelas previstas em lei;
- 8.2.** Uma vez que o usuário é responsável por qualquer atividade a partir de sua conta, o mesmo responderá diretamente por qualquer ação legal apresentada ao Governo do Estado do Ceará que envolva a sua conta de acesso a serviços;
- 8.3.** No caso de evidências de uso irregular dos recursos de acesso a serviços, o usuário terá seu acesso bloqueado para averiguação. Constatada a irregularidade, será realizado o cancelamento do acesso ao serviço e serão aplicadas as penalidades, de acordo com a legislação vigente;
- 8.4.** O usuário infrator será notificado e a ocorrência de transgressão comunicada ao seu gestor imediato e à gestão superior da CGE;
- 8.5.** Nenhuma sanção será aplicada sem a garantia da ampla defesa e do contraditório, na forma da lei.

9. REVISÃO

Este procedimento será validado anualmente e revisado sempre que necessário, em decorrência do processo de melhoria contínua do Sistema de Gestão da Qualidade.



Procedimento: CONTROLE DE ACESSO	Código: P.COTIC.004	Folha: 12/13
Processo: TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Primeira Edição: 01/12/14	
Área: COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Edição: 2ª	Data: 30/09/2019

10. APROVAÇÃO

NOME	FUNÇÃO	ASSINATURA
Paulo Roberto de Carvalho Nunes	Presidente do Comitê da Qualidade	
Cassia Matos	Coordenadora da Qualidade	
Anastácia da Silva Santos	Secretária do Comitê da Qualidade	
Marcos Henrique de C. Almeida	Coordenador de Tecnologia da Informação e Comunicação	

11. REFERÊNCIAS BIBLIOGRÁFICAS

- 11.1. Decreto nº 29.227, de 13 de março de 2008 – Dispõe sobre a Instituição da Política de Segurança da Informação dos Ambientes de Tecnologia da Informação e Comunicação - TIC do Governo do Estado do Ceará e do Comitê Gestor de Segurança da Informação do Governo do Estado do Ceará – CGSI.
- 11.2. Norma Complementar nº 07/IN01/DSIC/GSIP (Revisão 01). Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Publicada no DOU Nº 134, de 16 de julho de 2014 - Seção 1.
- 11.3. Norma Complementar nº 10/IN01/DSIC/GSIPR. Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Publicada no DOU Nº 30, de 10 de fevereiro de 2012 - Seção 1.
- 11.4. Norma Complementar nº 14/IN01/DSIC/GSIPR. Estabelece princípios, diretrizes e responsabilidades relacionados à segurança da informação para o tratamento da informação em ambiente de computação em nuvem, nos órgãos e entidades da Administração Pública Federal, direta e indireta. Publicada no DOU Nº 53, de 19 de março de 2018 - Seção 1, folhas 22 e 23.
- 11.5. Lei nº 8.745, de 09 de dezembro de 1993. Dispõe sobre a contratação por tempo determinado para atender a necessidade temporária de excepcional interesse público, nos termos do inciso IX do art. 37 da Constituição Federal, e dá outras providências.
- 11.6. Lei nº 9.962, de 22 de fevereiro de 2000. Disciplina o regime de emprego público do pessoal da Administração federal direta, autárquica e fundacional, e dá outras providências.



Procedimento: CONTROLE DE ACESSO	Código: P.COTIC.004	Folha: 13/13
Processo: TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Primeira Edição: 01/12/14	
Área: COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO	Edição: 2ª	Data: 30/09/2019

12. CONTROLE DE REGISTRO DA QUALIDADE

IDENTIFICAÇÃO	ARMAZENAMENTO	PROTEÇÃO	RECUPERAÇÃO		RETENÇÃO	DISPOSIÇÃO
			INDEXAÇÃO	ACESSO		
Registro de <i>logs</i> de acesso à <i>internet</i> fornecida pela CGE	Registro digital de eventos de <i>logs</i> inerentes aos servidores de filtro de conteúdo de acesso à internet em disco e mídias de <i>backup</i>	<i>Backup</i>	Cronológica	COTIC	30 dias	Subscrição
Registros de chamados no sistema de atendimento da CGE	Registro digital em banco de dados	<i>Backup</i>	Cronológica	COTIC	1 ano	Subscrição