Prodest
Tecnologia da Informação

2023

Política de Segurança da Informação

Acesse a versão online:
seguranca.prodest.es.gov.br

SUMÁRIO

APRESENTAÇÃO

Como órgão responsável pela tecnologia da informação e comunicação do Governo do Estado do Espírito Santo, é constante a preocupação da Prodest com a segurança das informações por ela processadas ou custodiadas, a fim de se evitar que quaisquer eventos indesejados ou inesperados possam colocar em risco a CONFIDENCIALIDADE, INTEGRIDADE, DISPONIBILIDADE, AUTENTICIDADE ou LEGALIDADE dessas informações, afetando serviços públicos e prejudicando os proprietários das informações e seus usuários – principalmente o cidadão.

Por esta razão implementamos, em 2004, nossa Política de Segurança da Informação (PSI), formalizando o comprometimento da autarquia com a gestão de riscos e nos obrigando ao desafio de aprimorarmos cada vez mais o nível de segurança das informações da administração pública sob nosso tratamento ou responsabilidade.

A Política de Segurança da Informação da Prodest contempla as principais diretrizes a serem seguidas para que se possa garantir a segurança das informações envolvidas em seus processos, procedimentos, ambientes e ativos. Essas diretrizes devem nortear as atividades e processos cotidianos executados pela autarquia e estão alinhadas com a legislação e regulamentações vigentes (incluindo a PESI - Política Estadual de Segurança da Informação) e com as melhores práticas de mercado, em conformidade com a ISO 27001 (principal norma internacional relacionada à segurança da informação).

Porém, a preocupação com a proteção da informação é também um compromisso individual e contínuo de todas as partes envolvidas – funcionários, estagiários, clientes, parceiros, prestadores de serviço ou qualquer pessoa que tenha acesso a quaisquer informações pertencentes, processadas ou custodiadas pela Prodest, ou que utilize seus serviços, recursos ou ativos de informação. Cada um de nós é corresponsável pela eficácia desse conjunto de medidas e pela disseminação da cultura de segurança da informação – não só cumprindo a PSI, como também participando pró-ativamente desse processo, através de sugestões e críticas que possam ajudar a aprimorar nossas políticas de Segurança da Informação e a aumentarmos cada vez mais o nível de segurança das informações, sistemas, aplicações, ambientes e processos que se encontrem sob nossa responsabilidade.

A Diretoria
Área de Gestão da Segurança da Informação

Esta Política de Segurança da Informação (PSI) é aplicável a quaisquer informações pertencentes, processadas ou custodiadas pela Prodest e deve ser conhecida e cumprida por qualquer pessoa ou ente público ou privado que estabeleça qualquer tipo de relação com a Prodest, seja formal ou informal, independentemente de sua duração. Ou seja, seus estagiários, comissionados, empregados, prestadores de serviço, fornecedores, parceiros, clientes (incluindo cidadãos que utilizem seus serviços ou ativos), servidores públicos a ela cedidos por outros órgãos – todos referenciados nesta PSI como "*usuários*".

Devido ao caráter evolutivo dos tópicos contemplados nesta PSI, seu conteúdo está sujeito a constantes alterações, sem aviso prévio ou posterior, razão pela qual sua última versão deve sempre ser consultada antes de serem tomadas

RESPONSABILIDADES INDIVIDUAIS

1) Todos os usuários devem conhecer e cumprir as determinações desta Política de Segurança da Informação que sejam aplicáveis e relacionadas ao escopo de suas relações com a autarquia, bem como quaisquer outras obrigações ou termos adicionais relativos à segurança da informação porventura estabelecidos e formalizados com a Prodest.

2) Todos os usuários devem tratar com a devida **CONFIDENCIALIDADE** todas as informações de caráter sigiloso às quais terão acesso ou conhecimento durante a vigência de sua relação com a Prodest, mesmo após seu encerramento ou extinção do vínculo com a autarquia, por tempo indeterminado ou pelos prazos previstos na legislação em vigor, não as reproduzindo, cedendo, divulgando ou permitindo acesso às mesmas a pessoas não autorizadas a acessá-los ou conhecê-los – à exceção de quando autorizado pelo proprietário da informação, ou se requerido por força de lei ou mandado judicial.

3) Todos os usuários devem zelar pela **INTEGRIDADE**, **DISPONIBILIDADE**, **AUTENTICIDADE** e **LEGALIDADE** das informações acima citadas, não as utilizando para benefício próprio ou para fins que possam trazer prejuízos de qualquer natureza à Prodest, aos seus proprietários, a terceiros ou ao Governo do Estado do Espírito Santo.

4) Usuários não devem compartilhar senhas, códigos, *tokens*, crachás, cartões de acesso ou quaisquer outros meios, credenciais ou dispositivos de autenticação que lhes sejam fornecidos para seu uso exclusivo de serviços, recursos ou ativos gerenciados pela Prodest, cuja utilização ocorrerá sob total responsabilidade dos mesmos.

5) Aqueles que utilizem ou administrem sistemas, ambientes ou quaisquer outros ativos ou recursos pertencentes a Prodest ou por ela gerenciados, não devem permitir que os mesmos sejam acessados por pessoas que não tenham necessidade de efetuarem tais acessos e que não possuam as devidas permissões requeridas para tal.

6) Os usuários devem se limitar a acessar apenas as informações e recursos necessários à execução das atividades relacionadas ao escopo de suas relações com a Prodest e conforme direitos, privilégios e permissões concedidos para a execução dessas atividades, observando os termos desta PSI e a legislação brasileira em vigor.

7) Os usuários são responsáveis por seus atos e pelos danos e incidentes provocados pelo mau uso que fizerem das informações e recursos sob suas responsabilidades, sendo aos mesmos imputadas as punições cabíveis.

ACESSO FÍSICO E SEGURANÇA PATRIMONIAL

1) O acesso físico de pessoas a setores, áreas e instalações, bem como a gestão desses acessos e a delimitação de perímetros de segurança físicos, devem ser efetuados conforme estabelecido nas Instruções de Serviço específicas publicadas na intranet da Prodest.

2) Usuários somente devem autorizar a entrada de pessoas na Prodest nos casos e ambientes permitidos pela autarquia, desde que possuam os devidos privilégios funcionais ou contratuais para efetuarem e permitirem tais acessos. Nos casos de ambientes restritos, é necessária autorização de um de seus responsáveis.

3) A entrada e a saída de bens, equipamentos e demais ativos tecnológicos das dependências da Prodest devem ser efetuadas com observância aos aspectos de segurança da informação aplicáveis a cada caso e conforme normatizado nas Instruções de Serviço relativas ao controle e gestão de patrimônio publicadas na intranet da Prodest, visando evitar acessos não autorizados a informações sigilosas armazenadas nesses ativos.

ACESSO LÓGICO E UTILIZAÇÃO DE RECURSOS

1) Todos os meios de comunicação eletrônica da Prodest devem garantir a rastreabilidade, o requerido grau de sigilo e a eficácia de entrega das mensagens enviadas.

2) Os equipamentos da Prodest disponibilizados aos usuários (estações de trabalho, notebooks, tablets, smartphones etc.) devem ser e permanecer configurados de forma a minimizar a probabilidade de incidentes de segurança.

3) Não é permitida a conexão de equipamentos pessoais ou de terceiros nas redes locais (cabeadas). Terceiros só devem ter acesso aos seus recursos se necessário à execução das atividades afins à relação estabelecida com a Prodest.

4) Autorizações de acesso a sistemas, ambientes e demais recursos devem ser concedidas mediante necessidade e sob o princípio dos privilégios mínimos.

5) Usuários com privilégios de administração de redes, sistemas, ambientes e demais recursos de alta criticidade não devem acessá-los ou gerenciá-los através de redes sem fio ou de redes inseguras.

6) O e-mail institucional (*usuário*@prodest.es.gov.br) deve ser usado apenas para fins relacionados ao trabalho, não devendo ser divulgado ou cadastrado em sites ou serviços relacionados a interesses exclusivamente pessoais.

7) Os usuários devem adotar todas as medidas que lhes forem possíveis para que suas caixas postais de correio eletrônico não sejam acessadas por terceiros, seja através de dispositivos próprios, alheios, ou pertencentes a Prodest.

8) Usuários realocados internamente ou entre órgãos, temporariamente afastados (inclusive em gozo de férias ou licenças de qualquer tipo), e exonerados ou desligados por motivo de rescisão contratual, deverão ter suas credenciais de acessos lógicos e físicos revogados ou temporariamente suspensos, de acordo com a particularidade de cada caso.

9) As regras de concessão e revogação de acessos às redes da Prodest e seus respectivos recursos se encontram no anexo "PSI-ANEXO-002 - Acesso às redes da Prodest".

COMPARTILHAMENTO DE INFORMAÇÕES

1) Dados ou informações só devem ser compartilhados com quem possa ou deva ter acesso aos mesmos.

2) O compartilhamento de arquivos entre usuários da rede local da Prodest deve ser efetuado, de preferência, através da pasta "Público" do servidor de arquivos da rede local, cujo conteúdo é acessível a todos os seus usuários e deve ser automaticamente apagado diariamente. Informações que não possam ser acessadas por usuários diferentes dos seus destinatários não deverão ser compartilhados através deste recurso.

3) O envio ou compartilhamento de arquivos (especialmente os de conteúdo confidencial) com pessoas que estejam fora do ambiente de rede local da Prodest, ou que não possam ou não devam ser enviados por correio eletrônico, deverão ser efetuados através da solução de armazenamento em "nuvem" oferecido pela autarquia (drive.es.gov.br).

4) Senhas de acesso a recursos e ambientes da Prodest que precisem ser compartilhadas entre seus administradores ou equipes devem ser armazenadas criptografadas em sistemas seguros, específicos para este propósito.

5) O atendimento a solicitações externas de fornecimento de informações pertencentes a entes públicos e custodiadas ou processadas pela Prodest, quando efetuadas por terceiros ou mesmo por seus próprios proprietários, deve ser efetuado conforme estabelecido no anexo "PSI–ANEXO-005 – Fornecimento de dados a terceiros".

ARMAZENAMENTO DE INFORMAÇÕES

1) Os usuários devem efetuar backups (cópias de segurança) dos arquivos digitais relevantes relacionados às suas atividades de trabalho, armazenando-os na rede local (em pastas pessoais ou nas pastas associadas aos setores nos quais estão lotados). Esse conteúdo deve fazer parte das rotinas de backup corporativas.

2) Conteúdo confidencial com alto grau de sigilo não deve ser armazenado fora dos ambientes da Prodest.

3) Documentos imprescindíveis às atividades dos usuários deverão ser armazenados na rede local corporativa e, preferencialmente, devem ser acessados e editados remotamente através da mesma.

4) Arquivos pessoais ou não pertinentes às atividades da Prodest não deverão ser copiados ou movidos para repositórios da rede corporativa, visando não comprometer o espaço de armazenamento disponibilizado e evitar incidentes de segurança da informação. Caso identificados, esses arquivos poderão ser excluídos definitivamente, sem aviso prévio.

5) As rotinas de backup devem ser planejadas e executadas conforme a natureza, requisitos e necessidades de processos, serviços, aplicações e requisitos legais e de conformidade com normas ou padrões cujo cumprimento seja necessário ou recomendado.

6) *Logs* (registros de eventos) devem ser armazenados pelos períodos definidos pelos proprietários ou gestores dos sistemas que os geraram, levando em consideração as exigências desta PSI e da legislação vigente.

DESCARTE DE INFORMAÇÕES

1) Meios, mídias e equipamentos contendo informações confidenciais ou de negócio devem ser instalados, utilizados, armazenados, transportados e descartados de forma segura.

2) O descarte de informações deve ser feito conforme as Tabelas de Temporalidade das atividades meio e fim, publicadas no website do PROGED (Programa de Gestão Documental do Governo do Estado do ES).

3) Todos os usuários devem devolver, após o término de suas relações com a Prodest, todas as mídias eletrônicas ou impressas que possuam quaisquer informações confidenciais pertencentes à Prodest ou a terceiros. Nos casos em que não houver essa possibilidade, comprometem-se a efetuar seu descarte seguro (ação sujeita à verificação da Prodest).

PRIVACIDADE E SIGILO

1) Não se deve presumir sigilo absoluto em mensagens eletrônicas, ou seja, os usuários devem considerar que o conteúdo de suas mensagens poderá ser acessado ou conhecido por outras pessoas além dos seus respectivos destinatários.

2) Os usuários devem aceitar que as atividades por eles executadas utilizando recursos da Prodest poderão por ela ser monitoradas, fiscalizadas e auditadas a qualquer tempo, mesmo sem aviso prévio ou anuência dos mesmos (a não ser quando houver restrições legais aplicáveis, ou exceções estabelecidas contratualmente).

3) Os usuários devem, na medida do possível, se certificarem de estar lidando com as pessoas certas ao fornecerem informações confidenciais em mensagens, telefonemas ou quaisquer outros meios de comunicação e interação.

4) A Prodest e seus representantes, contratados e parceiros devem proteger a privacidade de dados pessoais, conforme estabelecido contratualmente e/ou nos termos da legislação em vigor.

ACESSO À INTERNET

1) É proibido acessar a Internet através das redes da Prodest para praticar, incitar, induzir ou promover qualquer ideia, ato ou atividade ilegais ou que violem esta PSI, a Política Estadual de Segurança da Informação (PESI) do Governo do Estado do ES e o Código de Ética Profissional dos Servidores Civis do Estado do ES. E, também, nos seguintes casos:
    a) Envio de mensagens comerciais, sem prévia solicitação ou consentimento dos destinatários (*SPAM*).
    b) Usos que prejudiquem o desempenho das redes internas e demais recursos tecnológicos da Prodest.
    c) Utilização de recursos que mascarem, adulterem ou tornem anônima a identidade do usuário, se fazendo passar por outra pessoa ou organização, para cometimento de atos ilegais ou ações que prejudiquem terceiros.
    d) Exploração de vulnerabilidades de segurança em ativos tecnológicos da Prodest ou de terceiros (a não ser para fins necessários ao trabalho e desde que o usuário tenha as devidas prerrogativas legais ou funcionais).
    e) Invasão, utilização, ou acesso ilegal ou não autorizado a recursos ou ativos de informação da Prodest ou de terceiros (tais como senhas ou demais informações alheias, redes de computadores, computadores ou outros dispositivos, serviços ou recursos de uso restrito ou exclusivo), a não ser nos casos justificáveis e autorizados pela Prodest e/ou pelo proprietário ou gestor do ativo a ser acessado.

2) Visitantes e usuários internos que desejem acesso à Internet através de seus dispositivos móveis pessoais nas dependências da Prodest deverão utilizar apenas a rede sem fio disponibilizada para este fim.

3) O download e upload de grandes volumes de dados ou o uso de serviços que provoquem sobrecarga da rede ou do link de Internet, ainda que para fins profissionais, devem ser evitados e, quando imprescindível, devem ser deslocados, preferencialmente e se possível, para horários de menor pico de utilização ou fora do horário comercial.

4) Em atendimento à legislação em vigor, a Prodest registra todos os acessos à Internet efetuados através de suas redes ou dispositivos, podendo, inclusive, auditá-los para garantir a segurança de suas informações ou a utilização adequada dos recursos de sua propriedade e sob sua responsabilidade.

5) A Prodest se reserva o direito de bloquear, temporária ou permanentemente, o acesso a determinados websites e serviços de Internet. Caso o usuário necessite de acesso a um ou mais recursos cujo acesso esteja bloqueado, ou até mesmo de acesso livre e irrestrito à Internet, seja temporária ou permanentemente, o mesmo deverá solicitar ao gestor imediato ao qual esteja subordinado no exercício de suas atividades.

6) Em caso de abuso e/ou prejuízo para a Prodest ou para terceiros, o acesso concedido deverá ser imediatamente suspenso, até que o fato seja devidamente investigado e solucionado.

CLASSIFICAÇÃO DA INFORMAÇÃO

1) Toda informação deve ser classificada quanto ao seu grau de sigilo no momento de sua geração ou obtenção, e essa classificação deve ser preservada (incluindo eventuais alterações) durante todo o seu ciclo de vida.

2) A informação que não for classificada e pertencer à Prodest será considerada pública, desde que possa ser divulgada sem causar qualquer tipo de risco ou impacto negativo à Prodest, aos proprietários da mesma, a terceiros ou ao Governo do Estado do Espírito Santo, não requerendo medidas especiais para sua segurança e armazenamento.

3) Cabe somente ao proprietário da informação classificar seu nível de sigilo. Na ausência dessa classificação, todas as informações de terceiros que estejam sob a custódia ou processamento da Prodest devem ser tratadas como possuindo o mais alto grau de sigilo.

4) As normas de classificação de informação estão descritas no anexo "PSI-ANEXO-003 - Classificação da Informação".

ASPECTOS LEGAIS E RELAÇÕES COM TERCEIROS

1) Todos os contratos comerciais e de trabalho elaborados pela Prodest, bem como seus editais, devem possuir as seguintes cláusulas de segurança da informação, para cumprimento por todas as partes envolvidas:

   DA SEGURANÇA DA INFORMAÇÃO

   a) *As partes e seus representantes (empregados, associados, parceiros, conveniados, terceirizados e afins) deverão conhecer e cumprir a Política de Segurança da Informação da Prodest (disponível para consulta no site "seguranca.prodest.es.gov.br"), no que for aplicável e relacionado ao escopo de suas relações com a autarquia, bem como quaisquer outras políticas ou termos adicionais relativos à segurança da informação porventura estabelecidos e formalizados entre as partes, sob pena de adoção das punições cabíveis (incluindo rescisão contratual, quando aplicável).*

   b) *As partes e seus representantes deverão tratar com o devido nível de sigilo todas as informações às quais terão acesso ou conhecimento, não as comercializando, reproduzindo, cedendo ou divulgando para pessoas não autorizadas a acessá-las ou conhecê-las.*

   c) *O sigilo de informações confidenciais deverá ser mantido durante a vigência da relação estabelecida entre as partes e mesmo após seu encerramento, por tempo indeterminado ou pelos prazos previstos na legislação em vigor – exceto se estritamente necessário para cumprimento de obrigações contratuais ou quaisquer outros termos formalizados entre as partes, se autorizado pelo proprietário da informação ou responsável, ou se requerido por força de lei ou mandado judicial.*

   d) *Caberá às partes garantir que seus representantes, sejam pessoas físicas ou jurídicas, conheçam e cumpram as cláusulas acima, sendo solidariamente responsáveis por quaisquer descumprimentos e suas consequências.*

2) As áreas gestoras de editais e de contratos celebrados pela Prodest devem:

   a) Incluir, em editais e contratos, as cláusulas de segurança da informação descritas no item 1 acima, atualizando-as conforme sofram alterações, que deverão ser informadas às respectivas áreas gestoras pelo editor desta PSI

   b) Providenciar para que as partes signatárias desses contratos tenham conhecimento prévio dessas cláusulas antes do início do processo licitatório ou da formalização contratual

3) Estagiários, comissionados, empregados e servidores públicos cedidos à Prodest por outros órgãos de Governo devem assinar o "Termo de Compromisso" desta PSI, antes de iniciarem suas atividades, independentemente de seus prazos de vigência.

4) A assinatura do "Termo de Compromisso" também poderá ser aplicável a pessoas físicas ou representantes de pessoas jurídicas que estabeleçam relações breves e informais com a Prodest, em quaisquer dos seguintes casos:

   a) Se utilizarem a infraestrutura ou recursos tecnológicos da Prodest para realizarem atividades por ela autorizadas
   b) Se tiverem acesso a informações confidenciais pertencentes, processadas ou custodiadas pela Prodest

   A necessidade de assinatura deverá ser avaliada caso a caso, em conjunto com a área de Segurança da Informação.

5) Fiscais de contratos e demais representantes da Prodest responsáveis por acompanhar ou intermediar contratações ou contratos, Ordens de Compra, convênios, parcerias, eventos ou demais atividades com terceiros, devem:

   a) Providenciar a coleta da assinatura do "Termo de Compromisso" junto aos envolvidos, quando aplicável
   b) Instruí-los sobre a necessidade de conhecerem e cumprirem esta Política de Segurança da Informação
   c) Orientá-los e supervisioná-los quanto aos aspectos de segurança da informação a serem cumpridos

6) Toda informação produzida nos ambientes da Prodest, como resultado de atividades por ela contratadas, pertence à Prodest ou aos seus respectivos proprietários beneficiários, devendo as exceções serem explicitamente formalizadas.

INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

1) Todos os usuários devem comunicar quaisquer incidentes de segurança da informação ocorridos ou prováveis de ocorrerem, através do preenchimento do formulário "Registro de Incidentes de Segurança da Informação", disponível na página de Segurança da Informação do website da Prodest (seguranca.prodest.es.gov.br).

   - ✓ Quando possível, deve-se anexar provas ou evidências do fato, desde que sua produção não descaracterize o cenário afetado ou infrinja a Política de Segurança da Informação da Prodest ou qualquer legislação em vigor.
   - ✓ Apenas na impossibilidade de envio do formulário de registro de incidentes, deve-se enviar e-mail para "segurança.informacao@prodest.es.gov.br" (informando na mensagem todos os dados solicitados no formulário), ou entrar em contato com o setor de atendimento da Prodest, através do telefone (27) 3636-7200.

2) São considerados incidentes de segurança da informação quaisquer eventos que violem ou coloquem em risco a CONFIDENCIALIDADE, INTEGRIDADE, DISPONIBILIDADE, AUTENTICIDADE ou LEGALIDADE de informações pertencentes, processadas ou custodiadas pela Prodest, bem como o não cumprimento dos termos desta PSI. São alguns exemplos de incidentes de segurança da informação:

   a) Indisponibilidade total ou parcial de serviços, sistemas, sites, aplicações, equipamentos ou recursos
   b) Uso impróprio, indevido ou não autorizado de ativos de informação (incluindo a própria informação)
   c) Violações ou falhas de controles ou recursos de segurança
   d) Roubo, furto ou perda de dados (incluindo em mídias ou documentos em papel), equipamentos, credenciais
   e) Falhas nas rotinas de segurança patrimonial ou de controle de acesso ao prédio
   f) Entrada e saída não controlada de ativos de informação (equipamentos, documentos confidenciais etc.)
   g) Vazamento ou divulgação não autorizada de informações sigilosas
   h) Existência de ameaça ou iminência de ocorrência de incidente (mesmo que ainda não tenha ocorrido)

3) Quando necessário e se possível, até que os incidentes tenham sido devidamente tratados, deve-se interromper a utilização dos ativos, recursos ou serviços envolvidos nos mesmos, ou mesmo desabilitá-los, visando evitar maiores danos e prejuízos de qualquer natureza.

4) À exceção dos próprios gestores dos ativos envolvidos no incidente, quem o comunicar/registrar não deverá tentar averiguar por conta própria as causas do mesmo ou tentar tratá-lo, bem como não deverá alterar as características do ambiente, dos recursos ou ativos envolvidos no incidente – exceto se previamente autorizado pelos gestores dos ativos envolvidos, ou diante de situação crítica que exija ou justifique intervenção urgente e imediata para se interromper a continuidade de consequências indesejadas ainda em curso ou prestes a ocorrer.

5) Todos os usuários de recursos oferecidos pela Prodest, incluindo os contratantes de seus serviços, devem zelar para que a instalação, configuração ou uso desses recursos, quando sob sua responsabilidade,

   a) Não causem incidentes de segurança que afetem tais recursos
   b) Não permitam práticas abusivas que firam contratos ou que caracterizem mau uso
   c) Não sejam aplicados para o cometimento de atos ilegais que infrinjam qualquer legislação em vigor
   d) Não coloquem em risco a integridade ou disponibilidade de ambientes tecnológicos da Prodest ou de terceiros

   Ocorrendo a incidência de quaisquer das situações acima, e dependendo de sua gravidade, a Prodest poderá imediatamente efetuar a suspensão temporária dos serviços ou recursos disponibilizados, independentemente de aviso prévio, até que o usuário elimine a causa que motivou a suspensão.

6) A Prodest não será responsável por incidentes de segurança da informação resultantes de atos não solicitados ou não autorizados efetuados por seus clientes, parceiros, conveniados ou prestadores e fornecedores de produtos ou serviços, e nem pelas consequências provocadas por ações criminosas ou não autorizadas realizadas utilizando-se recursos tecnológicos da Prodest.

7) O fluxo interno de tratamento de incidentes de segurança da informação deve se dar conforme definido no anexo "PSI–ANEXO-004 – Tratamento de incidentes de segurança da informação".

DESENVOLVIMENTO E ADOÇÃO DE SISTEMAS E AMBIENTES

1) A adoção ou desenvolvimento de ambientes e sistemas, sejam tecnológicos ou não, tenham sido contratados, adquiridos, ou desenvolvidos pela própria Prodest, deverá ser previamente avaliada pelas áreas usuárias, em conjunto com todos os administradores dos ambientes envolvidos, para que se leve em consideração as melhores práticas de segurança da informação aplicáveis aos mesmos, de forma a garantir que sejam seguros "*por design*" e "*por padrão*".

2) Todos os requisitos de segurança de ambientes, sistemas ou quaisquer outros ativos ou recursos de informação devem ser identificados previamente à implementação dos mesmos e deverão ser testados na fase de avaliação ou desenvolvimento, confirmados na fase de homologação, e continuamente reavaliados durante sua utilização.

3) Ambientes de desenvolvimento, testes e homologação devem ser segregados entre si e dos ambientes de produção, de forma que impeçam acessos não autorizados a qualquer desses ambientes e o amplo e irrestrito acesso de desenvolvedores aos ambientes de produção. Entretanto, os ambientes de desenvolvimento, testes e homologação poderão consumir e ter acesso aos conteúdos disponibilizados nos ambientes de produção, desde que tais acessos não coloquem em risco a integridade, performance e demais aspectos de segurança dos ambientes de produção.

GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO

1) Deve ser realizada, anualmente, uma análise de riscos de segurança nos ativos de informação envolvidos nos processos mais críticos da Prodest e do seu datacenter, seguida da execução dos planos de tratamento necessários.

2) Mudanças em processos, serviços, equipamentos, sistemas ou ambientes, sejam tecnológicos ou não, devem, sempre que possível, ser precedidas de análises de riscos que identifiquem possíveis impactos relacionados à segurança da informação, visando garantir a aplicação das medidas que se fizerem necessárias.

3) Planos de contingência, recuperação de desastres e resposta a incidentes de segurança da informação devem ser elaborados, testados e atualizados periodicamente, visando garantir, no mínimo, a continuidade dos serviços mais críticos quando da ocorrência de eventos que afetem sua disponibilidade.

4) Áreas que executem atividade ou processo em atendimento a esta PSI, ou que realizem outros procedimentos relacionados à segurança da informação, devem elaborar e manter atualizados documentos que os normatizem.

5) Cabe à área de Segurança da Informação ajudar a definir, conceber, elaborar, implementar, revisar e efetuar a análise crítica da governança, diretrizes, políticas, normas, auditorias, ambientes, processos, procedimentos, contratações, produtos e serviços que afetem a segurança das informações pertencentes, custodiadas ou processadas pela Prodest.

PENALIDADES

1) Penalidades às violações desta PSI serão aplicadas conforme a gravidade do ato cometido, podendo variar de mera advertência verbal ou notificação escrita à aplicação das sansões previstas em contratos, estatutos e outros regulamentos, além das legislações trabalhista, civil, criminal e demais leis específicas aplicáveis.

2) Nos casos envolvendo empregados e servidores (incluindo comissionados e servidores cedidos), caberá à diretoria decidir pela abertura de Processo Administrativo Disciplinar interno, dependendo da gravidade da violação cometida.

3) Independentemente da adoção das medidas acima, caso sejam cometidas violações consideradas delitos ou crimes perante a legislação brasileira, a Prodest preservará as evidências e cooperará com as autoridades competentes.

SOBRE ESTA POLÍTICA DE SEGURANÇA

1) Esta PSI não pretende abranger todas as diretrizes necessárias. Assim, deverão ser observadas, de forma complementar e conforme as possibilidades, as exigências das normativas internas da Prodest e da legislação vigente aplicável, bem como as melhores práticas definidas nas normas nacionais e internacionais relacionadas à SI.

2) A Prodest poderá admitir flexibilizar ou mesmo abrir mão de determinadas exigências desta PSI, temporária ou permanentemente e mediante motivo justificável, sem desobrigar-se de seus princípios, para, sempre no interesse da segurança, adequá-la às necessidades ou condições de cada situação ou relação contratual específica. Tais exceções ou concessões não devem ser tratadas como prerrogativas para posteriores descumprimentos desta PSI e, sempre que possível, devem ser expressamente formalizadas.

3) É de responsabilidade de cada cliente, parceiro, prestador de serviço ou qualquer outro tipo de usuário externo da Prodest elaborar, implementar e gerir suas próprias políticas, recursos, sistemas e ativos de SI. Esta PSI foi concebida para utilização exclusiva pela Prodest, não devendo ser adotada como modelo para aplicação fora de seus ambientes.

4) Novos estagiários, comissionados, empregados e servidores públicos cedidos à Prodest devem, antes de iniciarem suas atividades, ser submetidos a uma breve apresentação sobre Segurança da Informação, na qual lhes serão apresentados os principais pontos de atenção desta PSI e, ao final, serão encaminhados ao departamento de Recursos Humanos para assinatura do "Termo de Compromisso", que deverá permanecer arquivado em suas pastas funcionais.

5) Gestores devem conhecer e disseminar esta PSI e fomentar a cultura da segurança da informação, orientando suas equipes a lerem e cumprirem-na, reportarem incidentes de segurança e efetuarem críticas e sugestões de melhoria que possam aumentar a segurança das informações pertencentes, processadas ou custodiadas pela Prodest.

6) Devido ao caráter evolutivo dos tópicos contemplados nesta PSI, seu conteúdo está sujeito a constantes alterações, sem aviso prévio ou posterior, razão pela qual sua última versão deve sempre ser consultada antes de serem tomadas decisões atreladas ao seu conteúdo.

ANEXOS

DOCUMENTO	ATUALIZAÇÃO	FORMATO	TAMANHO
PSI-ANEXO-002 - Acesso às redes da Prodest	23/11/2018	PDF	552 Kb
PSI-ANEXO-003 - Classificação da Informação	30/04/2014	PDF	528 Kb
PSI-ANEXO-004 - Tratamento de incidentes de segurança da informação	20/11/2018	PDF	527 Kb
PSI-ANEXO-005 - Fornecimento de dados a terceiros	22/02/2024	PDF	382 Kb

CONTATOS ÚTEIS

- ✓ Página de Segurança da Informação no site da Prodest: segurança.prodest.es.gov.br
- ✓ Contato para assuntos relacionados à Segurança da Informação: segurança.informacao@prodest.es.gov.br
- ✓ Setor de atendimento da Prodest (Helpdesk): atendimento@prodest.es.gov.br / (27) 3636-7200

GLOSSÁRIO

ANÁLISE DE RISCOS	Ação que visa identificar quais ameaças são relevantes em determinado processo ou ambiente e identificar os riscos associados. Compreende quatro principais objetivos: identificar ativos e seus valores; determinar vulnerabilidades e ameaças; determinar quais ameaças e riscos têm maior impacto; equilibrar o custo de um incidente e o custo das medidas de segurança.
APLICAÇÃO	Aplicativo, app, sistema, programa, software, incluindo aqueles acessados via Internet (ex.: Gmail, Twitter, Facebook, módulo de consulta de informações de CNH no website do DETRAN).
ATIVO DE INFORMAÇÃO	Tudo que contenha ou afete, direta ou indiretamente, a informação que se pretende proteger. Por exemplo: software, sistemas, aplicações, ambientes, equipamentos, redes etc. – incluindo a própria informação.
AUTENTICIDADE	Garantia de que a informação criada ou modificada vem mesmo da fonte anunciada, ou seja, de que o autor da informação é realmente quem diz ser.
CONFIDENCIALIDADE	Garantia de que somente pessoas autorizadas terão acesso à informação.
DISPONIBILIDADE	Garantia de que a informação estará pronta para uso (por pessoas autorizadas) quando for necessária.
INCIDENTE DE SEGURANÇA DA INFORMAÇÃO	Evento ou ocorrência que comprometa ou ameace a confidencialidade, integridade, disponibilidade, autenticidade ou legalidade de dados ou informações pertencentes à Prodest ou tratados ou custodiados por ela. Descumprimento de termos desta PSI.
INTEGRIDADE	Garantia de que a informação mantém as características originais estabelecidas por seu proprietário, ou seja, de que não foi modificada ou alterada de forma indevida.
LEGALIDADE	Quando a informação é criada ou utilizada respeitando a legislação vigente.
PERÍMETRO DE SEGURANÇA	Divisa entre locais que podem ser acessados, de locais cujo acesso é restrito ou proibido.
RASTREABILIDADE	Capacidade de traçar a origem, o histórico, a aplicação ou a localização de um item (informação, acesso, identidade de um usuário, local ou equipamento de onde foi efetuado um determinado acesso etc.) através de consulta ou cruzamento de informações previamente registradas.
RISCO	Potencial de uma determinada ameaça explorar uma ou mais vulnerabilidades.
SEGURO POR DESIGN	Quando a arquitetura, o design e a implementação de um software são concebidos de forma a protegê-lo e a proteger as informações que ele processa, além de resistir a ataques.
SEGURO POR PADRÃO	Nenhum software atingirá uma segurança perfeita. Portanto, os desenvolvedores devem considerar a possibilidade de haver falhas de segurança. Para minimizar os danos que ocorrem quando invasores miram nessas falhas restantes, a configuração padrão do software deve aumentar a segurança. Por exemplo, o software deve ser executado com o privilégio mínimo necessário, e os serviços e os recursos que não sejam amplamente necessários devem ser desabilitados por padrão ou ficar acessíveis apenas para uma pequena parte dos usuários.
TOKEN	Dispositivo eletrônico gerador de senhas temporárias. Variantes: smart card, smartphone com aplicativo que gere senhas temporárias.
USUÁRIO	Qualquer pessoa ou ente público ou privado que estabeleça qualquer tipo de relação com a Prodest, seja formal ou informal, independentemente de sua duração. Ou seja, seus estagiários, comissionados, empregados, prestadores de serviço, fornecedores, parceiros, clientes (incluindo cidadãos que utilizem seus serviços ou ativos), servidores públicos a ela cedidos por outros órgãos.