POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA AGÊNCIA PEIXE VIVO

DIRETORIA GERAL INTERINA
Rúbia Santos Barbosa Mansur

GERÊNCIAS
Berenice Coutinho Malheiros dos Santos - Gerente de Administração e Finanças (GEAF) Rúbia Santos Barbosa Mansur - Gerente de Integração (GI)
Taís Passos Guimarães (Interina) - Gerente de Gestão Estratégica (GEE)
Jacqueline Evangelista Fonseca (Interina) - Gerente de Projetos (GP)

CONSELHO DE ADMINISTRAÇÃO DA AGÊNCIA PEIXE VIVO
Gustavo Henrique Costa Simões - Presidente Interino Jadir Silva de Oliveira
Luiz Cláudio de Castro Figueiredo
Nelson Cunha Guimarães Kenede
Antônio dos Reis
Valter Vilela Cunha
Heloisa Cristina França Cavallieri

CONSELHO FISCAL DA AGÊNCIA PEIXE VIVO
André Amaral Horta - Presidente
Renato Júnio Constâncio
Tarcísio de Paula Cardoso

ELABORAÇÃO DE CONTEÚDO:
Thiago Henrique Cordeiro Alves – Analista de Desenvolvimento Sênior G4F SOLUÇÕES CORPORATIVAS LTDA
Contrato nº 037/2022
Ato Convocatório nº. 21/2022 CG
nº. 028/ANA/2020

REVISÃO:
Alison Moreira – Coordenador de Tecnologia da Informação
Taís Passos Guimarães (Interina) - Gerente de Gestão Estratégica (GEE)

1. CONTEXTUALIZAÇÃO

A Política de Segurança da Informação (PSI) da Agência Peixe Vivo (APV) é o documento que orienta e estabelece as diretrizes para a proteção dos ativos de informação criando regras para gerenciar e conscientizar sobre a segurança da informação, com o objetivo de obter maior controle e conformidade de práticas com as normas aplicáveis.

A PSI está baseada nas recomendações da ABNT NBR ISO/IEC 27002:2022, reconhecida mundialmente, e tem como referência a Lei Federal nº 13.709, de 14 de agosto 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). Além disso, foi estrutura a partir do mapeamento de riscos de segurança da informação.

Esta Política será reavaliada anualmente ou sempre que surgirem novos requisitos tecnológicos, corporativos e/ou legais, podendo ser complementada por normas e procedimentos específicos. Elanão excluias demais normas de privacidade e proteção de dados pessoais aplicáveis no âmbito da Agência Peixe Vivo.

As diretivas abaixo refletem os valores institucionais da Agência Peixe Vivo e reafirmam seu compromisso com a melhoria contínua dos processos.

Este documento integra e se alinha com as normas internas que regulamentam aspectos específicos dessas atividades na Agência Peixe Vivo.

2. DEFINIÇÕES

Para os fins desta Política, considera-se:

Informação: reunião ou o conjunto de dados e conhecimentos organizados que possam constituir referências sobre determinado acontecimento, fato ou fenômeno, não se tratando apenas do conteúdo de sistemas de tecnologia da informação ou informatizados.
Colaborador: toda e qualquer pessoa física que possua vínculo com a APV, como contratado peto regime da Consolidação das Leis do Trabalho (CLT), contrato de estágio, contrato de menor aprendiz, bem como membros associados e ocupantes de cargos eletivos da Agência;
Prestador de serviço: toda e qualquer pessoa, física ou jurídica, contratada e que exerça alguma atividade dentro ou fora da Agência;
Usuário: colaborador ou prestador de serviço que tenha acesso autenticado aos sistemas disponibilizados pela Agência para desempenhar determinada função, trabalho ou atividade;
Gestor: pessoa responsável por planejar e dirigir o trabalho de um grupo de colaborador;
Proprietário da informação: pessoa ou organismo que tenha responsabilidade autorizada para controlar a produção, o desenvolvimento, a manutenção, o uso e a segurança de ativos, no caso, por exemplo, informações contidas em documentos eletrônicos elou físicos sistemas de informação, bases de dados e/ou mídias de armazenamento (ISO/IEC 27.001);
Custodiante da informação: aquele que tem a posse, temporária ou definitiva, da informação corporativa (ISO/IEC 27.001);
Acesso: possibilidade de consulta ou reprodução de documentos e arquivos;
Ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos

diretos aos ativos ou prejuízos decorrentes de situações inesperadas;

Incidente de segurança: indício de fraude, sabotagem, desvio, falha, perda ou evento indesejável ou inesperado que tenha probabilidade de comprometer sistemas de informação ou de redes de computadores, ou arquivos físicos.

3. OBJETIVOS

A Política de Segurança da Informação (PSI) da Agência Peixe Vivo tem como objetivos:

I. estabelecer diretrizes e princípios gerais para implementar, manter e melhorar a gestão de segurança da informação na Agência;
II. universalizar a política de segurança junto a funcionários, colaboradores, terceirizados, prestadores de serviços e membros da Agência;
III. tratamentar os dados pessoais na Agência, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade;
IV. criar medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
V. orientar a implementação de controles e processos para garantir o cumprimento das diretrizes estabelecidas;
VI. preservar as informações da Agência Peixe Vivo quanto à:
    a) Integridade: garantir que a informação seja mantida no seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
    b) Confidencialidade: garantir que o acesso à informação ocorra somente por pessoas autorizadas;
    c) Disponibilidade: garantir que os colaboradores e prestadores de serviço autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
    d) Legalidade: procedimentos a segurança da informação precisam estar em conformidade com a LGPD.
    e) Autenticidade: garantir que a informação é proveniente de uma fonte confiável.

Este documento tem como finalidade descrever os conceitos, princípios, objetivos, diretrizes, competências e responsabilidades no âmbito da gestão de riscos de Segurança da Informação na Agência.

Com a finalidade de assegurar a proteção dos dados eletrônicos desta agência, o presente documento também apresenta a Política de Backup e Recuperação de Dados Digitais, na qual se estabelece diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pelas Coordenação de Tecnologia da Informação (DTD) e formalmente definidos como de necessária salvaguarda na Agência Peixe Vivo.

4. PRINCÍPIOS

São princípios da Política de Segurança da Informação da Agência Peixe Vivo.

I. visão abrangente e sistêmica da segurança da informação;
II. treinamento e disseminação do conhecimento como alicerce fundamental para o fomento da Agência;
III. orientação à gestão de riscos e à gestão da segurança da informação;
IV. prevenção e tratamento de incidentes de segurança da informação;
V. articulação entre as ações de segurança cibernética, de defesa cibernética e de proteção de dadose ativos da informação.

5. DESTINATÁRIOS

A presente Política se aplica a todos os membros do Conselho de Administração; do Conselho Fiscal; da Assembleia Geral, empregados, colaboradores, independentemente do nível hierárquico ou da função exercida, estagiários, convidados, parceiros, fornecedores, membros dos Comitês de Bacias hidrográficas, que, no âmbito da relação com a Agência Peixe Vivo, possam acessar as áreas e equipamentos informações arquivos redes e dados de titularidade ou propriedade da APV.

A PSI se aplica à informação em qualquer meio ou suporte e todos os destinatários deverão observar as presentes regras e recomendações em quaisquer operações que possam impactar na segurança das informações na APV.

O não cumprimento das disposições desta PSI sujeitará o infrator as sanções previstas em lei aplicáveis, bem como as demais penalidades regulamentadas no âmbito da Agência Peixe Vivo

6. DIRETRIZES DE MANIPULAÇÃO DE INFORMAÇÕES

Toda informação produzida ou recebida por colaboradores e prestadores de serviço, como resultado da atividade exercida em nome ou para a Agência Peixe Vivo, pertence à referida agência.

É necessário proteger a privacidade das informações pertencentes aos respectivos titulares, que são manipuladas ou armazenadas nos meios sobre os quais a Agência Peixe Vivo tem controle administrativo, observando-se que:

I. as informações devem ser acessadas apenas por pessoas autorizadas e capacitadas para o uso adequado;
II. as informações podem ser disponibilizadas para as empresas contratadas para prestação de serviços, exigindo-se de tais organizações o cumprimento da política e das diretivas de segurança e privacidade de dados da Agência Peixe Vivo;
III. as informações e os dados constantes dos cadastros da Agência Peixe Vivo, bem como outras solicitações que venham a garantir direitos legais, serão fornecidos exclusivamente aos próprios interessados;

Os dados pessoais são coletados, de forma ética e legal, para propósitos específicos e devidamente informados, ao teor da Lei Federal no 13.709, de 14 de agosto de 2018(Lei Geral de Proteção de Dados Pessoais - LGPD).

Todos os colaboradores e prestadores de serviço devem observar exigências e requisitos para manipular informações, haja vista o tipo de conteúdo considerado, sendo que as exigências previstas no documento serão definidas pelo proprietário ou responsável pela informação, seguindo orientações disponíveis nesta PSI. Os proprietários podem atribuir controles adicionais para maior restrição de acesso ou para ampliar a proteção de informações confidenciais ou restritas.

A divulgação de informações confidenciais e/ou restritas para quaisquer pessoas é estritamente proibida, salvo quando previamente autorizada pelo proprietário da informação, sendo que o acesso a informações confidenciais e/ou restritas deve ser, sempre, registrado e monitorado pelo gestor competente.

A reprodução de informações confidenciais e/ou restritas, incluindo a impressão de cópias adicionais, não é permitida salvo quando explicitamente autorizada pelo respectivo proprietário. Trechos, resumos, traduções ou qualquer material derivado

das informações referidas no documento ou resguardadas por direitos autorais não poderão ser elaborados a menos que o proprietário da informação os tenha previamente autorizado. O transporte físico das informações confidenciais e/ou restritas deve seguir as normas correlatas estabelecidas.

Quando as informações confidenciais restritas não forem mais necessárias e quando exigências legais ou regulatórias para a retenção não mais se aplicarem, aquelas deverão ser eliminadas, observando-se que:

I. é proibida a eliminação de documentos contendo dados confidenciais e\ou restritos em latas de lixo ou em depósitos de papel encaminhados para reciclagem;
II. quando não houver disposição contrária ou norma específica, os documentos devem ser eliminados com o uso de picotador/fragmentador.
III. a informação confidencial e/ou restrita armazenada em disquetes, fitas magnéticas ou outras mídias magnéticas computacionais deve ser eliminada via reformatação ou exclusão dos dados, caso o suprimento seja reutilizado na agência;
IV. a depender da avaliação do gestor, o suprimento informático poderá ser definitivamente destruído para proteger as informações confidenciais ou restritas nele existentes.

7. PAPÉIS E RESPONSABILIDADES REFERENTES À SEGURANÇA DA INFORMAÇÃO

É proibido o uso de computadores, equipamentos eletrônicos e demais recursos tecnológicos da Agência Peixe Vivo para:

I. tentar ou obter acesso não autorizado a outro computador, servidor ou rede, incluindo o acesso a informações confidenciais sem autorização explícita do proprietário;
II. burlar quaisquer sistemas de segurança;
III. vigiar secretamente outrem, por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);
IV. interromper serviços, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
V. praticar ou ser cúmplice de atos de violência moral, assédio sexual, perturbação, manipulação ou violação de direitos autorais ou de propriedades intelectuais;
VI. acessar, distribuir ou armazenar material pornográfico, racista ou qualquer outro com conteúdo discriminatório referente a religião, orientação sexual e procedência nacional em claro desrespeito ao ordenamento jurídico pátrio;
VII. violar ou tentar violar a ordem pública;
VIII. utilizar software pirata;

São consideradas violações à Política, a normas ou a procedimentos de segurança da informação, sem prejuízo de atos e omissões outras:quaisquer ações que exponham ou possam expor a Agência Peixe Vivo ou os titulares dos dados em seu poder a perdas e danos, direta ou indiretamente, em claro comprometimento aos ativos de informação;

I. o uso indevido de dados da Agência e divulgação não autorizada de informações, sem expressa e prévia permissão do gestor;
II. o uso de dados, informações, equipamentos, software, sistemas e outros recursos tecnológicos para propósitos ilícitos, que envolva a violação de leis, regulamentos, preceitos éticos, ou queo prestador de serviços tome conhecimento, direta ou indiretamente, no exercício da função.

III. a não comunicação ao gestor imediato de quaisquer descumprimentos a esta Política, a normas ou a procedimentos de segurança da informação que, porventura, o colaborador e/ou prestador de serviços tome conhecimento, direta ou indiretamente, no exercício da função.

Todos os colaboradores, prestadores de serviços e usuários de serviços de rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos computacionais da Agência Peixe Vivo, deverão:

I. conhecer a Política de Privacidade de Dados da Agência, disponibilizada no site da APV;
II. ser orientados, na fase de contratação, sobre os procedimentos e normas relacionados à Segurança da Informação, bem como sobre o uso correto dos ativos a fim de reduzir possíveis riscos;
III. assinar Termo de Responsabilidade sobre a utilização da rede interna (intranet), internet, computadores e e-mail corporativo da Agência Peixe Vivo, de tal forma a assumir o dever de observância às normas nele estabelecidas (ANEXO I);
IV. promover a segurança dos respectivos dados e credenciais de acesso, assumindo responsabilidades como custo diante de informações;
V. seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao manuseio de documentos físicos e ao uso dos recursos computacionais einformacionais da agência;
VI. utilizar, de forma ética, legal e consciente, os recursos computacionais e informacionais da Agência Peixe Vivo;
VII. manter-se atualizado quanto a esta PSI e aos procedimentos e normas a ela relacionados, buscando orientações do seu gestor ou da Coordenação de Tecnologia da Informação da AgênciaPeixe Vivo, sempre que não estiver absolutamente seguro nos processos de aquisição, uso elou descarte de informações.

Cabe a cada gestor, incluindo em relação aos colaboradores e prestadores de serviço sob a sua gestão:

I. exibir postura exemplar no que tange à segurança da informação, servindo como parâmetro e modelo de conduta;
II. informar, preliminarmente à concessão de acesso às informações da agência, dar conhecimento à esta PSI aos colaboradores e prestadores de serviço;
III. adaptar ou, quando não for competente, requerer a adaptação de normas, procedimentose sistemas para atender à PSI — Agência Peixe Vivo.

A Gerência de Gestão Estratégica, através da Coordenação de Tecnologia da Informação, possui os seguintes deveres específicos:

I. testar a eficácia dos controles utilizados e informar aos gestores sobre riscos residuaiseventualmente existentes;
II. implementar e testar, no mínimo anualmente, plano de contingência e continuidade dos principais sistemas e serviços para reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação;
III. registrar todo o uso dos sistemas e serviços visando garantir a disponibilidade e a segurança das informações utilizadas;
IV. acessar, enquanto administradora e operadora dos sistemas computacionais, arquivos e dados de outros usuários apenas quando necessário à execução de atividades operacionais sob sua responsabilidade, tais como manutenção de computadores, realização de cópias de segurança, auditoria e testes nos ambientes;
V. administrar, proteger e testar cópias de segurança dos programas e dados relacionados a processos críticos e

relevantes para a Agência Peixe Vivo;

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

a) as permissões para os logins individuais dos colaboradores são determinadas pelo gestor em conjunto com a Coordenação de Tecnologia da Informação. O colaborador é totalmente responsável pelo uso do seu login

b) as permissões para os logins dos prestadores de serviços são definidas pelo gestor da área contratante, em conjunto com a Coordenação de Tecnologia da Informação. O prestador de serviço é totalmente responsável pelo uso do seu login

VII. proteger continuamente todos os ativos de informações da agência contra códigos maliciosos, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de códigos maliciosos e/ou indesejados;

VIII. diligenciar para que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da Agência;

IX. definir regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da Agência;

X. garantir, da forma mais rápida possível, o bloqueio do acesso de colaborador ou prestadorde serviço em virtudeda rescisão do contrato (de trabalho ou de estágio, conforme o caso) ou do encerramento do mandato eletivo edo término do respectivo contrato de prestação de serviços (prestadores de serviços). Tal bloqueio também abarca as hipóteses de incidente, investigação ou fato outro relativo a colaborador ou prestador de serviço que exija medida restritiva para fins de salvaguarda dos ativos da Agência Peixe Vivo. Todo bloqueio, que se enquadre em uma das supracitadas hipóteses, decorrerá mediante a requisição do gestor imediato do colaborador e/ou do prestador de serviço;

XI. monitorar o ambiente de TI, gerando indicadores e históricos de:

a) uso da capacidade instalada da rede e dos equipamentos;

b) incidentes de segurança (vírus, trojans, furtos, acessos indevidos);

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

XII. propor metodologias e processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação;

XIII. propor e apoiar iniciativas que visem à segurança dos ativos de informação da Agência;

XIV. publicar, divulgar e promover a conscientização dos colaboradores e prestadores de serviço quanto a relevância da segurança da informação para a Agência Peixe Vivo, mediante campanhas, palestras, treinamentos e outras formas de endomarketing;apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços;

8. DISPOSITIVOS, DOS EQUIPAMENTOS E DOS RECURSOSELETRÔNICOS, DE COMUNICAÇÃO E DE INFORMÁTICA

Os usuários devem utilizar e manusear corretamente os dispositivos, equipamentos e recursos eletrônicos, de comunicação e de informática disponibilizados pela Agência Peixe Vivo para a realização de atividades profissionais. O uso pessoal dos itens mencionados no é permitido desde que não prejudique o desempenho dos sistemas e serviços da Agência Peixe Vivo.

É proibido todo e qualquer procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação de dispositivos, equipamentos e recursos eletrônicos, de comunicação e de informática, de propriedade da Agência Peixe Vivo, sem prévio conhecimento e acompanhamento de técnico(s) da Coordenação de Tecnologia da Informação da Agência, ou de quem essa determinar.

Os colaboradores e os prestadores de serviço deverão manter a configuração dos dispositivos, dos equipamentos e dos recursos eletrônicos, de comunicação e de informática, disponibilizados pela Coordenação de Tecnologia da Informação da Agência Peixe Vivo, seguindo os devidos controles de segurança exigidos por esta PSI e por normas específicas da agência.

Todas as atualizações e correções de segurança - sejam dos sistemas operacionais, sejam dos aplicativos - somente poderão ser realizadas após validadas no respectivo ambiente de homologação, e uma vez disponibilizadas pelo fabricante ou fornecedor.

Os sistemas e dispositivos, equipamentos e recursos eletrônicos, de comunicação e de informática, de propriedade da Agência Peixe Vivo ou que operem na rede corporativada Agência (agênciapeixevivo.org.br), devem contar com antivírus instalado, ativado e permanentemente atualizado (versões de software mais recentes).

O usuário, em caso de suspeita de vírus ou problemas de funcionalidade, deverá contatar o setor técnico responsável mediante chamado no sistema de solicitações da Agência Peixe Vivo.

Arquivos imprescindíveis para as atividades dos colaboradores e, se for o caso, de prestadores de serviço, deverão ser salvos em diretórios de rede, definidos e indicados pela Coordenação de Tecnologia da Informação.

Os arquivos gravados apenas localmente e nos dispositivos eletrônicos (por exemplo, no drive C: de computadores), não terão garantia de backup e poderão ser perdidos caso ocorram falhas no equipamento.

Colaboradores e prestadores de serviço com acesso à internet da Agência não poderão efetuar upload: de software licenciado a Agência Peixe Vivo; de informações elou de qualquer dado que seja de propriedade ou de responsabilidade da Agência, sem expressa autorização do gestor responsável.

Colaboradores e prestadores de serviço devem informar, ao setor técnico responsável, a existência de eventual dispositivo desconhecido e suspeito conectado a equipamento eletrônico de propriedade da Agência Peixe Vivo.

Todos os modems/switches/hubs, internos e externos, não fornecidos pela Coordenação de Tecnologia da Informação da Agência Peixe Vivo devem ser removidos ou desativados para impedir a invasão/evasão de informações e programas. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso de alguns equipamentos, mediante a autorização dos gestores das áreas e após parecer da Coordenação de Tecnologia da Informação da Agência Peixe Vivo.

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

Os setores que necessitarem de testes operacionais deverão solicitá-los previamente à Coordenação de Tecnologia da Informação da Agência Peixe Vivo, e estarão responsáveis, jurídica e tecnicamente, pelas ações realizadas.

.

Todos os computadores, tablets e impressoras deverão ser protegidos com senha (bloqueados) quando não forem utilizados.

Todos os dispositivos, os equipamentos e os recursos eletrônicos, de comunicaçãoe de informática, adquiridos pela Agência Peixe Vivo, devem ter as respectivas senhas padrão (default) alteradas pela Coordenação de Tecnologia da Informação da Agência.

É vedada a utilização de computadores, notebooks, tablets e smartphones pessoais de colaboradores e prestadores de serviço na rede interna da Agência Peixe Vivo, na rede de dados e na rede corporativa wi-fi (APV Corredor \ APV REUNIÃO), observando-se que:

I. o uso de computadores, notebooks, tablets e smartphones pessoais é permitido apenas no acesso à rede wi-fi "APV TI", quando houver necessidade.
II. demais equipamentos portáteis - como pen-drives, HDs externos e players de qualquer espécie quando não fornecidos ao colaborador ou prestador de serviço pela Agência PeixeVivo, não serão validados para uso e conexão na rede corporativa.
III. equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar elou processar dados, não devem ser usados para armazenarou processar informações relacionadas à Agência Peixe Vivo.

9. CORREIO ELETRÔNICO (E-MAIL CORPORATIVO)

O uso do correio eletrônico da Agência Peixe Vivo é permitido somente para fins corporativos e relacionados às atividades do colaborador e, se for o caso, do prestador de serviço autorizado pela instituição.

É proibido o uso do correio eletrônico da Agência Peixe Vivo, pelos usuários, para:

I. fins pessoais;
II. enviar mensagens não solicitadas para múltiplos destinatários, exceto quando relacionadas a legítimo interesse da Agência;
III. enviar mensagens por correio eletrônico com o nome de usuário de outro colaborador/prestador de serviço ou através de endereço de correio eletrônico que não esteja autorizado a utilizar;
IV. enviar qualquer mensagem por meios eletrônicos que torne o remetente, a Agência PeixeVivo ou respectivos departamentos vulneráveis a ações civis e/ou criminais;
V. divulgar informações não autorizadas contidas em documentos elou imagens de tela (print screen) incluindo de sistemas - e afins sem autorização expressa e formal concedida pelo proprietário do ativo de informação;
VI. falsificar informações de endereçamento, adulterar cabeçalhos para ocultar a identidade de remetentes e/ou destinatários, com o objetivo de evitar punições previstas;
VII. deletar mensagens de correio eletrônico quando qualquer uma das unidades da Agência Peixe Vivo estiver sujeita a investigações e auditorias;
VIII. produzir, transmitir ou divulgar mensagem que:
a) contenha documento ou forneça orientação que conflite ou contrarie os interesses da Agência Peixe Vivo;
b) contenha ameaças eletrônicas, como spam, mail bombfng, vírus de computador;

c) contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src,.cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente risco à segurançados sistemas de dados;

objetive obter acesso não autorizado a outro computador, servidor ou rede;

d) objetive interromper serviços, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
e) objetive burlar sistema de segurança;
f) objetive vigiar ou assediar colaborador(es) e prestador(es) de serviço;
g) objetive acessar informações confidenciais sem explícita autorização do proprietário;
h) objetive acessar, indevidamente, informações que possam causar prejuízos a outrem; inclua imagens criptografadas ou de qualquer forma mascaradas;
i) contenha anexo(s) superior(es) à 25MB para envio interno ou externo e de 25MB para recebimento externo;
j) contenha conteúdo impróprio, obsceno ou ilegal;
k) seja de caráter calunioso, difamatório degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
l) contenha discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional;
m) contenha fins políticos (propaganda política);
n) inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com os seguintes dados:

I. nome do colaborador ou do prestador de serviço;
II. cargo e/ou função;
III. departamento, divisão ou seção a que estiver vinculado;
IV. endereço;
V. telefone(s);
VI. correio eletrônico;
VII. aviso de confidencialidade, quando o for caso, nos seguintes termos: "AVISO DE CONFIDENCIALIDADE: Esta mensagem, assim como os arquivos eventualmente anexados, é confidencial e reservada apenas ao conhecimento da(s) pessoa(s) nela indicada(s) como destinatária(s). Se não for o destinatário, por recebimento indevido, solicitamos que não faça qualquer uso do respectivo conteúdo e proceda à sua eliminação, notificando o remetente."

10. INTERNET

As regras contidas neste item da Política de Segurança da Informação (PSI) bem como no Termo de Responsabilidade sobre a utilização da rede interna (intranet), internet, computadores e e- mail corporativo da Agência Peixe Vivo visam boas práticas e comportamentos profissionais éticos no uso da internet.

Qualquer informação acessada, transmitida, recebida ou produzida na internet está sujeita a auditorias. A Agência Peixe Vivo, em total conformidade legal, reserva-se o direito de monitorar e registrar os acessos ocorridos através da rede mundial de computadores.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet, os quais são de propriedade da Agência, poderão analisar e, se necessário, bloquear qualquer arquivo (armazenado em diretório da rede elou disco local), site,

correio eletrônico, domínio ou aplicação, com o intuito de assegurar o cumprimento desta PSI.

Toda alteração ou tentativa de alteração dos parâmetros de segurança da internet, por qualquer colaborador ou prestador de serviço, sem o devido credenciamento e autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo gestor. Caso a alteração ou tentativa de alteração ocorra para a prática de atividades ilícitas, serão encaminhadas para apuração de responsabilidade e aplicação de sanções, sem prejuízo da cooperação da Agência Peixe Vivo com as autoridades competentes para a repressão de ilícitos criminais e civis.

A internet disponibilizada pela instituição aos colaboradores e prestadores de serviço, poderá ser utilizada para fins pessoais, desde que:

I. não prejudique o andamento dos trabalhos nos setores;
II. não comprometa a banda da rede em horários estritamente comerciais;
III. não implique conflitos de interesse com as finalidades institucionais.

É proibida a divulgação elou o compartilhamento indevido de informações administrativas e gerenciais em listas de discussão, aplicativos de comunicação, sites, comunidades de relacionamento, salas de bate-papo e comunicadores instantâneos, salvo quando estes recursos forem adotados institucionalmente como ferramenta de trabalho a critério do(s) gestor(es).

Colaboradores e prestadores de serviço não poderão utilizar equipamentos e recursos disponibilizados pela Agência Peixe Vivo para download e/ou distribuição de softwares pirateados, porquanto atividades ilícitas segundo o ordenamento jurídico nacional.

Colaboradores e prestadores de serviço não poderão utilizar recursos da Agência Peixe Vivo para, deliberadamente, propagar vírus, worms, cavalo de troia, spam e programas de controle a computadores de terceiro(s), bem como para efetuar assédio e perturbação de terceiros.

O acesso a softwares peer-to-peer ou storage backup (eMule, BitTorrent, Dropboxe afins) não é permitido, bem como não é permitido o acesso a sites de proxy.

11. SISTEMAS, DRIVES E DA REDE INTERNA

Os sistemas, drives e a rede interna são de domínio da Agência, que poderá analisar e, se necessário, bloquear qualquer arquivo ou aplicação neles armazenados, com o intuitode assegurar o cumprimento desta Política de Segurança da Informação. Ao monitorar os sistemas, drives e a rede interna, a Agência Peixe Vivo, busca garantir a integridade dos dados, programas e aplicações.

Os sistemas e os servidores são utilizados por colaboradores e, se for o caso, por prestadores de serviço previamente autorizados para a realização de atividades em nome ou para a Agência Peixe Vivo.

Arquivos pessoais e/ou não pertinentes a Agência Peixe Vivo (fotos, músicas, vídeos, dentre outros) não deverão ser copiados/movidos para os drives de rede da agência, e, poderão ser permanentemente excluídos sem prévia comunicação ao titular, caso localizados.

Os colaboradores e prestadores de serviço não devem executar nenhum tipo de comando ou programa, os quais possam sobrecarregar a rede corporativa, sem prévia solicitação e autorização da Coordenação de Tecnologia da Informação.

Toda alteração ou tentativa de alteração dos parâmetros de segurança da rede, por qualquer colaborador ou prestador de serviço, sem o devido credenciamento e autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao usuário e aorespectivo gestor. Caso a alteração ou tentativa de alteração ocorra para a prática de atividades ilícitas, serão encaminhadas para apuração de responsabilidade e aplicação de sanções, sem prejuízo da cooperação da Agência Peixe Vivo com as autoridades competentes para a repressão de ilícitos criminais e civis.

Apenas os colaboradores e prestadores de serviço autorizados pela Agência PeixeVivo poderão enviar documentos e/ou imagens de tela (print screen) — incluindo de sistemas - a terceiros, com a devida observância a normas internas de privacidade e segurança da informação, bem como à legislação federal referente a uso de imagens, direitos autorais, proteção da imagem e de dados pessoais.

12. IDENTIFICAÇÃO DO COLABORADOR E DO PRESTADOR DE SERVIÇO

Todos os dispositivos de identificação utilizados para o exercício de atividades administrativas na Agência Peixe Vivo - número de registro; crachá; identificações de acesso a equipamentos eletrônicos, ambiente de rede e sistemas, com login e senha; certificados e assinaturas digitais e dados biométricos - devem encontrar- se associados a determinada pessoa física e atrelados inequivocamente aos documentos oficiais por ela apresentados reconhecidos pela legislação brasileira.

Os dispositivos de identificação protegem a identidade do colaborador e do prestador de serviço, de forma a prevenir que pessoas não autorizadas desempenhem atividades de forma ilícita perante a própria Agência e/ou perante terceiros (art. 307 do Código Penal - crime de falsa identidade).

Dispositivos de identificação pessoal não poderão ser compartilhados com terceiros salvo se, a critério do gestor, houver login de uso compartilhado por mais de um colaborador ou prestador de serviço.

É proibido, em qualquer caso, o compartilhamento de login para funções relacionadas à administração de sistemas.

O usuário vinculado aos dispositivos identificadores para funções relacionadas à administração de sistemas é responsável pelo seu uso correto, perante a agência e em nome da agência.

Todos os acessos a equipamentos eletrônicos, ambiente de rede e sistemas, bem como às dependências físicas da Agência Peixe Vivo devem ser bloqueados:

I. quando houver o término do vínculo do colaborador com a Agência Peixe Vivo decorrente do encerramento do mandato eletivo, da extinção do contrato det rabalho de funcionário ou da extinção de contrato de estágio;
II. quando houver o término do vínculo do prestador de serviço com a Agência Peixe Vivo decorrente da extinção do contrato de prestação de serviços.

Para fins de bloqueio de identificações de acesso a equipamentos eletrônicos, ambientede rede e sistemas, certificados, assinaturas digitais e dados biométricos, o término do vínculo do colaborador ou do prestador de serviço com a Agência deve ser comunicado imediatamente à Coordenação de Tecnologia da Informação da Agência Peixe Vivo:

I. pelo Departamento Pessoal da Agência Peixe Vivo, se se tratar de funcionários e estagiários;
II. pelo respectivo fiscal de contrato, quando se tratar de prestador de usuários cuja prestação de serviços for finalizada.

Para fins de bloqueio de crachá e demais autorizações de acesso às dependências da Agência Peixe Vivo, o término do vínculo do usuário com a Agência deve ser comunicado imediatamente à Gerência de Administração e Finanças da Agência Peixe Vivo para:

I. Coordenação de Recursos Humanos da Agência Peixe Vivo, quando se tratar de funcionários e estagiários;
II. respectivo fiscal de contrato, quando se tratar de prestador de serviço.

12.1 SENHAS

Caberá à Coordenação de Tecnologia da Informação instituir login e senha aos colaboradorese, se for o caso, aos prestadores de serviço da agência.

Ao realizar o primeiro acesso no equipamento eletrônico, ambiente de rede local ou sistema, o usuário deverá trocar imediatamente a senha padrão conforme as orientações recebidas.

A senha deverá conter caracteres em número e tipologia suficientes à proteção das informações e à garantia do sigilo dos dados. Cada usuário deverá memorizar a própria senha e/ou armazená-la em local seguro;

Caso o colaborador ou o prestador de serviço não se lembre do login elou senha, deverá requisitar, formalmente, a troca ou comparecer, pessoalmente, à área técnica responsável para cadastrar uma nova sequência.

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

Os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizaruma senha de no mínimo IO (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

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

A Coordenação de Tecnologia da Informação poderá instituir campanhas e processos regulares para a renovação de senhas dos respectivos colaboradores e prestadores de serviço.

Os usuários podem alterar a própria senha a qualquer tempo, mediante requerimento à Coordenação de Tecnologia da Informação, e devem fazê-lo imediatamente caso suspeitem que terceiros obtiveram acesso indevido ao respectivo logine

senha.

13. MONITORAMENTO E INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Para garantir as diretrizes da PSI, a Agência Peixe Vivo poderá utilizar sistemas de monitoramento nas estações de trabalho, notebooks corporativos, tablets corporativos, equipamentos de servidores, correio eletrônico, conexões com a internet, dispositivos móveis como pen-drives e HDs externos ou wireless, e outros componentes da rede. A informação gerada por tais sistemas poderá, ainda, ser usada para identificar usuários e respectivos acessos efetuados, bem como o material manipulado.

Além disso, a Agência Peixe Vivo poderá:

I. tornar públicas quaisquer informações obtidas pelos sistemas de monitoramento e auditoria, nas hipóteses de exigência judicial, solicitação de gerentes (ou superiores hierárquicos) ou por determinação da Coordenação de Recursos Humanos da Agência Peixe Vivo;
II. realizar, a qualquer tempo, inspeções físicas nos equipamentos da Agência Peixe Vivo;
III. instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM SEGURANÇA DA INFORMAÇÃO

Todo incidente de segurança da informação deverá ser comunicado inicial e imediatamente ao encarregado de Dados Pessoais (DPO) da Agência Peixe Vivo, que fará o registro, a triagem de acordo tabela de classificação de incidentes a ser elaborada, para o devido encaminhamento da demanda.

Caberá ao agente demandado pelo DPO, analisar, criticamente, os incidentes de segurança da informação, solicitando apoio e parecer da Coordenação de Tecnologia da Informação, especialmente quando se tratar de incidentes relacionados à Tecnologia da Informação.

Após o registro do incidente, deverão ser cientificados os envolvidos e os respectivos gestores, oportunizando-se prazo para manifestação.

A análise final dos incidentes será feita pelo Comitê de Segurança da Informação e Privacidade. Os processos de análises dos incidentes deverão ser concluídos em até 30 (trinta) dias, podendo este prazo ser prorrogado, mediante justificativa.

14. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO DA AGÊNCIA PEIXE VIVO

A gestão de riscos de segurança da informação na Agência Peixe Vivo tem como objetivo auxiliar a tomada de decisão com vistas a prover razoável segurança no cumprimento da missão e no alcance dos objetivos da agência, de forma a possibilitar a identificação, avaliação, tratamento, monitoramento e comunicação de riscos operacionais, tecnológicos e de imagem.

A Agência Peixe Vivo deverá ser operacionalizada em conjunto com instrumentos de gestão que suportam a concepção, implementação, monitoramento e melhoria contínua da gestão de riscos através de toda a organização e

compreende,entre outros: políticas, estruturas organizacionais, planos, programas, métodos, relacionamentos, responsabilidades, atividades, processos e recursos.

A gestão de riscos de segurança da informação deverá se integrar ao planejamento estratégico, aos processos e às políticas da Agência Peixe Vivo, sendo implementada de forma gradual em todas as áreas da Agência.

Para fins desta política, considera-se:
Risco: possibilidade de que um evento afete o alcance de objetivos;
Oportunidade: possibilidade de que um evento afete positivamente o alcance de objetivos;
Risco-chave: risco que, em função do impacto potencial a Agência Peixe Vivo, deve ser conhecido pela alta administração;
Apetite a risco: nível de risco que uma organização está disposta a aceitar;
Controles internos da gestão: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada, destinados a enfrentar os riscos e fornecer segurança razoável na consecução da missão e do alcance dos objetivos do órgão;
Fonte de risco: elemento que, individualmente ou combinado, tem o potencial intrínseco de dar origem ao risco;
Gestão de riscos: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dosobjetivos da organização;
Gestor de risco: pessoa, papel ou estrutura organizacional com autoridade e responsabilidade para gerenciar um risco;
Nível do risco: medida da importância ou significância do risco, considerando a probabilidade de ocorrência do evento e o seu impacto nos objetivos;
Processo: conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido;
Evento: um ou mais incidentes ou ocorrências, proveniente do ambiente internoou externo, ou mudança em um conjunto específico de circunstâncias, podendo também consistir em algo não acontecer.

Considerando a importância dos fatores humanos e culturais, as ações de gestão de riscos de segurança da informação na Agência Peixe Vivo são dirigidas, apoiadas e monitoradas pela alta administração.

A gestão de riscos de segurança da informação na Agência Peixe Vivo tem por objetivos:

I. contribuir para uma cultura de gestão de riscos, chamando a atenção para a importância de se identificar e tratar riscos relacionados à segurança da informação em todas as áreas e níveis organizacionais da Agência Peixe Vivo;
II. fomentar a gestão proativa;
III. facilitar a identificação de oportunidades e ameaças;
IV. aprimorar os controles internos da gestão, privilegiando ações de prevenção antes da ocorrência de danos ou de processos sancionadores;
V. aumentar a capacidade da organização de se adaptar a mudanças.

O processo de gestão de riscos de segurança da informação na Agência Peixe Vivo contempla o estabelecimento do contexto, a identificação, a análise, a avaliação, o tratamentode riscos, a comunicação e a consulta com partes interessadas, o monitoramento e a melhoria contínua.

- ✓ O estabelecimento do contexto consiste em compreender o ambiente externo e interno noqual o objeto de gestão de riscos de segurança da informação encontra-se inserido e em identificar parâmetro.
- ✓ A identificação do risco compreende o reconhecimento e descrição dos riscos relacionadosa um objeto de segurança da informação, envolvendo a identificação de possíveis fontes de riscos, eventos, causas e consequências.
- ✓ A avaliação do risco envolve a comparação do nível do risco com critérios, a fim de determinar se o risco é aceitável.
- ✓ O tratamento do risco compreende o planejamento e a realização de ações para modificar o nível do risco.
- ✓ O monitoramento compreende o acompanhamento e a verificação do desempenho ou da situação de elementos da gestão de riscos, podendo abranger a política, as atividades, os riscos,os planos de tratamento de riscos, os controles e outros assuntos de interesse.
- ✓ A comunicação e consulta refere-se à identificação das partes interessadas em objetos de gestão de riscos e obtenção, fornecimento ou compartilhamento de informações relativas à gestão de riscos sobre tais objetos, observada a classificação da Informação quanto ao sigilo.
- ✓ A melhoria contínua com os e critérios a serem considerados no processo de gestão de riscos.

A metodologia de riscos definirá os critérios de avaliação dos riscos, contemplando as escalas progressivas para avaliação do evento de risco nos parâmetrosde probabilidade e impacto, bem como a classificação final na matriz de risco.

No âmbito da Agência Peixe Vivo a gestão de riscos de segurança da informação é coordenada pela Gerência de Gestão Estratégica e sua Coordenação de Tecnologia da Informação, podendo ser apoiada por departamentos da estrutura auxiliar.

A Gerência de Gestão Estratégica da Agência Peixe Vivo representa o nível ético da ação, sendo responsável pela coordenação das ações e consolidação de informações estruturadas sobre riscos em conjunto com os demais departamentos, à quem compete, em especial:

I. propor a política de gestão de riscos de informações e suas revisões;
II. aprovar a metodologia de gestão de riscos de informações e suas revisões;
III. avaliar a evolução de níveis de riscos e a efetividade das medidas de controle implementadas;
IV. garantir o apoio institucional para promover a gestão de riscos, em especial os seus recursos, o relacionamento entre as partes interessadas e o desenvolvimentocontínuo dos colaboradores;
V. estimular a contínua capacitação do corpo funcional em gestão de riscos e em outras competências técnicas correlatas, por meio de palestras, cursos e eventos;
VI. incentivar a adoção de boas práticas de governança e de gestão de riscos;

Compete ao gerente de cada departamento monitorar riscos-chave e propor limitesde exposição a riscos relacionados à sua área de atuação e designar o gestor de risco do seu departamento

Gestor de risco é a pessoa responsável por coordenar ações e promover a execuçãodos procedimentos de gestão de risco no âmbito da divisão ou do setor a que se vincula, bem como prover informações ao gerente de seu departamento. Compete, ainda ao gestor do risco:

I. assegurar que o risco seja gerenciado de acordo com a política e metodologia;
II. monitorar o risco ao longo do tempo, de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados, de acordo com a política e metodologia de gestão de riscos;

III. garantir que as informações adequadas sobre o risco estejam disponíveis para asinstâncias do nível ético da gestão de riscos;
IV. promover a disseminação da cultura de gestão de riscos.

O departamento da estrutura auxiliar representa o nível operacional da ação, sendo responsável pelo gerenciamento das ações de identificação, avaliação e tratamento dos riscos dos processos sob sua responsabilidade, bem como pela proposição de respostas e respectivas medidas de controle a serem implementadas nos processos organizacionais sob sua responsabilidade.

Os demais colaboradores da Agência Peixe Vivo deverão auxiliar no limite de suas atribuições para o atingimento dos objetivos da gestão de riscos, assessorando no processo de gerenciamento de riscos com a aplicação de técnicas, métodos e instrumentos e comunicando as deficiências identificadas às instâncias superiores.

O Departamento da estrutura auxiliar e os Gestores de Risco deverão manter fluxo regular e constante de informações entre si, no limite de suas competências.

A Política de Gestão de Riscos de Segurança da Informação poderá ser revista sempre que necessário, no intuito de mantê-la atualizada diante de mudanças noambiente interno ou externo, a partir de proposta elaborada pela Gerência de Gestão Estratégica da Agência Peixe Vivo.

15. BACKUP E RECUPERAÇÃO DE DADOS DIGITAIS DA AGÊNCIA PEIXE VIVO

O objetivo deste documento é regulamentar a política de backup e recuperação dos dados digitais no âmbito da Agência Peixe Vivo. Desse modo, estabelece diretrizes para o processo de cópia, armazenamento dos dados e recuperação dos dados digitais sob a guarda da Coordenação de Tecnologia da Informação (DTI), visando garantir a segurança, integridade e disponibilidade, em conformidade com a Política de Segurança da Informação.

Os procedimentos próprios relacionados ao serviço de backup (cópia de segurança) devem considerar as seguintes diretrizes gerais:

I. o serviço de backup deve ser automatizado por sistemas informacionais próprios,com execuções agendadas - fora do horário normal de expediente da empresa ("janelas de backup", isto é, períodos em que há pouco ou nenhum acesso de usuários, bem como reduzidos processos automatizados);
II. a administração das mídias de backup deve ser contemplada em normas complementares sobre o serviço, para garantir a segurança e a integridade doprocesso;
III. a execução de rotinas de backup e restore deverá ser rigidamente controlada, documentada e auditada, nos termos das normas e procedimentos próprios.

Para manter a continuidade do negócio da Agência Peixe Vivo, é fundamental estabelecer mecanismos que permitam a guarda dos dados e sua eventual restauração emcasos de perdas por erro humano, ataques externos, catástrofes naturais ou outras ameaças.

Para fins desta política, considera-se:
Administrador de Backup: servidor do quadro da AGÊNCIA PEIXE VIVO responsável pelos procedimentos de

configuração, execução, monitoramento e testes dos procedimentos de backup;
Administrador de Recurso: servidor do quadro da AGÊNCIA PEIXE VIVO responsável pela administração de ativo de TIC, físico ou virtual, sob responsabilidade da agência;
Backup Completo (full): modalidade de backup na qual os dados são copiados em sua totalidade;
Backup Diferencial: modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup completo são copiados;
Backup Incremental: modalidade de backup na qual somente os arquivos novos oumodificados desde o último backup – seja completo, diferencial ou incremental - são copiados;
Clientes de backup: todo equipamento servidor no qual é instalado o agente de backup;
Recuperação de Desastre: estratégia de recuperação de dados motivada por sinistrosde grave amplitude física ou lógica;
Mídia: meio físico ou virtual no qual efetivamente armazenam-se os dados de um backup;
Retenção: período em que o conteúdo da mídia de backup deve ser preservado;
Objeto: qualquer dado passível de backup e restauração;
Tarefa de Backup: mecanismo que é executado sob demanda ou de acordo com um agendamento e vincula um ou mais objetos a uma modalidade de backup e um período de retenção.

PADRÕES OPERACIONAIS:

- ✓ A Política de Backup e Recuperação de Dados Digitais deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.
- ✓ As rotinas de backup devem ser orientadas para a restauração dos dados no menortempo possível principalmente quando da indisponibilidade de serviços de TI e devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviçosde TI críticos da Agência Peixe Vivo.

FERRAMENTAS DE BACKUP:

- ✓ As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.
- ✓ Os ativos envolvidos no processo de backup são considerados ativos críticos para a Agência Peixe Vivo,
- ✓ Compete å Coordenação de Tecnologia da Informação (DTI) solicitar, à Administração, com as justificativas pertinentes, os equipamentos necessários para manter o parque de ativos sempre atualizado e em quantidade necessária ao atendimento dademanda da Agência Peixe Vivo.

ATRIBUIÇÕES DO ADMINISTRADOR DE BACKUP:

- ✓ Propor modificações visando o aperfeiçoamento da política de backup;
- ✓ Criar e manter as tarefas de backup;
- ✓ Configurar a ferramenta de backup e os clientes;
- ✓ Considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados da Agência Peixe Vivo;
- ✓ Criar e manter mídias;
- ✓ Testar o backup e a restauração;
- ✓ Gerenciar mensagens e logs diários dos backups, fazendo o tratamento dos erros de forma que o procedimento de backup tenha sequência e os erros nasua execução sejam eliminados;
- ✓ Fazer manutenções periódicas dos dispositivos de backup;
- ✓ Fazer o carregamento das mídias necessárias para os backups programados.

OS PROCEDIMENTOS DE BACKUP DEVERÃO SER ATUALIZADOS QUANDO HOUVER:

- ✓ Novas aplicações desenvolvidas;
- ✓ Novos locais de armazenamento de dados ou arquivos;
- ✓ Novas instalações de bancos de dados;
- ✓ Novos aplicativos instalados;
- ✓ Outras informações que necessitem de proteção através de backups deverão serinformadas ao Administrador de Backup, pelo Administrador de Recurso.

PRAZO DE RETENÇÃO:

A retenção dos backups deve observar os seguintes prazos:

- ✓ Diário: Retenção em nuvem de doze meses, trata-se de file system;
- ✓ Semanal: Retenção em disco por 30 dias;
- ✓ Expirado o prazo de retenção dos dados armazenados, a mídia poderá ser reutilizada ou destruída, observando sempre seu estado de utilização e número de leitura/gravação.

PROCEDIMENTOS DE BACKUP:

A criação e operação dos backups deverão obedecer às seguintes orientações:

I. Criação de backups:
   a) O backup deverá ser programado para execução automática em horários de menor utilização dos sistemas;
   b) O backup, preferencialmente, deverá ser realizado através da rede de backup.

II. Operação de backups:
   a) O backup deverá ser monitorado pela equipe de TI;
   b) Para todos os backups realizados, deve ser gerado um extrato automatizado pela própria ferramenta de backup. Tal extrato deverá ser enviado por e-mail para o Administrador de Backup;
   c) O Operador de TI deverá gerar, por amostragem, relatório geral, mensal da execução de tais backups.

III. Os backups deverão ser realizados, preferencialmente, como disposto a seguir:
   a) Os backups diários serão executados de segunda à sexta-feira, entre 18h e 6h do dia posterior, em modo incremental;
   b) Os backups semanais serão executados nos finais de semana, iniciando aos sábados, em modo Full.
   c) Em caso de falha em algum procedimento de backup ou impossibilidade da sua execução, o Administrador de Backup deverá adotar as providências necessárias para promover a salvaguarda das informações através de outro mecanismo, como por exemplo: nova execução do backup em horário de comercial ou cópia dos dados para outro servidor.

PROCEDIMENTOS DE RESTAURAÇÃO:

A recuperação de backups deverá obedecer às seguintes orientações:

I. A solicitação de recuperação de objetos deverá, sempre, iniciar-se com o responsável pelo recurso, através de chamado técnico, utilizando a ferramenta de controle de atendimentos da Agência Peixe Vivo;

II. O chamado técnico deve conter, ao menos, o nome e setor do usuário, o(s) objeto(s) a ser(em) recuperado(s), localização em que se encontra(m), a datada versão que deseja recuperar, local alternativo para o armazenamento do(s) objeto(s) recuperado(s), se for o caso, e a justificativa para recuperação;

III. Este chamado será encaminhado ao Administrador de Backup, que após a conclusão da tarefa, realizará o fechamento do chamado indicando a restauraçãodo(s) objeto(s).

IV. A restauração de objetos somente será possível nos casos em que este tenhasido atingido pela estratégia de backup.

RECUPERAÇÃO DE DESASTRE:

I. As cópias do tipo Recuperação de Desastres serão feitas com base na replicação das mídias do backup diário e serão armazenadas em servidores a parte e/ou fitas de backup;

II. Quaisquer procedimentos programados nos equipamentos "servidores" e que impliquem riscos ao seu funcionamento ou em quaisquer dispositivos de armazenamento do CPD, somente deverão ser executados após a realização do backup dos seus dados;

III. Os backups devem ser testados periodicamente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados;

IV. Os testes de restauração dos backups devem ser realizados, por amostragem, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis na Agência Peixe Vivo;

V. A periodicidade, abrangência, os procedimentos e as rotinas inerentes aos testes de backup serão definidos em norma específica a ser elaborada pela Coordenação de Tecnologia da Informação em conjunto com os gestores das informações.

ANEXO I - TERMO DE RESPONSABILIDADE

TERMO DE CONFIDENCIALIDADE E NÃO DIVULGAÇÃO

Em observância à Lei Geral de Proteção de Dados número 13.853, de 2019.

Em observância à Lei Geral de Proteção de Dados nº 13.853 de 2019, através do presente instrumento,

eu_____, inscrito (a) no CPF sob número , doravante designado(a) simplesmente **RESPONSÁVEL**, se compromete, por intermédio do presente TERMO DE CONFIDENCIALIDADE E NÃO DIVULGAÇÃO, a não divulgar, sem autorização, quaisquer informações de propriedade da **AGÊNCIA DE BACIA HIDROGRÁFICA PEIXE VIVO**, doravante **APV**, em conformidade com as seguintes condições:

I. Reconheço que em razão da utilização das ferramentas tecnológicas/equipamentos disponibilizados pela **APV**, poderei ter acesso a diversas informações pessoais, sensíveis, estratégicas, comerciais, entre outras - confidenciais ou não - armazenadas nos sistemas informatizados sob a responsabilidade da **APV**;

II. Tenho ciência de que as credenciais de acesso *(login e senha)* à eventuais ferramentas tecnológicas/equipamentos são de uso pessoal e intrasferível e de conhecimento exclusivo e assumir o dever de observância às normas sobre a utilização da rede interna (intranet), internet, computadores e e-mail corporativo da Agência. É de minha inteira responsabilidade todo e qualquer prejuízo causado pelo fornecimento de minha senha pessoal à terceiros, independente do motivo.

III. Reconheço que para os fins deste documento serão consideradas confidenciais todas as informações, transmitidas por meios escritos, eletrônicos, verbais ou quaisquer outros e de qualquer natureza, incluindo, mas não se limitando a:

a. Dados pessoais - qualquer informação que possa tornar uma pessoa física identificada ou identificável;

b. Dados sensíveis - Qualquer dado pessoal que diga respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dado referente à saúde ou à vida sexual, dado genético ou biométrico;

c. Dados financeiros, informações sobre governança relacionadas à estruturas organizacionais, técnicas, design, especificações, desenhos, cópias, modelos, fluxogramas, croquis, fotografias, software, sistemas de informação, mídias, contratos, planos de negócios, propostas comerciais, processos, tabelas, projetos, nomes de clientes, resultados de pesquisas, invenções e ideias, financeiras, comerciais, dentre outros, as quais são extremamente importantes para o desenvolvimento das atividades da Agência.

IV. Me comprometo a não utilizar qualquer informação à qual tenha acesso, classificada como confidencial ou não, para fins diversos daqueles para os quais tive autorização de acesso;

V. Estou ciente que, é proibida a cópia, de qualquer informação para dispositivos estranhos à estrutura da **APV**, bem como a divulgação e compartilhamento, exceto se a referida ação, seja estritamente necessária para a prestação dos serviços contratados, devendo ser realizada com a maior segurança possível e com expressa e prévia autorização do

representante legal da **APV**;

VI. O **RESPONSÁVEL** obriga-se a informar imediatamente à **APV** qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus prestadores de serviço dos contratos de sua responsabilidade;

VII. Reconheço que os prejuízos causados por mim à **APV**, em razão da quebra de confidencialidade, disponibilidade ou integridade das informações às quais tenho acesso, poderão ser reclamados, judicial ou extrajudicialmente e, caso caracterizada qualquer infração penal, poderei ser pessoalmente responsabilizado;

VIII. Reconheço que meus dados pessoais utilizados para acesso aos sistemas disponibilizados pela **APV**, serão conservados durante o tempo que estiver vigente a relação contratual com a **APV** no qual estou vinculado e após esta finalizar, durante os períodos de retenção de dados legalmente exigíveis, de forma estritamente necessária, tais como, mas não se limitando, pelos prazos prescricionais para ajuizamento de ação penal ou civil, assim como para o exercício do direito de defesa em processo judicial de qualquer natureza ou para outra finalidade por período não excessivo adotado pela **APV**, garantida a transparência, confidencialidade, integridade e disponibilidade das minhas informações pessoais, bem como o exercício dos direitos previstos na Lei Federal nº 13.709/2018 ("LGPD") na vigência da relação contratual assim como após o término da referida relação;

IX. Reconheço, neste ato, ter lido, compreendido e sanado todas as dúvidas sobre o Termo de Confidencialidade e Não Divulgação.

Belo Horizonte, ____de _____de 2024.

ASSINATURA DO RESPONSÁVEL