RESOLUÇÃO Nº 02/2025/DIRETORIA EXECUTIVA/ISP

Institui a Política de Segurança da Informação, a qual dispõe sobre as normas de proteção das informações da INVEST SP.

A DIRETORIA EXECUTIVA DA AGÊNCIA PAULISTA DE PROMOÇÃO DE INVESTIMENTOS E COMPETITIVIDADE – INVEST SP, no exercício da competência que lhe confere o artigo 17, inciso VI do Estatuto Social vigente, bem como o deliberado na 1ª Reunião Ordinária de 2025:

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação no âmbito AGÊNCIA PAULISTA DE PROMOÇÃO DE INVESTIMENTOS E COMPETITIVIDADE – INVEST SP.

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 2º Esta Política de Segurança da Informação tem por finalidade estabelecer normas gerais visando o tratamento adequado e a proteção das informações da INVEST SP, e que devem ser seguidos por todos os empregados, diretores, conselheiros e demais que estiverem submetidos à abrangência da INVEST SP.

Art. 3º Os procedimentos e normas estabelecidos são aplicáveis a todas as áreas da INVEST SP, que estão sujeitas as várias interferências, como tecnológicas e físicas, a fim de prevenir eventuais danos.

CAPÍTULO II

APLICAÇÃO GERAL

Seção I

Do Gerenciamento da Informação

Art. 4º As informações que estão em constante circulação dentro da INVEST SP são ativos valiosos para a Instituição e, por esta razão, devem ser protegidas contra qualquer tipo de dano que possa ocorrer.

Art. 5º Este normativo deve ser entendido como um conjunto de ações a serem efetuadas para que seja alcançada uma condição de segurança, mediante a observância dos direcionais descritos na Política que visa reduzir a exposição aos riscos e ameaças, através do conhecimento de possíveis vulnerabilidades.

Art. 6º Para efeitos dessa Política, considera-se:

I - Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato

II - Documento: unidade de registro de informações, qualquer que seja o suporte ou formato

III - Informação Pessoal: aquela relacionada à pessoa natural identificada ou identificável

IV - Tratamento da Informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

V - Disponibilidade: toda vez que for necessária, a informação deverá estar disponível para todas as pessoas que necessitem utilizá-la;

VI - Confidencialidade: a informação deve ser tratada de maneira que somente pessoas autorizadas tenham acesso a ela;

VII - Integridade: as alterações que venham a ser necessárias nas informações só devem ser realizadas por pessoas autorizadas;

VIII - Autenticidade: a informação deve se manter original ao seu propósito, independentemente de como for utilizada;

IX - Privacidade: os locais onde informações sensíveis são manipuladas ou tratadas terão seus acessos restringidos e controlados por sistemas eletrônicos.

Seção II

Inventário de Ativos

Art. 7º O principal objetivo da segurança da informação é proteger os sistemas de informação contra usuários não autorizados, contra modificações, vazamentos e acessos não autorizados de dados, e as informações podem estar contidas em:

I - Mídia digital, Documentos Eletrônicos e *E-mails*;

II - Sistemas de informação / bases de dados;

III - Documentos Escritos e Impressos;

IV - Equipamentos de Armazenamento de Dados;

V - Informações Verbais;

VI - Internet;

VII - *Cloud* (*Microsoft, Google e Datacenter* externo);

Seção III

Tratamento da Informação

Art. 8º O tratamento da informação tem como objetivo criar uma hierarquia para os vários tipos de informações que circulam dentro da INVEST SP, de forma que somente a informação necessária estará disponível para o colaborador de acordo com o papel que desempenha dentro da Instituição;

Art. 9º Para obter um gerenciamento das informações durante o seu ciclo de vida (criação, manuseio, transporte, armazenamento e descarte), é necessário tratar a informação em diferentes níveis:

I - Confidencial: são as informações que devem ser mantidas em caráter de sigilo, disponíveis apenas para pessoas autorizadas, e que influem diretamente na responsabilidade de sigilo e continuidade das atividades da Instituição, caso sejam divulgadas indevidamente; e

II - Pública: informação isenta de qualquer restrição para divulgação e que podem ser acessadas tanto pelos empregados quanto pelo público.

Parágrafo único. São tratadas como confidencial, para os fins desta Política, quaisquer informações consideradas sujeitas a possibilidade de restrição nos termos da Lei de Acesso à Informação.

Seção IV

Do Funcionamento

Art.10. As áreas fiscalizadoras e respectivas competências no cumprimento do normativo serão:

I- Infraestrutura:

a) Controlar acessos;

b) Monitorar Ativos e Gestão da Rede;

c) Controlar acesso e atribuições dos Banco de Dados e Repositórios.

d) Conferir os equipamentos devolvidos quando do desligamento

II - Gestão de Pessoas:

a) Realizar, no processo de admissão, o preenchimento do formulário de requerimento de acessos a ser encaminhado para área de Infraestrutura;

b) Providenciar a geração de crachá de identificação e acesso físico ao edifício e às instalações da INVEST SP, de acordo com o setor de trabalho do contratado;

c) Comunicar o desligamento do empregado para área de Infraestrutura retirar os acessos concedidos;

d) Recolher o crachá e solicitar a devolução dos equipamentos disponibilizados para execução das atividades na Instituição para área de Infraestrutura.

Seção V

Das Normas Gerais

Art.11. Os equipamentos disponibilizados para o desenvolvimento das atividades profissionais devem ser utilizados de forma ética e em conformidade com as normas de conduta e segurança estabelecidas, em particular com a Política de Segurança da Informação, reservando o direito

da INVEST SP em controlar e monitorar os conteúdos e formas de uso, considerando que todos os recursos e equipamentos devem ser utilizados para o desenvolvimento do trabalho.

Art.12. As portas de conectividade (USB) de todos os equipamentos estão acessíveis, entretanto, só podem ser utilizadas para finalidades do trabalho e mediante conhecimento e autorização da supervisão direta.

Art.13. Equipamentos particular e privados, como computadores ou quaisquer dispositivos portáteis que possam armazenar e/ou processar dados, devem ser usados em via de exceção, mediante conhecimento e autorização prévia da supervisão direta, para os quais devem ser observados todos os direcionais dessa Política de Segurança da Informação, não devendo armazenar dados da INVEST SP nos referidos dispositivos, para o qual deve ser utilizado, exclusivamente, a nuvem da INVEST SP para armazenamento.

Art.14. Os recursos de comunicação internos da INVEST SP podem incluir o uso da internet, telefones fixos e celulares corporativos, bem como correio eletrônico, e devem ser utilizados sempre de maneira ética e para finalidade do trabalho.

Art.15. Caberá à Diretoria a definição de quais sites e redes sociais poderão ser acessados pelos colaboradores.

Art.16. Caberá à área de Infraestrutura o monitoramento de acesso não autorizado na rede, e a sua informação ao seu gestor responsável, para que as devidas medidas sejam tomadas.

Art.17. Todos os e-mails terão um aviso automático de que a mensagem pode conter informação confidencial, e que se o destinatário estiver errado a mesma deve ser apagada devendo ser excluído sem conteúdo.

Art.18. A realização de *downloads* d e *softwares* e aplicativos só será permitida quando for estritamente necessária ao trabalho do empregado, mediante conhecimento e autorização da supervisão direta e com suporte da área de Infraestrutura. .

Art.19. Alguns ambientes de trabalho da INVEST SP, como recepção e corredores de acesso por exemplo, serão monitorados por câmeras.

Seção VI

Das Normas dos Usuários

Art.20. Todos os usuários de informações da INVEST SP se comprometem a:

I - Executar todas as normas definidas neste documento de Política de Segurança da Informação durante o período em que estiver vinculado à INVEST SP;

II - Sempre que possível, propor ideias e melhorias que de alguma forma possam vir a agregar novas medidas de segurança para toda a Instituição;

III - Comunicar imediatamente ao seu superior qualquer incidente que venha a acontecer, e que

possa prejudicar a segurança da informação, para que este tome as medidas cabíveis com relação ao problema;

IV - Não executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede da INVEST SP;

V - Não executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a inoperância de serviços;

VI - Alterar suas senhas, sempre que suspeitar de qualquer comprometimento de seu sigilo;

VII - Cuidar adequadamente de todos os equipamentos disponibilizados pela INVEST SP, preservando o uso, limpeza e a correta utilização para finalidade do trabalho.

VIII - Impedir o uso de seu equipamento por outras pessoas e sempre bloquear o equipamento ao se ausentar de seu posto de trabalho;

IX - Manter os *notebooks* com a trava de segurança, e tomar os cuidados necessários quando a locomoção do equipamento; e

X - Não utilizar quaisquer recursos ou equipamentos disponibilizados para fins diversos daqueles necessários ao desempenho da sua atividade.

Art.21. É estritamente proibido divulgar quaisquer informações para pessoas não ligadas às atividades da INVEST SP, salvo quando devidamente autorizado pelos gestores.

Art.22. Com relação ao tratamento de informações são responsáveis pela observância os diretores, empregados, conselheiros e todos os que estiverem submetidos à abrangência da INVEST SP.

Art.23. Todos aqueles que receberem informações confidenciais deverão mantê-las e resguardá-las em proteção, bem como limitar seu acesso, controlar quaisquer cópias de documentos, dados e reproduções que porventura sejam extraídas das mesmas.

§1º Nenhuma das informações confidenciais poderá ser repassada para terceiros sem consentimento por escrito dos gestores responsáveis na INVEST SP.

§2ºQualquer revelação das informações confidenciais deverá estar de acordo com os termos e condições estabelecidos neste documento.

§3ºAs informações confidenciais somente poderão ser utilizadas para fins de execução dos trabalhos, devendo ser resguardas de forma estrita, a não ser para aqueles que eventualmente também estejam autorizados a recebê-las.

Art.24. Qualquer vazamento ou quebra de sigilo das informações deverão ser informados, prontamente, aos gestores responsáveis.

Seção VII

Das Normas de Mesa e Telas Limpas

Art.25. Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em qualquer dispositivo, eletrônico ou não, a fim de reduzir riscos de fraudes, violações, roubos e até acessos não autorizados de informações que possam ser obtidas por documentos, livros,

manuais, mídias, arquivos e outras fontes de informação que estão sendo deixadas à vista.

Art.26. As informações devem ser protegidas e tratadas com um alto grau de segurança e confidencialidade, não sendo recomendado manter informações sensíveis e/ou sigilosas expostas nas mesas, mas sim mantidas, quando não estiverem sendo utilizadas, armazenadas nas gavetas chaveadas.

Art.27. Ao usar uma impressora coletiva, após inserir a senha para impressão, recolher o documento impresso imediatamente.

Art.28. Para evitar qualquer dano a equipamentos e/ou documentos, não realizar refeições sobre as mesas de trabalho.

Art.29. Os terminais de computador não devem ser deixados logados quando não houver um operador (usuário) junto dos mesmos, e devem ser protegidos por senhas e outros controles quando não estiverem em uso.

Seção VII

Das Normas de Acesso Físico

Art.30. O acesso ao espaço físico da INVEST SP possui controle de entrada com abertura por crachá (cartão) ou biometria.

Art.31. Demais setores que requerem proteção deverão manter as portas fechadas.

Art.32. Os crachás e senhas são compatíveis com as funções desempenhadas por cada um de seus portadores e pela sensibilidade das informações contidas e tratadas em cada um dos espaços da INVEST SP.

Art.33. Visitantes e terceiros devem ser atendidos e contidos na área da recepção ou nas salas de reunião.

Parágrafo único. Somente quando devidamente autorizado pelos gestores, o visitante ou terceiro poderá adentrar na área interna e, para isso, deverão estar portando o crachá de visitante e permanentemente acompanhados por um empregado ou representante da INVEST SP.

Seção VIII

Das Normas para Senhas

Art.34. A senha é o meio pelo qual o usuário poderá validar seus dados para acessar os sistemas da INVEST SP, correios eletrônicos e perfis nas máquinas, e para tanto, devem obedecer às seguintes práticas:

I - Alterar a senha inicial utilizando letras, números, maiúsculas, minúsculas e caracter especial

com o mínimo de 8 (oito) posições;

II - Não utilizar senhas com letras ou números repetidos ou em sequência;

III - Não utilizar informações pessoais fáceis de serem obtidas, como data de nascimento, nomes e sobrenomes, números de telefone, e outros dados de fácil identificação;

IV - Digitar as senhas rapidamente, tomando cuidado com a observação de terceiros; e

V - Não permitir o reuso da última senha cadastrada.

Art.35. As senhas são de uso pessoal e intransferível.

Art.36. O usuário fica responsável pelas consequências de atos causados pelo uso indevido de suas senhas.

Art.37. Caso o empregado seja desligado da Instituição, o responsável pelo setor de Recursos Humanos enviará um e-mail para área de Infraestrutura solicitando que o login e senha sejam desativados, atualizando o registro nos sistemas de controle da INVEST SP, para fins de verificação.

Seção IX

Das Normas para Infraestrutura

Art.38. Caberá aos responsáveis do departamento de infraestrutura monitorar os acessos à rede e sua utilização, observando os seguintes aspectos:

I - Controle e monitoramento de acessos/permissões;

II - Monitoramento de *firewall*;

III - Monitoramento nos servidores;

IV - Monitoramento de versões de *software*;

V - Monitoramento do tráfego;

VI - Ativos utilizados e compartilhamentos;

VII - *Downloads* efetuados;

VIII - Endereço dos Protocolos de Internet - IPs; e

IX - Monitoramento dos serviços de *Cloud (Microsoft, Google e Datacenter* externo).

Seção X

Das Normas de Uso de Ferramentas de Suporte e Desenvolvimento

Art.39. Caberá à Diretoria definir o tipo de acesso que cada membro da equipe possuirá, de acordo com as funções específicas de cada empregado.

Art.40. Caberá à área de Infraestrutura o controle e atribuição dos dados de acesso das ferramentas descritas abaixo:

I - Sistemas Gerenciadores de Banco de Dados;

II - Sistemas internos;

III - Repositório de dados e

IV - Serviços *Cloud.*

Seção XI

Das Penalidades

Art.41. O descumprimento e a inobservância das legislações vigentes, desta Política, bem como dos demais normativos da INVEST SP, sujeita o empregado à sanção disciplinar, de acordo com o vínculo empregatício, e conforme os compromissos assumidos no Contrato de Trabalho e respectivo Termo de Sigilo e Responsabilidade.

Art.42. Despesas originadas pelo não cumprimento dos procedimentos de segurança citados nessa norma, deverão ser assumidas, exclusivamente, pela parte causadora após a devida apuração.

CAPÍTULO III

DA TRANSPARÊNCIA

Art.43. A Política de Segurança da Informação da INVEST SP em nada conflita com a transparência e com o direito fundamental de acesso a informação nos pontos aplicáveis à Instituição, considerando que continuarão sendo divulgadas e fornecidas todas as informações necessárias ao atendimento dos dispositivos legais que abrangem os temas citados, cuidando o presente normativo apenas de corroborar com a proteção, autenticidade, integridade e disponibilidade da informação ao direcionar o tratamento adequado e seguro por todos os empregados, diretores, conselheiros e demais que estiverem submetidos à abrangência da Instituição.

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

Art.44. Ficam revogados:

I - a Norma de utilização de *notebooks* - Portaria 04/10 da Diretoria Executiva.

II - a Norma de posse e uso de celular - Portaria 05/10 da Diretoria Executiva;

Art.45. Os casos omissos dessa Política serão resolvidos pela Diretoria Executiva da INVEST SP, ouvido o Jurídico.

Art.46. Esta Política entrará em vigor a partir da data de sua publicação.

São Paulo, na data da assinatura digital.

RUI GOMES DA SILVA JUNIOR
Presidente

ANEXO I – PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA

As diretrizes deste documento deverão ser utilizadas quando ocorrer algum tipo de incidente que afete a segurança da informação da INVEST SP.

Destina-se a garantir uma resposta rápida, eficaz e ordenada a uma violação de segurança da informação.

A natureza exata de um incidente e seu impacto não pode ser prevista com certeza e, portanto, é importante que o bom senso seja usado ao decidir as ações a serem tomadas.

No entanto, pretende-se que as estruturas apresentadas aqui sejam úteis para permitir que as ações corretivas sejam tomadas mais rapidamente e com base em informações precisas.

1. IDENTIFICAR E ANALISAR O INCIDENTE

Um incidente pode ser identificado inicialmente de várias formas e através de várias fontes diferentes, dependendo da natureza e localização do incidente.

Alguns incidentes podem ser detectados automaticamente por meio de ferramentas de software usadas pela INVEST SP ou por empregados que notam atividades incomuns. Outros podem ser notificados por um terceiro, como um cliente, fornecedor ou agência de aplicação da lei que tenha conhecimento de uma violação.

É normal que haja uma demora entre a ocorrência do incidente e sua identificação real. Um dos objetivos de uma abordagem proativa à segurança da informação é reduzir esse período de tempo. O fator mais importante é que o procedimento de resposta a incidentes deve ser iniciado o mais rápido possível após a identificação para que uma resposta efetiva possa ser dada.

Uma vez que o incidente tenha sido identificado, uma avaliação de impacto inicial deve ser realizada a fim de decidir a resposta apropriada. Esta avaliação de impacto deve medir:

A extensão do impacto na infraestrutura de TI, incluindo computadores, redes, equipamentos e acomodações;

Os ativos de informação que podem estar em risco ou foram comprometidos;

A duração provável do incidente, ou seja, quando pode ter começado;

As unidades da instituição afetadas e a extensão do impacto para elas

Indicação inicial da causa provável do incidente.

Essas informações devem ser documentadas para que haja um entendimento claro, disponível para uso atual ou em uma revisão posterior.

Uma lista de ativos de informação incluindo dados pessoais, operações negociais, produtos, serviços, equipes e processos de suporte que possam ter sido afetados pelo incidente deve ser criada juntamente com uma avaliação da extensão do impacto.

Uma vez notificado de um incidente, as seguintes situações servem como diretrizes para determinar se uma resposta formal a um incidente deve ser iniciada:

Existe uma perda real ou potencial, significativa, de informação, incluindo dados pessoais;

Há uma interrupção, significativa, real ou potencial, nas operações da instituição;

Existe um risco, significativo, para a reputação da instituição;

Qualquer outra situação que possa causar impacto significativo para a organização.

Um plano deve ser criado para que seja oferecida uma resposta de nível inferior pelos meios normais de gerenciamento.

A comunicação do incidente deve ser registrada e atender as seguintes responsabilidades:

Comunicação e envolvimento da Diretoria e outras partes interessadas de alto nível;

A Diretoria deverá preparar as reuniões e registrar as ações e decisões;

Avaliar a extensão e o impacto do incidente;

Fornecer as informações para a equipe;

Definir a abordagem da comunicação para manter as partes afetadas informadas;

2. GESTÃO, MONITORAMENTO E COMUNICAÇÃO DE INCIDENTES

Uma vez que uma resposta apropriada ao incidente tenha sido identificada, a equipe precisa ser capaz de gerenciar a resposta, monitorar o status do incidente e assegurar que a comunicação efetiva esteja ocorrendo em todos os níveis.

É vital que as comunicações efetivas sejam mantidas entre todas as partes envolvidas na resposta ao incidente.

3. CONTENÇÃO. ERRADICAÇÃO, RECUPERAÇÃO E NOTIFICAÇÃO DE INCIDENTES

O primeiro passo será tentar impedir que o incidente se agrave, ou seja, contenha-o. No caso de um surto de vírus, isso pode implicar na desconexão das partes afetadas da rede, e para um ataque de hackers, pode envolver a desativação de certos perfis ou portas no firewall ou até mesmo a desconexão completa da rede interna da Internet. As ações específicas a serem executadas dependerão das circunstâncias do incidente.

Nota: se for considerado provável que seja necessário coletar provas digitais que serão posteriormente usadas, devem ser tomadas precauções para garantir que tais evidências permaneçam admissíveis. Isso significa que os dados relevantes não devem ser alterados deliberadamente ou por acidente.

Se houver suspeita de crime no incidente, registros precisos devem ser mantidos das ações tomadas e as evidências coletadas de acordo com as diretrizes forenses. Os princípios destas diretrizes são os seguintes:

Princípio 1 – Não altere nenhum dado. Se alguma coisa for feita que resulte na alteração dos dados do sistema, isso afetará qualquer processo judicial subsequente.

Princípio 2 – Acesse somente os dados originais em circunstâncias excepcionais. Um especialista treinado usará ferramentas para fazer uma cópia de qualquer dado armazenado na memória, seja em um disco rígido, memória ou cartão SIM de um telefone. Toda a análise terá local certo na cópia, e a original nunca deverá ser tocada, a menos que em circunstâncias excepcionais.

Princípio 3 – Sempre mantenha a trajetória da auditoria realizada. As ferramentas forenses farão isso automaticamente, mas isso também se aplica às primeiras pessoas em cena. Tirar fotografias e vídeos é incentivado desde que nada tenha sido tocado.

Princípio 4 – A pessoa responsável deve assegurar que as diretrizes sejam seguidas. Antes da chegada de um especialista, as informações básicas devem ser coletadas. Isso pode incluir:

o Fotografias ou vídeos de mensagens ou informações relevantes;

o Registros manuais escritos da cronologia do incidente;

o Documentos originais, incluindo registros de quem os encontrou, onde e quando;

o Detalhes de quaisquer testemunhas.

Uma vez coletadas, as evidências serão mantidas em um local seguro, onde não podem ser adulteradas.

Em seguida, uma ideia clara do que aconteceu precisa ser estabelecida. A extensão do incidente e as implicações devem ser averiguadas antes que qualquer tipo de ação de contenção.

Ações para corrigir os danos causados pelo incidente (ex. exclusão de malware) devem passar pelo processo de gerenciamento de alterações. Essas ações devem ter como objetivo corrigir a causa atual e impedir que o incidente ocorra novamente. Quaisquer vulnerabilidades que tenham sido exploradas como parte do incidente devem ser identificadas. Dependendo do tipo de incidente, a erradicação pode, às vezes, ser desnecessária.

Durante a fase de recuperação, os sistemas devem ser restaurados à sua condição anterior ao incidente, embora as ações necessárias devam ser realizadas para resolver quaisquer vulnerabilidades que foram exploradas como parte do incidente.

A notificação de um incidente de segurança da informação e perda de dados resultante é um assunto delicado que deve ser tratado com cuidado e com total aprovação da Diretoria. A equipe decidirá, com base em pareceres jurídicos e de outros especialistas e com uma compreensão total do impacto do incidente, a notificação necessária a ser feita.

Os registros coletados como parte da resposta a incidentes podem ser exigidos para quaisquer investigações dos órgãos reguladores.

4. ATIVIDADE PÓS-INCIDENTE

A Diretoria decidirá, com base nas informações mais recentes, o ponto em que as atividades de resposta devem cessar e a equipe deve ser desativada. Observe que a recuperação e execução de planos podem continuar além desse ponto, mas sob um controle menos formal.

Essa decisão deve basear-se nos seguintes critérios:

A situação foi totalmente resolvida ou é razoavelmente estável;

O ritmo de mudança da situação diminuiu a um ponto em que poucas decisões são necessárias;

A resposta apropriada está bem encaminhada e os planos de recuperação estão progredindo;

O grau de risco para o negócio diminuiu para um ponto aceitável;

Responsabilidades legais e regulamentares imediatas foram cumpridas.

Se a recuperação do incidente estiver em andamento, a Diretoria deve definir as próximas ações a serem tomadas, que podem incluir:

Reuniões menos frequentes da equipe, dependendo das circunstâncias;

Informar todas as partes envolvidas de que a equipe permanece;

Garantir que toda a documentação do incidente está certa;

Solicitar que todos os empregados não envolvidos em trabalhos futuros retornem às tarefas normais.

Todas as ações tomadas devem ser registradas. Os registros relevantes do incidente serão examinados pela Diretoria para garantir que eles estejam completos e precisos.

Uma revisão pós-incidente mais formal será realizada em um momento a ser decidido pela alta

direção de acordo com a magnitude e a natureza do incidente.

ANEXO II – RETENÇÃO E ELIMINAÇÃO DE DADOS E DOCUMENTOS

A INVEST SP deve manter os documentos físicos e digitais armazenados em conformidade com requisitos contratuais, regulatórios e demais bases legais aplicáveis.

É importante que esses registros sejam protegidos contra perda, destruição, falsificação, acesso não-autorizado e liberação não-autorizada ou qualquer outro incidente de Segurança da Informação.

Para isso, uma variedade de controles é usada, como backups, controle de acesso e criptografia.

1. Retenção de Documentos Físicos e Digitais

Os documentos serão retidos pelo período necessário ao cumprimento da obrigação contratual e obrigação legais ou regulatórias relacionadas, bem como o exercício de direitos em processos administrativos ou judiciais, destacando alguns exemplos:

Para registros de ordem tributária, trabalhista e previdenciária, a INVEST SP poderá se reservar no direito de mantê-los armazenados até o fim do prazo prescricional estipulado em lei ou do período de retenção definido em legislação específica.

Informações coletadas para (i) gestão do RH, como por exemplo, gerenciamento de tempo de trabalho, salários, benefícios, contribuições previdenciárias e impostos; férias, licenças e ausências; (ii) gestão de carreira, como treinamentos, avaliações, experiência profissional; (iii) administração do RH, como relatórios e pesquisa; (iv) saúde ocupacional, como atestados médicos, prontuário médico, atestados de saúde ocupacional e todos os demais relacionados à saúde do empregado; e (v) gestão de viagens de negócios, como informações para organização de viagens (preferências, local etc.); CNH e despesas: podem ser retidos após o término do contrato de trabalho, estágio ou contrato de trabalho temporário até o fim do período prescricional para cumprir os períodos legais de armazenamento definidos na legislação trabalhista, previdenciária ou tributária.

Após o período de retenção, os documentos e dados poderão ser descartados com segurança.

2. Descarte Após Expiração do Período de Retenção

Em todos os casos os seguintes procedimentos devem ser observados:

Identificação dos locais de armazenamento, como exemplo:

· Servidores próprios;

· Servidores de terceiros;

· Contas de e-mail;

· Dispositivos da INVEST SP;

· Dispositivo Pessoais;

· Armazenamento de cópias de segurança; e/ou

· Arquivos em papel.

Descarte de Dados Pessoais em Ambientes Físicos e Digitais

Sempre que o descarte de informações for necessário, este deve ser realizado com o emprego de medidas que impossibilitem a sua reconstrução, seja ele físico ou digital.

Registro de Descarte

Recomenda-se que seja mantido registro das operações de descarte dos principais documentos.

Descarte de Documentos Físicos: devem triturados e dispostos em lixo específico, disponível pelo departamento responsável pelo descarte (não devem ser dispostos em lixo comum).

Documento assinado eletronicamente por **Rui Gomes Da Silva Junior**, **Presidente**, em 30/01/2025, às 12:11, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

A autenticidade deste documento pode ser conferida no site https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0054502218** e o código CRC **C8736EFA**.