Agência Goiana de Regulação, Controle e Fiscalização

PSI – Política de Segurança da Informação

Documento de Diretrizes e Normas Administrativas

Índice

Sumário

1. INTRODUÇÃO

1.1. A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da Agência Goiana de Regulação, Controle e Fiscalização de Serviços Públicos – AGR, para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas desta agência.

1.2. A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27031:2015, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está conforme as leis vigentes em nosso país.

1.3. Com a intenção de aumentar a segurança da infraestrutura tecnológica direcionada ao uso governamental, foi desenvolvida paralelamente uma Norma de Segurança da Informação, visando a orientação para a utilização dos ativos de tecnologia da informação disponibilizados.

2. OBJETIVOS

2.1. Estabelecer diretrizes que permitam aos colaboradores da Agência Goiana de Regulação, Controle e Fiscalização de Serviços Públicos seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da Agência e do indivíduo.

2.2. Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

2.3. Preservar as informações da AGR quanto à:

2.3.1. **Integridade:** garantia de que a informação seja mantida em seu estado original,

visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;

2.3.2. **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

2.3.3. **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

3. APLICAÇÕES DA PSI

3.1. As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

3.2. Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da AGR poderão ser monitorados e gravados, com ou sem prévia informação, conforme previsto nas leis brasileiras.

3.3. É também obrigação de cada colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência de Apoio Administrativo – Unidade Setorial de Tecnologia da Informação, sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

4. PRINCÍPIOS DA PSI

4.1. Toda informação produzida ou recebida pelos colaboradores de cargos de provimento Efetivo, Comissionado e/ou terceirizado como resultado da atividade profissional pertence à referida agência. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

4.2. Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

4.3. A Agência Goiana de Regulação, por meio da Gerência de Apoio Administrativo – Unidade Setorial de Tecnologia da Informação, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

5. REQUISITOS DA PSI

5.1. Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores da AGR a fim de que a política seja cumprida dentro e fora da empresa.

5.2. Deverá haver ao menos um Analista responsável pela gestão da segurança da informação, doravante designado como Analista de Segurança da Informação.

5.3. Tanto a PSI quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Analista de Segurança.

5.4. A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um termo de responsabilidade.

5.5. Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Gerência de Apoio Administrativo – Unidade Setorial de Tecnologia da Informação e ela, se julgar necessário, deverá encaminhar posteriormente ao Analista de Segurança da Informação para análise.

5.6. Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

5.7. Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados

durante a fase de execução.

5.8. Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pela AGR ou por terceiros.

5.9. Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

5.10. A AGR exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

5.11. Esta PSI será implementada na AGR por meio de procedimentos específicos do órgão, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

5.12. O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

6. DAS RESPONSABILIDADES ESPECÍFICAS

6.1. DOS COLABORADORES EM GERAL

6.1.1. Entende-se por colaborador toda e qualquer pessoa física, com vínculo ao órgão por meio de cargos de provimento efetivo, comissionado, celetista ou prestadora de serviço, por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

6.1.2. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que sofrer ou causar a AGR e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

6.2. DOS COLABORADORES EM REGIME DE PRESTAÇÃO DE SERVIÇO

6.2.1. Devem entender os riscos associados à sua condição e cumprir rigorosamente o que está previsto no aceite concedido pelo Analista de Segurança da Informação.

6.2.2. A concessão do acesso poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

6.3. DOS GESTORES DE PESSOAS E/OU PROCESSOS

6.3.1. Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

6.3.2. Atribuir aos colaboradores sob sua responsabilidade na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da AGR.

6.3.3. Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da AGR.

6.3.4. Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

6.3.5. Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

7. DOS CUSTODIANTES DA INFORMAÇÃO

7.1. DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

7.1.1. Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

7.1.2. Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

7.1.3. Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI, e pelas Normas de Segurança da Informação complementares.

7.1.4. Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

7.1.5. Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

7.1.6. Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

7.1.7. Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

7.1.8. Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a AGR.

7.1.9. Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

7.1.10. A Gerência de Apoio Administrativo – Unidade Setorial de Tecnologia da Informação, não se responsabiliza por dados pessoais nos equipamentos, sendo assim, é de inteira responsabilidade do colaborador fazer o backup de assuntos pessoais, tais como, fotos, músicas, documentos etc.

7.1.11. Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

7.1.12. Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

7.1.12.1. Os usuários (logins) individuais de funcionários serão de responsabilidade do próprio colaborador.

7.1.13. Proteger continuamente todos os ativos de informação da AGR contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

7.1.14. Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da AGR em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

7.1.15. Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da empresa.

7.1.16. Realizar auditorias periódicas de configurações técnicas e análise de riscos. Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

7.1.17. Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

7.1.18. Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da AGR operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

7.1.19. Monitorar o ambiente de TI, gerando indicadores e históricos de:

7.1.19.1. Uso da capacidade instalada da rede e dos equipamentos;

7.1.19.2. Tempo de resposta no acesso à internet e aos sistemas da AGR;

7.1.19.3. Períodos de indisponibilidade no acesso à internet e aos sistemas da AGR;

7.1.19.4. Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);

7.1.19.5. Atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

7.2. DA ÁREA DE SEGURANÇA DA INFORMAÇÃO

7.2.1. Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.

7.2.2. Propor e apoiar iniciativas que visem à segurança dos ativos de informação da AGR.

7.2.3. Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas

pelo Analista de Segurança da Informação;

7.2.4. Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da AGR, mediante campanhas, palestras, treinamentos e outros meios de endomarketing;

7.2.5. Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

7.2.6. Analisar criticamente incidentes em conjunto com o Analista de Segurança da Informação.

7.2.7. Manter comunicação efetiva com o Analista de Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a AGR.

7.2.8. Buscar alinhamento com as diretrizes corporativas da instituição.

7.3. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

7.3.1. Para garantir as regras mencionadas nesta PSI, a AGR poderá:

7.3.1.1. Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

7.3.1.2. Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior);

7.3.1.3. Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

7.3.1.4. Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

8. CORREIO ELETRÔNICO

8.1. O objetivo desta norma é informar aos colaboradores da AGR quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

8.2. O uso do correio eletrônico webmail goiás é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a AGR e também não cause impacto no tráfego da rede.

8.3. Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da AGR:

8.3.1. enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da agência;

8.3.2. enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa, ou endereço de correio eletrônico que não esteja autorizado a utilizar;

8.3.3. enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a AGR vulneráveis a ações civis, ou criminais;

8.3.4. divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

8.3.5. falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, visando evitar as punições previstas;

8.3.6. apagar mensagens pertinentes de correio eletrônico quando a AGR estiver sujeita a algum tipo de investigação.

8.3.7. produzir, transmitir ou divulgar mensagem que:

8.3.7.1. Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da AGR e do Governo do Estado de Goiás;

8.3.7.2. Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;

8.3.7.3. Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;

8.3.7.4. Vise obter acesso não autorizado a outro computador, servidor ou rede;

8.3.7.5. Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito, ou não autorizado;

8.3.7.6. Vise burlar qualquer sistema de segurança;

8.3.7.7. Vise vigiar secretamente ou assediar outro usuário;

8.3.7.8. Vise acessar informações confidenciais sem explícita autorização do proprietário;

8.3.7.9. Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

8.3.7.10. Inclua imagens criptografadas ou de qualquer forma mascaradas;

8.3.7.11. Contenha anexo(s) superior(es) a 20 MB para envio (interno e internet) e 20 MB para recebimento (internet)

8.3.7.12. Tenha conteúdo considerado impróprio, obsceno ou ilegal;

8.3.7.13. Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

8.3.7.14. Contenha perseguição preconceituosa baseada em sexo, raça, política, incapacidade física ou mental, ou outras situações protegidas;

8.3.7.15. Tenha fins políticos locais ou do país (propaganda política);

8.3.7.16. Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

8.3.8. As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

8.3.8.1. Nome do colaborador;

8.3.8.2. Gerência ou departamento;

8.3.8.3. Telefone(s);

8.3.8.4. Correio eletrônico.

9. INTERNET

9.1. Todas as regras atuais da AGR visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

9.2. Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a AGR, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

9.3. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da agência, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

9.4. O AGR, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada

inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

9.5. A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades.

9.6. Como é do interesse da AGR que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

9.7. Somente a assessoria de comunicação da AGR está devidamente autorizada a falar em nome da AGR para os meios de comunicação e poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

9.8. Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

9.9. É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

9.10. Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades da AGR e deverão abrir um chamado (Help Desk) para que um técnico possa fazer a instalação do programa. Caso o programa precise de licença e a agência não obter a mesma, o programa não será instalado no computador. Neste caso fica a critério do colaborador providenciar o que for necessário para regularizar a licença e o registro desses programas.

9.11. O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela Unidade Setorial de Tecnologia da Informação.

9.12. Os colaboradores não poderão em hipótese alguma utilizar os recursos da AGR para fazer o download ou distribuição de software, ou dados pirateados, atividade considerada delituosa conforme a legislação nacional.

9.13. O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) são expressamente proibidos.

9.14. Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

9.15. Os colaboradores não poderão utilizar os recursos da AGR para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores (Team Viewer, Any Desk).

9.16. O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos e os serviços web conferência (Webex teams, Skype) deverão ser solicitados previamente via help desk, a disponibilização do serviço será por agendamento e deve ter a mesma duração da conferência. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea (whatsapp web, telegram e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisite formalmente à Unidade Setorial de Tecnologia da Informação.

9.17. Não é permitido acesso a sites de proxy.

10. SÍTIO ELETRÔNICO INSTITUCIONAL

10.1. A Agência Goiana de Regulação, Controle e Fiscalização de Serviços Públicos possui o sítio

eletrônico institucional www.goias.gov.br/agr onde são disponibilizados informações relevantes das atividades administrativas do órgão.

10.2. O ambiente computacional que armazena todo o conteúdo é hospedado no Data Center da S**ubsecretaria da Tecnologia da Informação - STI da Secretaria de Geral de Governo – SGG** que está protegido pela Política de Segurança da informação deste órgão.

11. PORTAL DE SERVIÇOS DIGITAIS

11.1. A Agência Goiana de Regulação, Controle e Fiscalização de Serviços Públicos possui o portal web https://www.portal.agr.go.gov.br. A aplicação também está hospedada no no Data Center da **Subsecretaria da Tecnologia da Informação - STI da Secretaria de Geral de Governo – SGG** que está protegido pela Política de Segurança da informação deste órgão.

11.2. O Portal disponibiliza os seguintes serviços digitais:

11.2.1. Emissão de documentos;

11.2.2. Transações eletrônicas via webservice com outros órgãos da administração pública estadual;

11.2.3. Consulta de autenticidade de documentos;

11.3. As operações devem ser realizadas com autenticação mútua via Certificado Security Socket Layer- SSL do tipo Global visando confirmar se o servidor web cliente da AGR é exatamente aquele quem diz ser e se está autorizado a executar com integridade, confidencialidade e autenticidade as transações eletrônicas. O Certificado SSL deve realizar as seguintes operações:

11.3.1. Autenticação e verificação: verifica e autentica informações referentes à identidade de um domínio (site) e um servidor, deixando os sinais de segurança visíveis aos visitantes: cadeado na barra do browser, Selo Site Seguro e a letra S no HTTP, ficando HTTPS. Ao clicar nesses sinais, os dados sobre o Certificado são exibidos, confirmando a segurança do ambiente ao internauta.

11.3.2. Criptografia: Todas as informações que trafegam em um ambiente protegido por um Certificado SSL são protegidas contra a interceptação de terceiros por meio da criptografia dos dados. Os certificados SSL/TSL Web trabalham com criptografia simétrica de até 256-bits, algoritmo SHA-2 de chave pública RSA e Chave de 2048-bits.

11.3.3. Validação de Organização: Os certificados SSL/TSL Web emitidos devem possuir Validação do órgão. Este processo dever ser seguro, pois, além de certificar que o órgão está legalmente constituído, deve assegurar que o mesmo está em operação e que o domínio do certificado é de sua propriedade. Este processo previne que a certificação do domínio seja utilizada para fins maliciosos (Exemplo: Phishing).

11.3.4. Aplicação do Selo Site Seguro: Ao final da autenticação do seu domínio é concedido o direito de utilizar o nosso selo interativo de segurança em seu site. O Selo Site Seguro é sinônimo de confiança na web e melhora comprovadamente a visibilidade do site e contribui para a diminuição no abandono de carrinho.

12. IDENTIFICAÇÃO

12.1. Os dispositivos de identificação (crachá) e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a AGR e/ou terceiros.

12.2. O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

12.3. Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

12.4. Todos os dispositivos de identificação utilizados na AGR, como o crachá, as identificações de acesso aos sistemas (senhas), os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

12.5. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

12.6. Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

12.7. Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a AGR e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

12.8. É proibido o compartilhamento de login para funções de administração de sistemas.

12.9. A Gerência Institucional da AGR é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

12.10. A Unidade Setorial de Tecnologia da Informação responde pela criação da identidade lógica dos colaboradores na agência, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.

12.11. Devem ser distintamente identificados os colaboradores, visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

12.12. Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

12.13. Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

12.14. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

12.15. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como "abcdefgh", "87654321", entre outras.

12.16. Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário solicite que outro colaborador abra um chamado via sistema (Help Desk), caso não tenha nenhum colaborador disponível para fazer a abertura deste chamado, o usuário deverá entrar em contato com a Unidade Setorial de Tecnologia da Informação através do telefone 3226-6466, neste caso o técnico deverá estabelecer um processo para a renovação de senha (confirmar a identidade).

12.17. Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

12.18. A periodicidade máxima para troca das senhas é 45 (quarenta e cinco) dias, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 30 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

12.19. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for exonerado/demitido ou solicitar exoneração/demissão, a Gerência Institucional deverá imediatamente comunicar tal fato a Unidade Setorial de Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

13. COMPUTADORES E RECURSOS TECNOLÓGICOS

13.1. Os equipamentos disponíveis aos colaboradores são de propriedade da AGR, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da

agência, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

13.2. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da Unidade Setorial de Tecnologia da Informação, ou de quem este determinar.

13.3. Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

13.4. Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de solicitação de atendimento *Service Desk*.

13.5. A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver conforme a classificação de tal informação e com a real necessidade do destinatário.

13.6. Arquivos pessoais e/ou não pertinentes da AGR (fotos, músicas, vídeos, etc.) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente sem comunicação prévia ao usuário.

13.7. Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede (PASTA DADOS). Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

13.8. Os colaboradores da AGR e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando, ou programa que venha sobrecarregar os serviços

existentes na rede corporativa sem a prévia solicitação e a autorização da Unidade Setorial da Tecnologia da Informação.

13.9. No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

13.9.1. Todos os computadores de uso individual deverão ter senha de administrador para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas Unidade Setorial de Tecnologia da Informação, que terá acesso a elas para manutenção dos equipamentos.

13.9.2. Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.

13.9.3. É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da USTI ou por terceiros devidamente contratados para o serviço.

13.9.4. Todos os modems internos ou externos devem ser removidos, ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de informática.

13.9.5. É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.

13.9.6. O colaborador deverá manter a configuração do equipamento disponibilizado pela AGR, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da agência, assumindo a responsabilidade como custodiante de informações:

13.9.6.1. Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.

13.9.6.2. Todos os recursos tecnológicos adquiridos pela AGR devem ter imediatamente suas senhas padrões (default) alteradas.

13.9.6.3. Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

13.9.7. Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da AGR:

13.9.7.1. Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.

13.9.7.2. Burlar quaisquer sistemas de segurança.

13.9.7.3. Acessar informações confidenciais sem explícita autorização do proprietário.

13.9.7.4. Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).

13.9.7.5. Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito, ou não autorizado.

13.9.7.6. Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais, ou propriedades intelectuais sem a devida autorização legal do titular;

13.9.7.7. Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

13.9.7.8. Utilizar software pirata, atividade considerada delituosa conforme a legislação nacional.

14. DATACENTER

14.1. O acesso ao Datacenter na Sede da AGR somente deverá ser feito por colaboradores da Unidade Setorial de Tecnologia da Informação.

14.2. Deverá ser verificado diariamente o funcionamento do Datacenter, fazendo uma verificação dos ativos de rede, ar condicionado, no-break entre outros.

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

14.4. Deverão existir duas cópias de chaves da porta do Datacenter. Uma das cópias ficará de posse do coordenador responsável pelo Datacenter, a outra, de posse do Gerente.

14.5. O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do departamento de Serviços Gerais.

14.6. Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

14.7. A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pelo responsável do Datacenter.

15. BACKUP

15.1. Todos os backups devem ser automatizados por sistemas de agendamento automatizado para serem preferencialmente executados fora do horário comercial, nas chamadas "janelas de backup" – períodos em que não há nenhum ou pouco acesso de usuários, ou processos automatizados aos sistemas de informática.

15.2. Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

15.3. É necessária a previsão, em orçamento anual, da renovação dos discos em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante dos discos para qualquer uso emergencial.

15.4. Discos que apresentam erros devem ser primeiramente formatados e testados. Caso o erro persista, deverão ser inutilizadas.

15.5. É necessário ser inserido, periodicamente, o dispositivo de limpeza nas unidades de backup nos termos do Procedimento de Controle de Mídias de Backup.

15.6. Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios da AGR, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e conforme a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

15.7. Na situação de erro de backup e/ou Restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

15.8. Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade nos termos do Procedimento de Controle de Backup e Restore.

15.9. Quaisquer atrasos na execução de backup ou restore deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Mídias de Backup.

15.10. Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, segundo a criticidade do backup.

15.11. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

15.12. Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo coordenador de infraestrutura, nos termos do Procedimento de Controle de Backup e Restore.

15.13. Os colaboradores responsáveis descritos nos devidos procedimentos e na planilha de responsabilidade poderão delegar a um custodiante a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.

16. DAS DISPOSIÇÕES FINAIS

16.1. Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da Agência Goiana de Regulação, Controle e Fiscalização de Serviços Públicos. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela agência.