DESENVOLVE SP
A AGÊNCIA DO EMPREENDEDOR

POLÍTICA DE SEGURANÇA CIBERNÉTICA

1. OBJETIVO

A Política de Segurança Cibernética tem como objetivo atender a Resolução nº 4.893, de 26 de fevereiro de 2021, do Conselho Monetário Nacional (CMN), e estabelecer os princípios, conceitos, valores e práticas que devem ser adotados pelo Desenvolve SP para garantir a proteção das informações tratadas pela instituição.

2. CONTEÚDO

Princípios, conceitos, valores e práticas adotados pelo Desenvolve SP para garantir a proteção das informações tratadas pela instituição.

3. FINALIDADES

- Proteger a imagem da instituição e a de seus clientes;
- Proteger os sistemas e os dados da instituição e de seus clientes contra acessos indevidos e modificações não autorizadas, assegurando, ainda, que as informações estarão disponíveis a todas as partes autorizadas, sempre que demandadas;
- Identificar violações de Segurança Cibernética, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes, ameaças e vulnerabilidades nos ambientes físicos e lógicos, objetivando a mitigação dos riscos cibernéticos e a correta resposta a incidentes;
- Garantir a disponibilidade dos recursos que suportam os negócios, protegendo os processos críticos de interrupções inaceitáveis causadas por ataques cibernéticos e vulnerabilidades na segurança;
- Atender os requisitos legais, regulamentares e as obrigações contratuais pertinentes à atividade da instituição;
- Conscientizar, educar e treinar os colaboradores, a partir dos conceitos desta Política de Segurança Cibernética, incluindo também outras normas e procedimentos internos aplicáveis à Segurança Cibernética em suas atividades diárias;
- Estabelecer um Plano de Ação e Resposta a Incidentes (Pari) relacionado à Segurança Cibernética.

4. CONCEITOS

A Segurança Cibernética constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo seu compartilhamento de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

4.1 Conceitos adotados neste documento

- **Política de Segurança Cibernética (PSC);**
- **Política de Segurança da Informação (PSI):** documento que complementa esta PSC;
- **Plano de Continuidade de Negócios (PCN)**;
- **Confidencialidade**: garantia de que a informação é acessível somente às pessoas autorizadas;
- **Integridade**: salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;
- **Riscos Cibernéticos**: riscos de ataques cibernéticos, oriundos de *malware*, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets) e fraudes externas, desprotegendo dados, redes e sistemas da instituição, causando danos financeiros e de reputação consideráveis.

4.1.1 Malwares

- **Vírus**: *software* que causa danos à máquina, rede, *softwares* e banco de dados;
- **Cavalo de Troia**: aparece dentro de outro *software* e cria uma porta para a invasão do computador;
- ***Spyware***: *software* malicioso para coletar e monitorar o uso de informações;
- ***Ransomware***: *software* malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

4.1.2 Engenharia social

- ***Pharming***: direciona o usuário para um *site* fraudulento, sem o seu conhecimento;

- ***Phishing***: *links* transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial, para obter informações confidenciais;
- ***Vishing***: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
- ***Smishing***: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;
- **Acesso pessoal**: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

4.1.3 Fraudes externas e invasões

Realização de operações por fraudadores, utilizando-se de ataques às plataformas de negócios, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

4.1.4 Ataques DDoS e Botnets

Ataques visando negar ou atrasar o acesso aos serviços ou sistemas da empresa. No caso dos Botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e enviar *spam* ou vírus, ou inundar uma rede com mensagens, resultando na negação de serviços.

4.1.5 Outros conceitos

- Backup de dados: atividade que gera uma cópia dos dados armazenados em diferentes localidades;
- Criptografia: ciência que define princípios e técnicas para transformação da informação, da sua forma original, para outra ilegível, de forma que a mensagem possa ser conhecida apenas por seu destinatário, tornando-a difícil de ser lida por alguém não autorizado;
- Computação / armazenamento “em nuvem”: termo utilizado para descrever uma rede de servidores. A nuvem não é uma entidade física, mas uma vasta rede de servidores remotos que são conectados e operam como um único ecossistema. Estes servidores podem ser responsáveis por armazenar e

gerenciar dados, executar aplicativos ou fornecer conteúdo ou serviços, como transmissão de vídeos, webmail, software de produtividade ou mídias sociais. Em vez de acessar arquivos e dados do local ou de um computador pessoal, o usuário pode acessá-los online, pela internet.

5. APLICABILIDADE

A Política de Segurança Cibernética é aplicável a todas as unidades e colaboradores (funcionários, estagiários e terceiros) do Desenvolve SP, bem como aos fornecedores de serviços de computação em nuvem.

Terceiros em uso das informações e de ativos do Desenvolve SP também devem estar em conformidade para com as diretrizes desta Política. Como “terceiros” estão incluídos, entre outros:

- Prestadores de serviços de apoio e manutenção;
- Prestadores de serviços de operações relacionadas a sistemas de Tecnologia da Informação (TI), serviços de coleta de dados, operações de atendimento, entre outros;
- Clientes;
- Consultores;
- Auditores;
- Pessoal temporário, estagiários, menores aprendizes e outros contratados de curta duração.

Principais fornecedores de tecnologia de sistema de negócios e processamento de dados do Desenvolve SP:

- Partec Tecnologia LTDA: fornecedora do sistema $Finance, sistema transacional dos negócios e de gestão corporativa do Desenvolve SP;
- Companhia de Processamento de Dados do Estado de São Paulo (Prodesp): empresa provedora de Data Center, para acesso à rede corporativa e aos sistemas de negócios, por meio da nuvem;
- Prodesp: fornecedora de licenças Microsoft e de serviços de desenvolvimento e manutenção de aplicações.

6. PRINCÍPIOS

A proteção e privacidade de dados da própria instituição e dos clientes refletem os valores do Desenvolve SP e reafirmam o compromisso com a melhoria contínua da eficácia do processo de Segurança Cibernética para proteção de sistemas e dados.

Quanto à coleta e ao tratamento dos dados, são práticas determinantes:

- São coletadas de forma ética e legal, para propósitos específicos e devidamente informados;
- Somente são acessadas por pessoas autorizadas e capacitadas para o seu uso adequado;
- Podem ser disponibilizadas às empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossas diretrizes de segurança e privacidade de dados;
- As informações constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais ou contratuais, somente são fornecidas aos próprios interessados, mediante a solicitação formal, seguindo os requisitos legais vigentes.

7. DIRETRIZES CORPORATIVAS

A Política de Segurança Cibernética estabelece diretrizes que buscam complementar a Política de Segurança da Informação (PSI) do Desenvolve SP, para assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pela instituição e por seus clientes.

O Desenvolve SP atua frequentemente no aperfeiçoamento de suas aplicações e de seus códigos fontes, onde executa análises DAST/SAST, efetuadas pelo fornecedor do sistema transacional dos negócios e de gestão corporativa.

O Desenvolve SP deve implementar controles para reduzir as vulnerabilidades dos processos da instituição a incidentes e também para atender aos demais objetivos de segurança cibernética, incluindo:

- a autenticação;
- a criptografia;
- a prevenção e a detecção de intrusões;
- a prevenção de vazamento de informações (da instituição e de clientes);
- a realização periódica de testes e varreduras para detecção de vulnerabilidades

e softwares maliciosos.

O sistema transacional dos negócios e de gestão corporativa do Desenvolve SP fica hospedado em estrutura externa de fornecedor de *Data Center*.

O Desenvolve SP possui controle de rastreabilidade das alterações ocorridas no banco de dados do sistema transacional dos negócios e de gestão corporativa, por meio de armazenamento de *logs* transacionais. Tais arquivos são retidos desde a implementação do sistema, ocorrida em 2010.

O Desenvolve SP monitora, através de relatórios e comunicação com seu fornecedor de *Data Center*, todos os eventos relacionados com a segurança de seu perímetro de rede. Este monitoramento ocorre mensalmente. Incidentes relevantes identificados são registrados e tratados.

O Desenvolve SP estruturou, como complemento desta PSC e de sua PSI, o Plano de Ação e Resposta a Incidentes (Pari), conforme o Capítulo II deste MNP, contendo controles e procedimentos de monitoramento, reporte e resposta a incidentes, incluindo análise da causa e do impacto, com foco principal nos ambientes de produção dos fornecedores de *Data Center* (acesso pela nuvem) e fornecedor do sistema transacional dos negócios e de gestão corporativa.

O Desenvolve SP deve implementar em sua PSI classificação dos dados e das informações quanto a relevância e nível de confidencialidade. O grau de relevância deve variar entre baixo, médio e alto, de acordo com a importância da informação. O cumprimento da Política de Segurança Cibernética é de responsabilidade de todos os colaboradores e dos prestadores de serviços, conforme suas atribuições, os quais devem obedecer às seguintes diretrizes:

- Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada;
- Prover a adequada classificação da informação, sob os critérios de confidencialidade, disponibilidade e integridade;
- Assegurar que os recursos utilizados para o desempenho de sua função sejam utilizados apenas para as finalidades aprovadas pelo Desenvolve SP;
- Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;
- Garantir a continuidade do processamento das informações críticas de negócios;

- Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo;
- Comunicar imediatamente à Genet.2 quaisquer descumprimentos da Política de Segurança Cibernética.

8. ESTRUTURA DE GERENCIAMENTO

O Desenvolve SP conta com uma unidade (Sunet) ou função específica para planejar, estabelecer, executar e monitorar as atividades e controles relacionados com Segurança das Informações e Segurança Cibernética. Esta função se reporta diretamente à Diretoria da instituição.

As atividades e os controles de Segurança Cibernética executados sob a responsabilidade dessa unidade objetivam assegurar que os procedimentos operacionais de segurança sejam desenvolvidos, implementados e mantidos ou modificados de acordo com os objetivos estabelecidos por esta Política de Segurança Cibernética.

Os subitens abaixo descrevem os principais processos de gerenciamento.

8.1 Gestão de acessos às informações

Os acessos às informações devem ser controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente, aprovados pelo gestor da informação, e cancelados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço.

8.2 Proteção do ambiente

São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações que garantem a segurança na infraestrutura tecnológica de redes locais e internet, por meio de um gerenciamento efetivo no monitoramento, tratamento e respostas aos incidentes, para minimizar o risco de falhas e assegurar a administração segura de redes de comunicações, incluindo a gestão de serviços contratados de processamento e armazenamento de dados e informações em nuvem.

8.3 Segurança física e lógica

Os equipamentos e as instalações de processamento de informação críticos ou sensíveis são mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

Os requisitos de segurança de sistemas de informação são identificados e acordados antes do seu desenvolvimento e/ou de sua implementação, para que assim possam ser protegidos, visando a manutenção de sua confidencialidade, integridade e disponibilidade.

Os colaboradores e terceiros do Desenvolve SP devem ser treinados periodicamente sobre os conceitos de Segurança da Informação, por meio de um programa efetivo de conscientização, executado sob a responsabilidade da Sunet.

8.4 Continuidade de negócios

O processo de gestão de continuidade de negócios relativo a segurança da informação é implementado para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, a um nível aceitável, por meio da combinação de requisitos como operações, funcionários-chave, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres.

Incluem-se, nesse processo, a continuidade de negócios relativos aos serviços providos aos clientes do Desenvolve SP.

Tais diretrizes são detalhadas no MNP – Plano de Continuidade de Negócios, incluindo as diretrizes para a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios.

O Desenvolve SP deve assegurar que suas políticas e planos de continuidade de negócios contemplem:

- O tratamento dos incidentes relevantes relacionados com segurança das informações;
- Os procedimentos a serem seguidos no caso da interrupção de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados, abrangendo cenários que considerem a substituição da empresa contratada e o reestabelecimento da operação normal do Desenvolve SP;

- Os cenários de incidentes considerados nos testes de continuidade de negócios. Exemplos:
  - Falta de energia elétrica, localizada ou não, por motivos diversos (exemplos: fornecedor de energia, curto-circuito, falha interna, etc.);
  - Falta de água, localizada ou não;
  - Interdição da entrada do prédio do ambiente principal;
  - Problemas com telefonia: PABX e/ou *link* de comunicação com Telefônica;
  - Indisponibilidade de *link* com o fornecedor de *Data Center*, afetando a comunicação com banco de dados (prédio do Desenvolve SP com o prédio do fornecedor de *Data Center*);
  - Indisponibilidade de *link* do fornecedor de *Data Center* com internet, ou seja, toda a rede funcionando, mas sem acesso à internet, por falhas do *link* do fornecedor de *Data Center*;
  - Indisponibilidade da infraestrutura física e/ou tecnológica do fornecedor de *Data Center*;
  - Outros incidentes/acidentes (exemplo: incêndio).
- A execução de testes formais de continuidade de negócios, abrangendo os principais cenários de incidentes e interrupções de serviços, que podem impactar na continuidade das operações da instituição.

8.4.1 Continuidade de negócios em serviços de computação em nuvem

Os procedimentos adotados pelo Desenvolve SP para gerenciamento de riscos, no tocante à continuidade de negócios, devem contemplar:

- O tratamento previsto para mitigar os efeitos dos incidentes relevantes e da interrupção dos serviços de processamento, armazenamento de dados e de computação em nuvem contratados;
- O prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos;
- A comunicação tempestiva à Diretoria das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, que configurem uma situação de crise pelo Desenvolve SP, bem como das providências para o reinício das suas atividades.

8.5 Serviços de processamento, armazenamento de dados e computação em nuvem

Em conformidade com a Resolução CMN nº 4.893/2021, para a contratação de serviços de terceiros para processamento, armazenamento de dados e computação em nuvem, o Desenvolve SP assegura um procedimento efetivo para a aderência às regras previstas na regulamentação em vigor.

Nas relações contratuais com os fornecedores de serviços que processam dados da instituição, o Desenvolve SP exige termos de confidencialidade, incluindo a obrigação da tempestividade da comunicação de ocorrência de incidentes relevantes, caso tais incidentes ocorram com os dados do Desenvolve SP e de seus clientes.

Caso receba comunicações de incidentes com dados sensíveis de seus clientes, o Desenvolve SP deve efetuar o registro, a análise da causa e do impacto, bem como o controle dos efeitos destes incidentes relevantes para as atividades de seus clientes, abrangendo, inclusive, os detalhes e demais informações recebidas da empresa prestadora de serviços ao Desenvolve SP.

9. UTILIZAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

Para os fins do disposto nesta Política, os serviços de computação em nuvem abrangem a disponibilidade ao Desenvolve SP, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

- Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam ao Desenvolve SP implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela instituição ou por ela adquiridos;
- Implantação ou execução de aplicativos desenvolvidos pelo Desenvolve SP, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços; ou
- Execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

O Desenvolve SP, previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, deve adotar

procedimentos que contemplem:

- A adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas;
- A verificação da capacidade do potencial prestador de serviço de assegurar:
- o cumprimento da legislação e da regulamentação em vigor;
- o acesso do Desenvolve SP aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
- a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
- a sua aderência a certificações exigidas pelo Desenvolve SP para a prestação do serviço a ser contratado;
- o acesso do Desenvolve SP aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;
- o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- a identificação e a segregação dos dados dos clientes do Desenvolve SP por meio de controles físicos ou lógicos;
- a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes do Desenvolve SP.

Na avaliação da relevância do serviço a ser contratado, o Desenvolve SP deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado, levando em conta, inclusive, a classificação das informações, realizada em conjunto com o desenvolvimento desta Política.

No caso da execução de aplicativos por meio da internet, o Desenvolve SP deve assegurar que o potencial prestador dos serviços adote controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada ao Banco Central do Brasil em até dez dias após a contratação dos serviços.

A comunicação ao Bacen sobre a contratação deve conter as seguintes informações:

- A denominação da empresa contratada;
- Os serviços relevantes contratados;
- A indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, no caso de contratação no exterior.

A Sunet pode vetar ou impor restrições para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem quando constatar, a qualquer tempo, a inobservância do disposto nesta Política, estabelecendo prazo para a adequação dos referidos serviços.

9.1 Contratos com fornecedores de serviços em nuvem

Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever:

- A indicação dos países e da região em cada país onde os serviços podem ser prestados e os dados podem ser armazenados, processados e gerenciados;
- A adoção de medidas de segurança para a transmissão e armazenamento dos dados;
- A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações do Desenvolve SP e dos clientes da instituição;
- A obrigatoriedade, em caso de extinção do contrato, de:
  - transferência dos dados citados ao novo prestador de serviços ou ao Desenvolve SP;
  - exclusão dos dados pela empresa contratada substituída, após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos.
- O acesso do Desenvolve SP às:
  - informações fornecidas pela empresa contratada, visando verificar o cumprimento do disposto na Política;
  - informações relativas às certificações e aos relatórios de auditoria especializada;
  - informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados.

- A obrigação de a empresa contratada notificar o Desenvolve SP sobre a subcontratação de serviços relevantes para a instituição;
- A permissão de acesso do Desenvolve SP à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;
- A obrigação de a empresa contratada manter o Desenvolve SP permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor;
- A obrigação de notificação prévia do responsável do Desenvolve SP sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:
  - a empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo Desenvolve SP;
  - a notificação prévia deve ocorrer inclusive na situação em que a interrupção seja motivada por inadimplência do Desenvolve SP.

Todos os contratos com fornecedores de serviços em nuvem (atuais e futuros) devem atender ao disposto nesta Política. No caso de contratos em vigência no momento da divulgação e/ou revisão desta Política e que não estão aderentes ao disposto neste documento, os mesmos devem ser atualizados para estar em plena conformidade com esta Política de Segurança Cibernética. A Sunet e a Gepin.2 estão envolvidas na avaliação de aderência de todos os contratos para com esta Política.

Atualmente o Desenvolve SP possui um fornecedor classificado como provedor de serviço de processamento de dados em nuvem:

- Prodesp: empresa provedora de *Data Center*, para acesso à rede corporativa e aos sistemas de negócios.

O contrato de prestação de serviço deste fornecedor será atualizado de forma a contemplar todas as diretrizes desta Política.

10. PROCEDIMENTOS E CONTROLES

O Desenvolve SP adota procedimentos e controles para reduzir as vulnerabilidades a incidentes e atender aos demais objetivos de Segurança Cibernética. Os principais procedimentos estão descritos nos subitens abaixo.

10.1 Procedimentos e controles de autenticação

O Desenvolve SP adota controles de autenticação, tanto na rede como nos aplicativos de negócios (exemplos: *Active Directory* para acesso à rede; senha e usuário adicional para acesso os sistemas corporativos).

As senhas para acesso ao sistema transacional dos negócios e de gestão corporativa devem atender a critérios de complexidade, que protegem a descoberta da mesma.

10.2 Procedimentos e controles de criptografia e proteção de código-fonte

O Desenvolve SP usa a criptografia em todas as senhas de suas aplicações.

O sistema transacional dos negócios e de gestão corporativa possui *software* de versionamento para guarda de código fonte, bem como possui *backup* tanto do código fonte como também das versões dos instaladores das aplicações. O fornecedor deste sistema investe em treinamento de metodologia em desenvolvimento seguro para seus colaboradores e também usa programas para análises SAST e DAST de suas aplicações.

10.3 Procedimentos e controles de prevenção e detecção de intrusão

Os fornecedores de *Data Center* do Desenvolve SP e o fornecedor do sistema transacional dos negócios e de gestão corporativa devem implementar recursos em seus dispositivos de rede e nos sistemas, de forma que permitam a detecção de intrusos, bem como a resposta a incidentes.

O Desenvolve SP possui ferramentas de prevenção e detecção de intrusões (IPS e IDS).

O Desenvolve SP deve executar, com periodicidade semestral, testes de penetração/intrusão – Pentest – em um conjunto de aplicações de maior relevância para a operação da instituição, com o objetivo de identificar, preventivamente, possíveis vulnerabilidades que possibilitem intrusões maliciosas.

Após a realização de cada execução dos testes de penetração semestrais, deverão

ser elaborados relatórios identificando:

- As possíveis vulnerabilidades identificadas;
- As recomendações para correção e eliminação das vulnerabilidades identificadas e/ou a minimização dos riscos associados a essas vulnerabilidades;
- O planejamento das ações, com a definição de prazos e responsabilidades, para o atendimento das recomendações apresentadas.

Os relatórios semestrais devem ser submetidos à aprovação da Superintendência de Desenvolvimento de Negócios e Tecnologia.

10.4 Procedimentos e controles de prevenção de vazamento de informações

O Desenvolve SP tem como diretriz prevenir e detectar todo e qualquer vazamento de informações sensíveis em seu ambiente de tecnologia. Para isso, adota processos e utiliza recursos que mitigam eventos de vazamento de dados, tais como a utilização de ferramentas de *Data Loss Prevention* (DLP).

O fornecedor de *Data Center* atua com Suíte Apex Trend, conexão somente via VPN Lan-To-Lan.

O Desenvolve SP passa a adotar solução de *Endpoint Protection*, com os objetivos principais de:

- Prevenção contra *malwares*, especialmente os *ransomwares*;
- Prevenção contra mecanismos de engenharia social;
- Prevenção à perda de dados – de forma a evitar o vazamento deliberado ou acidental de ativos digitais da instituição e de dados e informações sensíveis;
- Defesa contra ameaças – com base em listas de objetos suspeitos.

A solução deve ser instalada em todos os equipamentos – *desktops* e *notebooks* – utilizados pelos colaboradores do Desenvolve SP por meio de agentes específicos para a manutenção das proteções mencionadas.

A Gerência de Infraestrutura de TI do Desenvolve SP é a responsável pela instalação e manutenção dos agentes da solução de *EndPoint Protection* em todos os equipamentos e é responsável também pelo gerenciamento e o controle centralizado da execução da solução.

10.5 Realização periódica de testes e varreduras para detecção de vulnerabilidades

O Desenvolve SP adota processos e utiliza recursos que visam minimizar as vulnerabilidades em seu ambiente, tais como a utilização da ferramenta Nessus.

O *software* Nessus é uma ferramenta de análise de vulnerabilidades, desenvolvido para verificar redes de computadores, aplicativos, *switches*, computadores, servidores e outros equipamentos. Dentre os diversos tipos de identificadores de vulnerabilidades destacam-se a varredura de portas, a enumeração de rede e o *service scanners*.

Esta análise de vulnerabilidades é realizada trimestralmente. O relatório gerado pela análise é enviado para a Suric. As correções necessárias no ambiente tecnológico, com base no relatório, são implementadas pela Genet.2 e pelo fornecedor de *Data Center* (quando as vulnerabilidades identificadas forem de responsabilidade deste fornecedor). Estas vulnerabilidades, bem como as correções, são registradas em um chamado de tratativa de Incidentes de Segurança da Informação.

O fornecedor de *Data Center* possui ferramentas para a realização de testes periódicos de detecção de vulnerabilidades. O resultado destes testes é enviado para a Sunet, para o devido acompanhamento das vulnerabilidades e ações corretivas para as mesmas. O fornecedor de *Data Center* atua conforme estruturação da ISO 27001, garantindo os testes obrigatórios anualmente e atuação no Plano de Ação.

Adicionalmente, são realizados testes de vulnerabilidade no sistema transacional dos negócios e de gestão corporativa, semestralmente. É efetuado o registro das vulnerabilidades e tratativas dadas às mesmas**.**

10.6 Proteção contra *softwares* maliciosos

O Desenvolve SP utiliza programas específicos para se proteger contra *softwares* maliciosos, dentre eles o antivírus McAfee, as ferramentas VirusScan Enterprise e AntiSpyware Enterprise e a solução Apex One da Trend Micro.

Os fornecedores do sistema transacional dos negócios e de gestão corporativa e do *Data Center* possuem mecanismos de proteção contra vírus maliciosos.

Para toda estrutura de servidores do fornecedor de *Data Center,* há camada de antivírus.

10.7 Mecanismos de rastreabilidade

O Desenvolve SP possui controles específicos, incluindo os voltados para a rastreabilidade da informação, que buscam garantir a segurança das informações sensíveis. Há controles e procedimentos de geração de *logs* transacionais de todos os bancos de dados dos ambientes de produção dos sistemas corporativos.

Para o sistema transacional dos negócios e de gestão corporativa, os *logs* registram os acessos aos sistemas, abertura e fechamento de telas e inclusão/alteração de dados.

10.8 Controles de acesso e segmentação da rede de computadores

Os dados sendo trafegados entre a o fornecedor de *Data Center* e o Desenvolve SP são protegidos contra acesso indevido.

Para a comunicação entre o fornecedor de *Data Center* e o Desenvolve SP, a estrutura de *link* é formada por Link Lan-to-Lan dedicado ao cliente e com dupla abordagem de operadoras, onde em toda estrutura o cliente possui uma VLAN dedicada para segmentação de seu tráfego até a chegada do *firewall*.

Adicionalmente, a estrutura de redes e segurança do Data Center é composta por equipamentos redundantes, onde na camada externa, juntamente com os roteadores de borda, há solução de proteção contra ataques DDoS. A camada de *firewall* é formada por equipamentos que trabalham da Camada 3 à Camada 7 com as devidas regras de liberação ou bloqueio. Juntamente a essa solução, há também os recursos de IPS/IDS e WAF para prevenção de ataques e vazamento de informações por meio de acessos indevidos.

O Desenvolve SP possui *firewall* em seu *link* de conexão de contingência da Intragov.

10.9 Procedimentos que garantem a manutenção de cópias de segurança dos dados e das informações

O Desenvolve SP executa *backups* diários incrementais, bem como semanais e mensais integrais, dos dados produtivos de seus sistemas corporativos. Este *backup* é executado pelo fornecedor de *Data Center*, e fica armazenado em um local distante dos *data-centers* de produção.

A base de dados produtiva do sistema transacional dos negócios e de gestão corporativa é enviada ao fornecedor por meio de *Secure File Transfer Protocol* (SFTP),

como *backup*. Este envio de dados via SFTP utiliza protocolo criptografado e requer autenticação para acesso.

10.10 Procedimentos de monitoramento e controle de incidentes de segurança

O processo de monitoramento e resposta a incidentes está descrito no Capítulo Plano de Ação e Resposta a Incidentes, deste MNP.

11. MONITORAMENTO DE SEGURANÇA, ACESSOS E ATIVIDADES

11.1 Acessos e atividades

- Atividades realizadas no ambiente informatizado do Desenvolve SP e que gerem impacto no negócio da instituição devem ser registradas (gerar *log* para consulta quando necessário);
- A geração de *logs* (trilhas de auditoria) para atividades com impacto no negócio deve abranger os seguintes sistemas e plataformas:
  - Rede (sistema de arquivos);
  - Aplicativos de negócios e portais;
  - Bancos de dados;
  - Demais plataformas avaliadas como relevantes (por possuírem informações sensíveis ao negócio do Desenvolve SP, de acordo com a classificação das informações).
- No mínimo, as seguintes informações devem ser identificadas e registradas em trilhas de auditoria:
  - Usuário que realizou o acesso;
  - Atividades realizadas no acesso (leitura, escrita, deleção, etc.);
  - Informações que foram alteradas (com histórico da informação anterior à modificação);
  - Plataforma utilizada no acesso.
- O acesso de profissionais de TI ao ambiente de produção dos sistemas e plataformas tecnológicas do Desenvolve SP, quando aplicável, deve gerar trilhas de auditoria. Tais trilhas não podem ser manipuláveis pelos executores das transações.

12. TREINAMENTOS PERIÓDICOS EM SEGURANÇA DA INFORMAÇÃO

O Desenvolve SP deve dispor de mecanismos / treinamentos para disseminação da cultura de segurança da informação, incluindo:

- Palestra e/ou workshop sobre segurança da informação, com frequência anual e/ou conforme a necessidade de atualização de seus colaboradores;
- Envio periódico de e-mails, a todos os colaboradores, contendo diretrizes de segurança da informação;
- Disseminação de Cartilha de Segurança da Informação e Cibernética, contendo as principais diretrizes destes temas, a todos os colaboradores da instituição;
- A prestação de informações a clientes e fornecedores sobre precauções na utilização de produtos e serviços financeiros (de acordo com Cartilha de Segurança da Informação).

13. RESPONSABILIDADES

13.1 Da Diretoria

A Diretoria do Desenvolve SP deve se comprometer com a melhoria contínua dos procedimentos e controles relacionados nesta Política, os quais devem ser objeto de pautas recorrentes de reuniões de membros da Diretoria juntamente com o responsável por Segurança da Informação.

É responsabilidade da Diretoria suprir a Sunet com os recursos mínimos necessários para que a unidade possa atender às premissas e quesitos constantes nesta PSC e no Plano de Ação e Resposta a Incidentes.

Adicionalmente, a Diretoria deve revisar e aprovar a PSC, sempre que uma nova versão for enviada à sua apreciação.

13.2 Da Sunet

É responsabilidade do Gerente e do Coordenador de TI:

- Planejar e implementar os recursos de segurança cibernética, de forma a atender aos objetivos de segurança definidos nesta PSC;
- Manter os recursos de segurança cibernética (ferramentas, pessoas e processos) atualizados e disponíveis, de forma a atender os preceitos definidos nesta PSC;

- Prover relatórios periódicos sobre os incidentes de segurança cibernética e as respectivas respostas dadas a estes. Tais relatórios devem ser enviados para a Diretoria Responsável do Desenvolve SP;
- A Sunet é também responsável por atualizar a PSC e submetê-la à aprovação da Diretoria, sempre que necessário;
- Adicionalmente, criar uma pauta periódica de reuniões com a Diretoria, referente a discussões sobre melhorias em aspectos de segurança cibernética e acompanhamento do desenvolvimento do Pari.

13.3 Dos colaboradores do Desenvolve SP

- Atender às normas e procedimentos contidos nesta PSC e na PSI, de forma a permitir que a instituição mantenha os níveis de segurança esperados;
- Reportar à Sunet todo e qualquer evento ou fato relevante que possa, de alguma forma, impactar na segurança cibernética dos recursos da instituição e de seus clientes, conforme disposto no item 14;
- Estar em completa aderência para com esta Política de Segurança Cibernética;
- Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição para o trabalho;
- Responder pelo uso exclusivo e intransferível de suas senhas de acesso à rede, e-mail, sistema operacional e demais sistemas;
- Buscar o conhecimento necessário para a correta utilização dos recursos de hardware e software disponibilizados pela instituição;
- Relatar prontamente à Sunet qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, confidencialidade, mau funcionamento, identificação de vírus maliciosos, etc.;
- Assegurar que as informações e dados de propriedade do Desenvolve SP não sejam disponibilizados a terceiros, a não ser com autorização por escrito do responsável da unidade.

13.4 Dos gestores e líderes

- Apoiar e zelar pelo cumprimento desta Política, servindo como modelo de conduta para os colaboradores sob a sua gestão;
- Disseminar, entre os usuários sob sua responsabilidade, os princípios e

procedimentos de Segurança da Informação;

- Notificar imediatamente a Sunet sobre quaisquer vulnerabilidades, ameaças e quebra de segurança das informações;
- Relatar imediatamente à Sunet, Gepin.1 e Diretoria, a violação dos princípios ou procedimentos de segurança da informação realizadas por colaboradores sob sua responsabilidade.

13.5 Da Gepin.1

- Atribuir, na fase de contratação e de formalização dos contratos individuais de trabalho CLT, estágio, prestação de serviços ou de parceria, a responsabilidade do cumprimento da Política de Segurança Cibernética. O documento "Cartilha de Segurança da Informação", que faz referência às principais diretrizes de Segurança da Informação, deve ser recebido por todos os colaboradores da instituição, antes do início de suas atividades;
- Gerenciar a participação dos colaboradores do Desenvolve SP nos treinamentos que forem realizados de Segurança da Informação / Cibernética.

13.6 Da Sunet – Genet.1 e Genet.2

- Configurar os equipamentos e sistemas para o cumprimento dos requisitos desta Política de Segurança Cibernética;
- Aplicar os controles de segurança da informação em novos sistemas e serviços informatizados;
- Realizar o *backup* periódico das informações da instituição, de forma que estas possam ser recuperadas quando necessário;
- Implementar ferramentas para a proteção de todos os ativos de informação da instituição contra códigos / vírus maliciosos;
- Realizar inspeções periódicas de configurações técnicas, bem como tratar as inconsistências / riscos identificados;
- Promover a conscientização dos colaboradores em relação à relevância da segurança da informação, por meio de treinamentos (ao menos semestralmente) e notificações periódicas (ao menos mensalmente);
- Validar a aplicação os controles de segurança da informação em novos sistemas e serviços informatizados;

- Manter o registro dos incidentes de segurança da informação (identificação de vírus, *trojans*, acessos indevidos, etc.). O registro deve descrever o incidente e a tratativa dada para a resolução do mesmo;
- Realizar, periodicamente, revisões de avaliação e monitoramento para a validação dos itens desta Política de Segurança Cibernética, de forma a identificar possíveis desvios existentes;
- Notificar os líderes das unidades e a Diretoria, no caso de não conformidade com esta Política;
- Desenvolver, em conjunto com as unidades, Planos de Ação para a mitigação e resolução de não conformidades em relação a esta Política;
- Revisar a Política de Segurança Cibernética e submetê-la para aprovação da Diretoria, pelo menos uma vez por ano.

14. COMUNICAÇÃO DE IRREGULARIDADE

Todo e qualquer indício de irregularidade ou de descumprimento da PSC deve ser imediatamente comunicado à Sunet, por meio do endereço de e-mail sup.tecnologia@desenvolvesp.com.br.

As ocorrências serão avaliadas pela Sunet e pelos gestores das unidades relacionadas a estes incidentes.

15. DÚVIDAS

Quaisquer dúvidas sobre a Política de Segurança Cibernética e suas diretrizes devem ser esclarecidas com a Sunet, através do e-mail SegurancaTI@desenvolvesp.com.br.

16. DIVULGAÇÃO

- Esta Política deve ser divulgada a todos os colaboradores do Desenvolve SP e estar disponível na rede da instituição para consulta a qualquer momento;
- O Desenvolve SP deve divulgar, aos prestadores de serviços e outras pessoas que possam acessar informações de sua propriedade ou custódia, um resumo contendo as linhas gerais desta Política.

17. APROVAÇÕES E REVISÕES

- A Política de Segurança Cibernética deve ser aprovada pela Diretoria Colegiada e, previamente à aprovação pelo Conselho de Administração, deve ser apresentada ao Comitê de Auditoria. A revisão deve ocorrer, no mínimo, anualmente.