Política de Segurança da Informação e Comunicações (POSIC)

Terracap

Agência de Desenvolvimento do Distrito Federal

ÍNDICE

1. INTRODUÇÃO

A Terracap tem na informação um dos seus principais ativos, devendo ele ser adequadamente utilizado e protegido contra riscos, ameaças, violações, acessos não autorizados e danos. É imprescindível, portanto, a adoção de condutas, normas e procedimentos padronizados que tenham como objetivo garantir a proteção dos três aspectos básicos da segurança da informação: confidencialidade, integridade e disponibilidade.

Uma política de segurança da informação ou PoSIC (Política de segurança das informações e comunicações) tem por objetivo possibilitar o gerenciamento da segurança em uma organização, estabelecendo regras e padrões para proteção da informação. A política possibilita manter a confidencialidade, garantir que a informação não seja alterada ou perdida e permitir que a informação esteja disponível quando for necessário.

2. ESCOPO

Os objetivos e diretrizes aqui estabelecidos serão desenvolvidos para toda a organização, devendo ser observados por todos empregados, colaboradores, fornecedores e prestadores de serviço, e se aplicam à informação em qualquer forma (arquivos eletrônicos, mensagens eletrônicas, dados de intranet e internet, bancos de dados, arquivos impressos, informações expressadas verbalmente, mídias de áudio e vídeo, dentre outros) e em qualquer meio ou suporte, durante todo o seu ciclo de vida (criação, manuseio, divulgação, armazenamento, transporte e descarte).

Integram também a PoSIC as os enunciados normativos e os procedimentos complementares destinados à proteção da informação e à disciplina de sua utilização.

3. REFERÊNCIAS LEGAIS E NORMATIVAS

Esta Política de Segurança foi elaborada em consonância com os seguintes enunciados normativos:

- Instrução Normativa GSIPR nº 01/2008, que dispõe sobre as orientações que deverão ser implementadas na Gestão de Segurança da Informação pelos órgãos e entidades da Administração Pública Federal;
- Norma Complementar nº 03/IN01/DSIC/GSIPR, que institui diretrizes para a elaboração da Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;
- Política de Segurança da Informação e Comunicação Governo do Distrito Federal (POSIC/GDF);

- Decreto Federal nº 9.637/2018, que institui a Política Nacional de Segurança da Informação;
- Lei Federal nº 12.965/2014, que instituiu o Marco Civil da Internet;
- Lei Distrital nº 2.572/2000, que dispõe sobre a prevenção das entidades públicas do Distrito Federal com relação aos procedimentos praticados na área de informática;
- Decreto Distrital nº 25.750/2005, que regulamenta a Lei nº 2.572/2000 (Segurança da Informação no âmbito do DF);
- Lei Federal nº 12.527/2011, que dispõe sobre o acesso a informações no âmbito do setor público;
- Decreto Federal nº 7.724/2012, que regulamenta a Lei de Acesso a Informação;
- Lei Distrital nº 4.990/2012, que regula o acesso a informações no Distrito Federal;
- Decreto Federal nº 7.845/2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo;
- Artigo 482 do Decreto-Lei nº 5.452/1943 (Consolidação das Leis Trabalhistas - CLT);
- Normas ABNT NBR ISO/IEC 17799:2005, 27001:2013, 27002:2013 e 27005:2011;
- Código de Conduta e Integridade da Terracap;
- Lei Federal n.º 13.709/18, que trata da Lei Geral de Proteção de Dados Pessoais (LGPD).

4. CONCEITOS E DEFINIÇÕES

Abaixo seguem, em ordem alfabética, os principais conceitos referidos neste documento, de forma a evitar dificuldades de interpretação ou ambiguidades:

a) Algoritmo: conjunto das regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número finito de etapas;

b) Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (ABNT, 2005);

c) *Antispyware*: *software* de segurança que tem o objetivo de detectar e remover *softwares* maliciosos;

d) Assinatura Digital: mecanismo criptográfico que tem por objetivo assinar documentos digitalmente;

e) Ativo de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que têm acesso a eles (Portaria 45 SE-CDN, 2009);

f) Autenticidade: propriedade que determina que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

g) Backup: é o processo de cópia de dados de um dispositivo de armazenamento para outro com o objetivo de proporcionar a proteção contra a perda dos originais;

h) Certificação Digital: é um arquivo eletrônico que serve como identidade virtual para uma pessoa física ou jurídica, e por ele podem ser feitas transações *online* com garantia de autenticidade e proteção das informações trocadas;

i) Classificação da informação: processo que tem como objetivo identificar e definir níveis e critérios adequados para a proteção das informações, de acordo sua importância para as organizações;

j) Código Malicioso: tipo de código de computador ou *script* da *Web* nocivo que tem como objetivo criar vulnerabilidades no sistema, violações de segurança, roubo de dados e informações, além de outros danos possíveis;

k) Confidencialidade: somente pessoas devidamente autorizadas pelo órgão devem ter acesso à informação;

l) Continuidade de Negócios: Capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação de atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido (NC 06 DSIC/GSIPR,2009);

m) Controle de Acesso: processo por meio do qual os acessos aos sistemas e a seus respectivos dados são autorizados ou negados; os acessos autorizados e, em alguns casos, também os negados ficam registrados para posterior auditoria;

n) Criptografia: mecanismo de segurança e privacidade que torna determinada comunicação (textos, imagens, vídeos, entre outros) ininteligível para quem não tem acesso aos códigos de "tradução" da mensagem;

o) Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

p) Dispositivos Móveis: equipamentos portáteis dotados de capacidade computacional ou dispositivos removíveis de memória para armazenamento;

q) Engenharia Social: habilidade de conseguir acesso a informações confidenciais ou a áreas importantes de uma instituição por meio de habilidades de persuasão;

r) FTP (*File Transfer Protocol*): protocolo que permite a transferência de arquivos entre computadores conectados à *Internet*;

s) Gestão de Risco: avalia os riscos relativos a segurança, disponibilidade de dados e desempenho dos ativos de informação e também a conformidade com exigências regulatórias e legais;

t) Gestão de Segurança de Informação e Comunicação: processo que visa a proteção dos ativos de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão e a modificação desautorizada de dados armazenados ou em trânsito, inclusive a segurança dos recursos

humanos, da documentação, das áreas e das instalações computacionais e de comunicações;

u) Informação: dados estruturados, organizados e processados, apresentados dentro do contexto, o que o torna relevante e útil para a pessoa que o deseja.

v) Integridade: alterações, supressões e adições nas informações devem ser realizadas apenas sob processos legalmente válidos, por pessoas devidamente autorizadas para tal (autênticas). Garante que as ações que modifiquem as informações não ocorram de forma acidental ou não autorizada;

w) Incidente: qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança dos sistemas, das informações ou das redes de computadores;

x) Impacto: mudança adversa no nível obtido dos objetivos do negócio (ABNT, 2008);

y) *Login*: processo para acessar um sistema informático restrito feita por meio de autenticação ou identificação do utilizador;

z) Mídia Removível: tipo de memória que pode ser removida do seu aparelho de leitura, conferindo portabilidade para os dados que carrega;

aa) Plano de Continuidade de Negócio (PCN): documento que estabelece mecanismos para restabelecer a atividade de uma organização, em caso de interrupção;

bb) Programas Antivírus: programas usados para proteger e prevenir computadores e outros aparelhos de códigos ou vírus, a fim de dar mais segurança ao usuário;

cc) Risco: efeito da incerteza nos objetivos (ABNT ISO GUIA 73,2009);

dd) Segurança da Informação e das Comunicações: ações que visam viabilizar e assegurar disponibilidade, integridade e confidencialidade das informações;

ee) Servidor: *software* ou *hardware* que fornece um ou mais serviços a uma rede de computadores;

ff) *Software*: programa, rotina ou conjunto de instruções que controlam o funcionamento de um computador;

gg) Termo de Responsabilidade e Sigilo: documento pelo qual o empregado ou colaborador se compromete a não revelar as informações de caráter secreto, sigiloso e confidencial da Companhia;

hh) *Torrent*: extensão de arquivos utilizados por um protocolo de transferência do tipo P2P (*Peer to Peer*);

ii) Vírus de Computador: *software* malicioso capaz de infectar um sistema, fazer cópias de si e se espalhar para outros computadores e dispositivos;

jj) *Wireless*: tecnologia que significa “sem fio” (em livre tradução), e possibilita a transmissão da conexão entre pontos distantes sem precisar usar fios (como ocorrem em telefones sem fio, rádios ou celular).

5. PRINCÍPIOS

O conjunto de documentos que compõe esta PoSIC deverá se guiar pelos seguintes princípios:

a) Simplicidade: a complexidade aumenta a chance de erros, portanto, todos os controles de segurança deverão ser simples e objetivos;
b) Privilégio Mínimo: usuários devem ter acesso apenas aos recursos de tecnologia da informação necessários para realizar as tarefas que lhe foram designadas;
c) Segregação de função: funções de planejamento, execução e controle devem ser segregadas, de forma a reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos, bem como para permitir maior eficácia dos controles de segurança;
d) Auditabilidade: todos os eventos significantes de usuários e os processos devem ser rastreáveis até o evento inicial por meio de registro consistente e detalhado;
e) Mínima dependência de segredos: os controles deverão ser efetivos, ainda que se conheça a existências deles e como eles funcionam;
f) Resiliência: os controles de segurança devem ser projetados para que possam resistir ou se recuperar dos efeitos de um desastre;
g) Defesa em profundidade: os controles de segurança devem ser concebidos em múltiplas camadas, de modo a prover redundância para que, no caso de falha, outro controle possa ser aplicado.

6. OBJETIVOS

São objetivos desta Política:

a) Proteger a informação da Terracap, de forma a garantir sua confiabilidade, autenticidade e integridade;
b) Estabelecer diretrizes para a utilização dos recursos de informação, serviços de redes de dados, estações de trabalho, *Internet*, telecomunicações, correio eletrônico e outros;
c) Designar papéis e responsabilidades relativas à segurança da informação na Companhia;
d) Ser transparente e inclusiva, de forma a conscientizar todos os empregados da Terracap sobre a importância das informações e de suas vulnerabilidades;
e) Promover e desenvolver a cultura de segurança da informação em todos os níveis da Companhia;
f) Ser parte integrante dos processos organizacionais;
g) Possibilitar a criação de controles e promover a otimização dos recursos de tecnologia da informação.

7. ESTRUTURA NORMATIVA DA SEGURANÇA DA INFORMAÇÃO

7.1. DEFINIÇÃO

A estrutura normativa da Segurança da Informação da Terracap é composta por um conjunto de documentos com três níveis distintos, relacionados a seguir:

- Política de Segurança da Informação (Política): constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação;
- Enunciados normativos de Segurança da Informação: estabelecem obrigações e procedimentos específicos alinhados com a Política, a serem seguidos em diversas áreas em que a informação é tratada;
- Procedimentos de Segurança da Informação (Procedimentos): instrumentalizam o disposto nas Normas e nas Diretrizes, permitindo a direta aplicação nas atividades da Terracap.

7.2. DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

A Política e os Enunciados Normativos de Segurança da Informação devem ser divulgados a todos os empregados da Terracap e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

Os Procedimentos de Segurança da Informação ficarão disponíveis na rede interna da Companhia, e devem ser divulgados às áreas diretamente relacionadas à sua aplicação.

8. ATRIBUIÇÕES E RESPONSABILIDADES NA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

8.1. GERAIS

Cabe a todos os empregados, diretores/presidente, estagiários, prestadores de serviço e terceirizados da Terracap:

a) Cumprir fielmente a Política, os Enunciados Normativos e os Procedimentos de Segurança da Informação da Terracap;
b) Manter-se atualizado em relação a esta Política, demais normas e procedimentos relacionados, buscando informação junto a seu superior ou

junto à autoridade competente sempre que não estiver absolutamente seguro quanto a obtenção, uso e/ou descarte de informações;

c) Promover a segurança de seu usuário corporativo, departamental ou de rede local, bem como de seus respectivos dados, credenciais de acesso e quaisquer informações a que tenha acesso em virtude do cargo que ocupa;
d) Utilizar de forma ética, legal e consciente os recursos computacionais e informacionais da Terracap, estando ciente de que sua estrutura não poderá ser utilizada para fins particulares e que quaisquer ações que tramitem em sua rede poderão ser auditadas;
e) Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pela Terracap;
f) Cumprir as leis e as normas que regulamentam os aspectos da propriedade intelectual;
g) Comunicar imediatamente à Coordenação de Tecnologia da Informação e Inovação (COTIN) qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos;
h) Ser responsável por qualquer prejuízo ou dano que vier a sofrer ou causar à Terracap em decorrência da não obediência às diretrizes e às normas referidas na Política de Segurança da Informação e das Comunicações e às normas e aos procedimentos específicos dela decorrentes.

Adicionalmente, são definidas as seguintes responsabilidades e atribuições específicas relacionadas à segurança da informação:

8.2. DIRETORIA COLEGIADA

Em relação à segurança da informação, cabe à Diretoria Colegiada:

a) Aprovar a Política de Segurança da Informação e os enunciados normativos de Segurança da Informação e suas revisões.

8.3. COMITÊ DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO (CTSI)

A gestão da segurança da informação na Terracap será realizada por comitê multidisciplinar, chamado COMITÊ DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO - CTSI. Cabe ao CTSI:

a) Propor normas relativas à segurança da informação e de comunicações;
b) Assessorar a implementação das ações de segurança da informação e comunicações da companhia;
c) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e de comunicações;

d) Analisar os casos de violação da Política e dos Enunciados Normativos de Segurança da Informação, encaminhando-os à autoridade competente, quando for o caso;
e) Propor o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação;
f) Determinar a elaboração de relatórios, levantamentos e análises que deem suporte à gestão de segurança da informação e à tomada de decisão;
g) Acompanhar o andamento dos principais projetos e iniciativas relacionados à segurança da informação;
h) Propor a relação de "responsáveis" pelas informações da Terracap.

8.4. ÁREA DE TECNOLOGIA DA INFORMAÇÃO (COTIN)

Cabe à Coordenação de Tecnologia da Informação e Inovação (COTIN):

a) Propor ajustes, aprimoramentos e modificações de regras, em relação à Segurança da Informação;
b) Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação da Terracap, mantendo-se atualizada em relação às melhores práticas existentes no mercado e em relação às tecnologias disponíveis;
c) Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso lógico da Terracap, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários;
d) Prover todas as informações de gestão de segurança da informação solicitadas pelo CTSI, podendo solicitar informações às demais áreas da Terracap (diretorias, coordenações, entre outras), caso necessário;
e) Prover ampla divulgação da Política e dos Enunciados Normativos de Segurança da Informação para todos os empregados da Terracap;
f) Oferecer orientação e treinamento sobre a Política de Segurança da Informação e seus Enunciados Normativos a todos os empregados da Terracap;
g) Realizar testes e averiguações em sistemas e equipamentos, com o intuito de verificar o cumprimento da Política e dos Enunciados Normativos de Segurança da Informação;
h) Realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação e dos demais ambientes em que circulam as informações da Terracap;
i) Estabelecer mecanismo de registro e controle de não-conformidades com a Política e os Enunciados Normativos da Informação, solicitando que o CTSI tome as providências.

8.5. RESPONSÁVEL PELA INFORMAÇÃO

O responsável pela informação é um diretor ou um coordenador da Terracap, formalmente indicado pela Presidência, responsável por concessão, manutenção, revisão e cancelamento de autorizações de acesso ao conjunto de informações pertencentes à sua área de atuação.

Cabe ao responsável pela informação:

a) Elaborar, para toda informação sob sua responsabilidade, matriz que relaciona cargos e funções da Terracap às autorizações de acesso concedidas;
b) Autorizar a liberação de acesso à informação sob sua responsabilidade, observadas a matriz de cargos e funções, a Política, os Enunciados Normativos e os Procedimentos de Segurança da Informação da Terracap;
c) Manter registro e controle atualizados, em relação a todas as liberações de acesso concedidas. Deve ser determinada, sempre que necessário, a pronta suspensão ou a alteração de tais liberações;
d) Reavaliar, sempre que necessário, as liberações de acesso concedidas, cancelando aquelas que não forem mais necessárias;
e) Solicitar relatórios de controle de acesso com o objetivo de identificar desvios em relação à Política e aos Enunciados Normativos de Segurança da Informação, tomando as ações corretivas necessárias;
f) Participar da investigação de incidentes de segurança relacionados à informação sob sua responsabilidade;
g) Participar, sempre que convocado, das reuniões do COMITÊ DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO, prestando os esclarecimentos solicitados.

8.6. DIRETORIAS, COORDENAÇÕES E DEMAIS ESTRUTURAS ORGANIZACIONAIS

Cabe a Diretorias, Coordenações e demais estruturas organizacionais:

a) Cumprir e fazer cumprir esta Política, os Enunciados Normativos e os Procedimentos de Segurança da Informação;
b) Assegurar que suas equipes possuam acesso e conhecimento desta Política, dos Enunciados Normativos e dos Procedimentos de Segurança da Informação aplicáveis;
c) Ajudar a redigir os Procedimentos de Segurança da Informação relacionados às suas áreas;
d) Comunicar imediatamente eventuais casos de violação de segurança da informação à COTIN.

8.7. COORDENAÇÃO GERAL DE GESTÃO DE PESSOAS

Cabe à Coordenação Geral de Gestão de Pessoas:

a) Colher assinatura do Termo de Sigilo e Responsabilidade de todos os empregados da Terracap, arquivando-o nos respectivos prontuários;
b) Informar a Área de Tecnologia Da Informação sobre desligamentos, licenças, afastamentos e modificações no quadro funcional, para que sejam tomadas as medidas cabíveis em relação à segurança da informação.

9. DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO

Neste capítulo, são apresentadas as diretrizes gerais da Política de Segurança da Informação da Terracap. Essas diretrizes constituem os principais pilares da Gestão de Segurança da Informação da Companhia, norteando a elaboração das Normas e dos Procedimentos.

Enunciados Normativos e Procedimentos específicos para um ou mais tópicos aqui presentes poderão ser criados, a critério da CTSI.

9.1. ADOÇÃO DE COMPORTAMENTO SEGURO

Independentemente do meio ou da forma em que se encontre, a informação está presente no dia a dia de todos os empregados da Terracap. Portanto, é fundamental para a sua proteção que seja adotado comportamento seguro e condizente com o objetivo de proteger os ativos informacionais da companhia, com destaque para os seguintes itens:

a) Todos os empregados e prestadores de serviços devem assumir atitude proativa e engajada no que diz respeito à proteção das informações da Terracap;
b) Todos os empregados da Terracap devem compreender as ameaças externas e internas que podem afetar a segurança da informação na empresa, tais como vírus de computador, interceptação de mensagens eletrônicas, bem como engenharia social e outras artimanhas frequentemente utilizadas para a roubar senhas e obter acesso a sistemas de informação;
c) Todos os recursos de informação da Terracap devem ser projetados e utilizados para a consecução dos objetivos finalísticos da companhia. É vedada a utilização desses recursos para fins particulares;
d) Toda informação produzida ou recebida pelos empregados, terceirizados, fornecedores e prestadores de serviço, em resultado da função exercida e/ou atividade profissional contratada, no âmbito da Terracap, é de

propriedade da Companhia. Quaisquer exceções devem ser devidamente formalizadas;

e) Cada usuário é responsável pela segurança das informações dentro da Terracap;
f) Todo tipo de acesso à informação da Terracap que não for explicitamente autorizado é proibido;
g) As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive empregados da própria Companhia), anotadas em papel ou em sistema visível ou de acesso não-protegido;
h) Qualquer tipo de dúvida sobre a Política de Segurança da Informação e seus Enunciados Normativos deve ser imediatamente esclarecida com o COMITÊ DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO ou com a Área de Tecnologia Da Informação (COTIN).

9.2. ADOÇÃO DE INVENTÁRIO E DE SISTEMA DE CLASSIFICAÇÃO DA INFORMAÇÃO

Deve ser implementado na Terracap sistema de classificação de informações, de forma que todas as suas informações sejam categorizadas e disponibilizadas apenas às pessoas que tenham acesso.

a) As áreas de negócio devem manter um inventário atualizado que identifique e documente a existência e as principais características de todos os seus ativos de informação (base de dados, arquivos, diretórios de rede, trilhas de auditoria, códigos fonte de sistemas, documentação de sistemas, manuais, planos de continuidade, entre outros);
b) As informações inventariadas devem ser classificadas de acordo com o grau de confidencialidade e criticidade para a Terracap, e com base no Enunciado Normativo de Segurança da Informação;
c) As informações inventariadas devem ser associadas a um “responsável”, que deverá ser diretor ou coordenador da Terracap, formalmente designado pela Presidência como responsável pela autorização de acesso às informações sob a sua responsabilidade;
d) O COMITÊ DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO será responsável por verificar a conformidade do inventário elaborado pelas coordenações, de modo a orientá-las sobre a correção de eventuais falhas.

9.3. ACESSO À INFORMAÇÃO

A informação é o ativo mais valioso de qualquer instituição e, como tal, deve ser protegida.

a) A Terracap deve fornecer informações aos cidadãos, desde que não exista impedimento legal relativo à confidencialidade da informação, conforme estabelece a Lei nº 4.990/2012,que regulamenta o acesso a informações no DF;
b) É vedado às pessoas físicas ou jurídicas que de alguma forma estão relacionadas com a Terracap divulgar quaisquer informações a que tenham acesso em virtude do cargo sem autorização por escrito de autoridade competente da Terracap, sob pena de aplicação das sanções cabíveis;
c) É vedado aos usuários de sistema de informação da Terracap prestar consultoria a pessoa física ou jurídica, inclusive sindicato ou associação de classe, valendo-se de dados e informações não divulgadas publicamente;
d) É vedada a alteração ou a deturpação do teor de quaisquer documentos, bem como a retirada das instalações da Terracap, sem estar devidamente autorizado, de qualquer documento ou bem pertencente ao patrimônio da Companhia;
e) No tratamento da informação classificada, devem ser utilizados sistemas de informação e canais de comunicação seguros, que atendam aos padrões mínimos de qualidade e segurança;
f) A unidade de gestão de pessoas da Terracap deve providenciar a coleta do aceite e da assinatura do Termo de Responsabilidade e Sigilo de todos os empregados, diretores, conselheiros, comissionados, conveniados, estagiários e empregados aprendizes da Companhia, bem como dos novos contratados, no ato da contratação;
g) Os gestores de contratos que possuam prestadores de serviços devem providenciar a coleta do aceite e da assinatura do Termo de Responsabilidade e Sigilo dos prestadores de serviço que tenham acesso aos sistemas de informação da Terracap;
h) A liberação de Acesso Físico ou Lógico a qualquer sistema de informação, documento ou recurso de processamento e ou armazenamento de dados da Terracap somente será efetuado após a concordância do usuário com o Termo de Responsabilidade e Sigilo da Companhia, sendo completamente vedada a liberação de acesso a qualquer recurso informacional sem a assinatura do documento.

9.4. SEGURANÇA FÍSICA

A proteção do ambiente da Terracap deve prevenir a empresa contra perda, dano ou comprometimento dos ativos, contra a interrupção das atividades do negócio, bem como contemplar, quando for o caso, medidas de segurança contra: roubo, fogo, explosivos, fumaça, água (ou falha do abastecimento), poeira, vibração, efeitos químicos, interferência no fornecimento elétrico e radiação eletromagnética, umidade e fungos,

roedores e insetos, intempéries (raio, vendaval, granizo, entre outros), impacto de veículos ou aeronaves, curto-circuito e outros danos elétricos, atos por pessoas (vandalismo, sabotagem, entre outros) e interrupção no fornecimento de climatização.

a) Áreas cuja natureza ou o manuseio de documentos e a utilização dos recursos de processamento da informação não exijam proteção são consideradas áreas de acesso livre;
b) Áreas que abriguem em seu interior documentos, processos, recursos de processamento da informação ou reuniões e eventos de caráter reservado devem ser consideradas áreas de acesso restrito;
c) A localização das áreas de acesso restrito, bem como a sua capacidade de resistência a acessos não autorizados devem ser adequados ao grau de confidencialidade de documentos e informações existentes em seu interior;
d) Assuntos confidenciais e de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, entre outros).

9.5. MEIOS DE INFORMAÇÃO

Faz-se necessário proteger e controlar os meios de armazenagem de informações contra danos que possam prejudicar as atividades do negócio:

a) Todos os meios de informação devem ser armazenados de forma segura, seguindo as recomendações dos fabricantes;
b) A retirada de qualquer informação, independentemente do meio, deve ser autorizada por escrito pela diretoria, gerência ou coordenação, que deverá ainda manter os registros dessas retiradas para fins de auditoria e controle;
c) Informações confidenciais da Terracap não podem ser transportadas em qualquer meio (CD, DVD, disquete, pen-drive, papel, entre outros) sem as devidas autorizações e proteções especificadas por Diretrizes ou Normas;
d) Quando a utilização de uma informação não for mais necessária, ela deve ser removida de qualquer meio reutilizável em que se encontre;
e) Os meios que possuírem informações sensíveis devem ser descartados de forma segura, como, por exemplo: fragmentação de listagens, eliminação de informações magnéticas (de forma a não ter como se recuperar), desmagnetização de meios defeituosos, entre outros.

9.6. CRIPTOGRAFIA

A criptografia é uma grande aliada da segurança da informação, e poderá ser utilizada para manter a confidencialidade, a autenticidade e a integridade das informações pertencentes à Terracap.

a) O uso de criptografia poderá ser utilizado somente quando aprovado pela COTIN, ou seja, em casos específicos, devidamente formalizados, e seguindo normas ou procedimentos relativos ao manuseio de informações classificadas;
b) Os algoritmos e os métodos de criptografia utilizados devem se basear em padrões de mercado e utilizar apenas tecnologias homologadas pela COTIN;
c) Certificação digital e assinatura digital poderão ser utilizados como forma de garantir a segurança nas comunicações institucionais.

9.7. CONTROLE DE ACESSO

Todo acesso às informações e aos ambientes lógicos da Terracap deve ser controlado, de forma a garantir permissão apenas às pessoas autorizadas pelo respectivo proprietário da informação, observando as seguintes diretrizes:

a) Procedimento formal de concessão e cancelamento de autorização de acesso aos sistemas de informação;
b) Comprovação da autorização do proprietário da informação;
c) Utilização de identificadores de usuário (ID de usuário) individualizados, de forma a assegurar a responsabilidade de cada usuário por suas ações;
d) Verificação se o nível de acesso concedido é apropriado ao propósito da atividade exercida e se é consistente com a Política de Segurança da Informação e com suas Normas;
e) Remoção imediata de autorizações dadas a usuários afastados ou desligados do órgão, ou que tenham mudado de função;
f) Processo de revisão periódica das autorizações concedidas;
g) Política de atribuição, manutenção e uso de senhas.

O controle de acesso deverá considerar e respeitar o princípio do menor privilégio, em que cada usuário deverá possuir o mínimo de privilégios necessários para desempenhar suas atividades.

9.8. USO E ACESSO À INTERNET E À INTRANET

A utilização dos recursos informacionais da companhia deve ser pautada de forma ética e profissional, sempre priorizando a proteção dos ativos de informação da Terracap.

a) O uso de recursos e serviços de TI da companhia é restrito aos empregados da Terracap e usuários externos credenciados e autorizados, sendo vedada a sua utilização fora dessas condições;
b) A Terracap poderá, a qualquer tempo e sem aviso prévio aos usuários, bloquear, restringir, filtrar, monitorar, capturar, controlar ou auditar todos os

recursos e os serviços de TI no âmbito da Companhia, estejam eles nas estações de trabalho ou nos servidores de rede, visando assegurar o cumprimento de sua Política de Segurança da Informação e de Comunicações;

c) É vedado o uso de recursos computacionais e de comunicação da Terracap para disseminação de conteúdo protegido por direitos autorais, ilegais, via *Torrent*, FTP ou qualquer outro mecanismo de compartilhamento de arquivos;
d) É vedado o uso de *Internet* para acesso de conteúdos que não estejam relacionados às atividades laborais, sendo prerrogativa da COTIN a avaliação da liberação de acessos a sítios bloqueados;
e) É vedada a concessão de privilégio de administrador local dos computadores, salvo quando expressamente autorizada pela COTIN, de acordo com os critérios técnicos por ela definidos;
f) Possíveis exceções de privilégios para acesso a ambientes bloqueados devem ser solicitadas pela chefia imediata do usuário, com respectiva justificativa, e somente serão liberadas após avaliação e autorização da COTIN, que terá a responsabilidade pelo gerenciamento das exceções;
g) É proibido, sob qualquer alegação ou pretexto, o uso de qualquer meio ou subterfúgio para burlar, fraudar, anular ou impedir a ação dos sistemas de segurança da informação implementados na Terracap;
h) Falhas de segurança da informação percebidas pelos usuários deverão ser comunicadas à COTIN imediatamente para que sejam tomadas as devidas providências;
i) Perfis institucionais mantidos nas redes sociais devem, preferencialmente, ser administrados e gerenciados por equipes compostas exclusivamente por empregados públicos ocupantes de cargo efetivo. Quando não for possível, a equipe pode ser mista, desde que sob a coordenação e responsabilidade de um empregado do quadro permanente da Terracap.

9.9. CORREIO ELETRÔNICO

O correio eletrônico é uma ferramenta de trabalho disponibilizada para todos os usuários da Terracap, independentemente de seu vínculo funcional. Dessa forma, ela deverá ser utilizada somente para fins corporativos e relacionados às atividades do empregado, sendo vedada a sua utilização para tratar de assuntos de cunho pessoal.

9.10. PROTEÇÃO CONTRA SOFTWARES MALICIOSOS

Devem ser implementadas medidas de prevenção e detecção automática de *softwares* maliciosos, assim como programas de conscientização dos usuários. Os usuários devem ser orientados de que a prevenção é sempre a melhor solução.

a) Os Recursos de Tecnologia da Informação da Terracap devem estar sempre munidos de soluções de detecção e bloqueio de programas de código malicioso, como, por exemplo, *antispyware*, programas antivírus, programas de análise de conteúdo de correio eletrônico e de acesso à Internet;
b) A instalação e a configuração da solução de detecção e bloqueio de programas maliciosos somente devem ser realizadas pela COTIN;
c) Tais softwares devem ser atualizados constantemente, e sua execução deve ser agendada para ocorrer periodicamente, fazendo uma varredura completa nas estações de trabalho ou dispositivos móveis da Terracap;
d) Qualquer mídia removível de origem duvidosa ou não autorizada deve ser avaliada quanto à presença de vírus ou outros *softwares* maliciosos antes de ser utilizada. Arquivos recebidos por correio eletrônico também devem ser inspecionados;
e) É vedada a instalação de *softwares* nos recursos computacionais da Terracap sem o prévio conhecimento e autorização da área responsável. Os usuários devem fazer uso apenas de *softwares* licenciados e homologados pela COTIN.

9.11. DATACENTER (CENTRO DE PROCESSAMENTO DE DADOS)

Regras para a administração do centro de processamento de dados da companhia poderão ser fixadas em Enunciado Normativo próprio, considerando as seguintes diretrizes gerais:

a) O datacenter deverá ser mantido com sistema de tranca e monitoramento 24 horas do dia, 07 dias por semana, e seu acesso se dará somente por pessoas autorizadas e credenciadas;
b) Quando houver a necessidade de entrada de terceiros no interior do datacenter, o acesso deverá ser realizado com a presença de um empregado da COTIN;
c) Imediatamente após o desligamento de usuários que possuam acesso ao data center, deverá ser providenciada a sua exclusão da relação de pessoas autorizadas para realizarem o acesso às suas instalações;
d) A função de administrador do datacenter deverá ser atribuída exclusivamente a empregado efetivo, preferencialmente vinculado à área de Infraestrutura de TI (DIRAU/COTIN).

9.12. BACKUP (CÓPIA DE SEGURANÇA)

Os procedimentos próprios ao serviço de *backup* (cópia de segurança) institucional deverão ser fixados em Enunciado Normativo complementar, considerando as seguintes diretrizes gerais:

a) A realização do *backup* institucional consistirá no armazenamento da cópia dos dados contidos nos computadores servidores da Terracap. A realização de *backup* dos dados contidos nas estações de trabalho é de responsabilidade de cada usuário. A empresa não se responsabiliza por nenhum conteúdo presente nas máquinas utilizadas pelos usuários;
b) Todos os documentos pertinentes às atividades institucionais da Terracap deverão ser armazenados nos servidores da companhia. Tais arquivos, se gravados apenas localmente nos computadores dos usuários, não serão incluídos na rotina de *backup* e poderão ser perdidos caso ocorra uma falha na máquina, situação em que a responsabilidade será inteiramente do usuário, podendo ele ser responsabilizado por quaisquer prejuízos à Terracap;
c) Arquivos pessoais e/ou não pertinentes às atividades institucionais da Terracap (fotos, músicas, vídeos, entre outros) não deverão ser copiados ou movidos para os *drives* de rede. Caso identificados, esses arquivos poderão ser excluídos sem a necessidade de comunicação prévia ao usuário;
d) É vedado o armazenamento de informações corporativas, tais como bases de dados, arquivos, ou demais documentos em locais inadequados, tais como serviços de armazenamento em nuvem, computadores pessoais ou servidores de prestadores de serviço, salvo com a autorização expressa da COTIN.

9.13. MONITORAMENTO, CONTROLE E AUDITORIA

A rede, os sistemas, as informações e os serviços utilizados pelos usuários são de exclusiva propriedade da Terracap, não podendo ser interpretados como de uso pessoal. Todos os empregados da Terracap devem ter ciência de que o uso da rede, das informações e dos sistemas de informação da Terracap pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política e dos Enunciados Normativos de Segurança da Informação e, conforme o caso, servir como evidência em processos administrativos e/ou legais. Visando efetivar esse controle, a Terracap poderá:

a) Implantar sistemas de monitoramento em estações de trabalho, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, de forma que a informação gerada ou trafegada por eles permita a sua rastreabilidade, identificando usuários e respectivos acessos efetuados;
b) Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria no caso de exigência judicial, solicitação de coordenador ou gerente

(ou autoridade superior), ou por determinação do COMITÊ DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO;

c) Realizar, a qualquer tempo, inspeção física nos equipamentos de sua propriedade;
d) Instalar sistemas de proteção, preventivos e/ou repressivos, para garantir segurança das informações e dos perímetros de acesso;
e) Desinstalar, a qualquer tempo, qualquer *software* ou sistema que represente risco ou esteja em desconformidade com políticas, normas, procedimentos e princípios vigentes.

9.14. TRATAMENTO DE INCIDENTES EM REDES COMPUTACIONAIS

No Tratamento de Incidentes em redes computacionais, a equipe técnica da COTIN deverá considerar as seguintes diretrizes:

a) O incidente deverá ser investigado, estudado e sanado, de forma a preservar disponibilidade, integridade, confidencialidade e autenticidade da informação;
b) Todos os incidentes notificados ou detectados deverão ser registrados, com a finalidade de assegurar registro histórico das atividades desenvolvidas;
c) Caberá aos usuários comunicar a COTIN sobre as falhas e os incidentes de que tomem conhecimento;
d) No caso de indícios de ilícitos criminais, o CTSI e a COTIN terão como dever, sem prejuízo de suas demais atribuições, acionar as autoridades competentes para a adoção dos procedimentos legais cabíveis.

9.15. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

O CTSI deverá realizar, de forma sistemática, a avaliação dos riscos relacionados à segurança da informação da Terracap, que servirá como base, entre outros, para o Plano de Continuidade de Negócios institucional (PCN).

9.16. GESTÃO DE CONTINUIDADE DE NEGÓCIOS

A Terracap deverá criar, manter e testar periodicamente uma estratégia de continuidade dos processos críticos institucionais, pronta para operar em caso de interrupção total ou parcial de suas atividades.

10. VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SANÇÕES

O descumprimento ou a inobservância de quaisquer regras ou diretrizes definidas nesse instrumento e em suas normas complementares constituem falta grave, sobre as quais a Terracap aplicará todas as medidas cabíveis nos âmbitos administrativo, civil e judicial.

São considerados comportamentos contrários à Política de Segurança da Informação da Terracap:

a) praticar atos irregulares que causem prejuízo à Terracap, com o intuito de obter lucro ou vantagem de qualquer espécie (próprio ou para terceiros), ou que provoquem abuso de confiança; erros ou prejuízos por motivo fútil; uso indevido de senha ou processo de identificação de terceiros; ou a utilização de qualquer meio fraudulento;
b) Qualquer comportamento comissivo ou omissivo no tratamento das informações, na guarda e no manuseio dos sistemas e das redes de computadores e dados, bem como de documentos físicos que lesem a Terracap, quem nela trabalha ou terceiros;
c) A utilização de qualquer dos recursos da Terracap para fins unicamente particulares;
d) Apagar, destruir, modificar ou, de qualquer forma, inutilizar, total ou parcialmente, dados, programas de computador, documentos físicos ou quaisquer outros de forma indevida ou não autorizada;
e) Obter, manter ou fornecer a terceiro acesso de forma indevida ou não autorizada a dados, instrução, computador, rede de computadores, ambientes ou qualquer meio de identificação, tais como crachás, senhas, *logins*, entre outros;
f) Obter segredos, informações sigilosas ou dados pelos quais o usuário não possui acesso, armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar, bem como documentos físicos, de forma indevida ou não autorizada;
g) Criar, desenvolver ou inserir dado ou programa em computador ou rede de computadores, de forma indevida ou não autorizada, com a finalidade de apagar, destruir, inutilizar ou modificar dados ou programas de computador, ou de qualquer forma dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores;
h) Realizar *download* e *upload* de jogos, filmes, conteúdo pornográfico, bem como de qualquer outro programa que atenda única e exclusivamente aos interesses do usuário e não da Companhia;
i) Distribuir cópia não autorizada de arquivos, informações, *software* ou qualquer outro ativo da Terracap;

j) Utilizar o serviço de correio eletrônico para envio de mensagens com teor político/partidário, racista, comercial, preconceituoso, pornográfico, pejorativo, publicitário ou com outros fins não pertinentes às atividades da Terracap;
k) Valer-se de qualquer meio ou subterfúgio para burlar, fraudar, anular ou impedir a ação dos sistemas de segurança da informação implementados na Terracap;
l) Agir em desacordo com padrões e procedimentos específicos de utilização dos recursos e serviços de rede corporativa da Terracap.

11. CONSIDERAÇÕES FINAIS

Para a uniformização da informação organizacional, esta Política de Segurança da Informação e de Comunicações deverá ser distribuída a todos os gestores, empregados, terceirizados e prestadores de serviço da Terracap, a fim de que seja conhecida e cumprida.

12. REVISÕES

Versão	Data	Responsável	Motivação
1.0	29/07/2019	Cássio da Nóbrega Santiago	Criação do documento.
2.0	30/07/2019	Cássio da Nóbrega Santiago	Reformulação do documento.
2.1	05/08/2019	Cássio da Nóbrega Santiago	Ajustes e complementações.
2.2	25/09/2019	Cássio da Nóbrega Santiago	Ajustes.
2.3	21/07/2020	Rafael Scofield Sardenberg	Finalização do documento e ajuste para novo organograma da Terracap.
2.4	23/11/2020	Rafael Scofield Sardenberg	Ajustes apontados pela empregada Carine Vogel Dutra Telles.
2.5	27/07/2021	Rafael Scofield Sardenberg	GEINF -> ASINF. Alterações nas aprovações necessárias.

2.6	15/07/2025	Fransuescley Oliveira de Farias	ASINF -> COTIN. Alterações nas aprovações necessárias.