PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

OUTUBRO DE 2023

PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Documento de Diretrizes e Normas Administrativas.

Histórico de alterações e atualizações

Data	Versão	Criado por	Descrição da alteração
09/10/2023	1.0	Alexander Silva Leão	Layout e Estruturação da POSIC.
16/10/2023	2.0	Robson Bezerra de Sousa	Primeira versão da POSIC finalizada.
23/10/2023	3.0	Kleverton Willams Silva	Terceira versão da POSIC finalizada.

Histórico de revisões

Data	Revisado por	Seções revisadas
30/10/2023	Robson Bezerra de Sousa	Todas

SUMÁRIO

Rua Binga Uchoa, 10 - Centro - CEP 68900-090 - Macapá/AP - CNPJ 03.281.445/0001-85
Fone: (96) 4009-2400

DISTRIBUIÇÃO E VIGÊNCIA

Este documento consiste na Política de Segurança da Informação – PSI da Amapá Previdência - AMPREV, que deve ser mantida como uma medida de boas práticas, estabelecendo diretrizes para a proteção de ativos e prevenção de responsabilidades.

No entanto destaca-se que a mesma deve ser adotada, cumprida e aplicada em todas as áreas da instituição.

Esta versão pode ser alterada a qualquer momento, uma vez que os pontos apontados para mudanças sejam informados e discutidos com os demais colaboradores da Diretoria Executiva.

Contudo a versão da PSI deve ser revisada a cada ano, considerando a data de sua aprovação.

Rua Binga Uchoa, 10 - Centro - CEP 68900-090 - Macapá/AP - CNPJ 03.281.445/0001-85
Fone: (96) 4009-2400

GLOSSÁRIO:

Ativo: Algo que tenha valor para a organização.

Evento: Acontecimento que acarrete na mudança do estado atual de um processo.

Incidente: Evento que traz prejuízos à organização.

LGPD: Lei Geral de Proteção de Dados.

Risco: Combinação da probabilidade de ocorrência de um evento e seus respectivos impactos.

Vulnerabilidade: Fragilidade de um ativo que pode ser explorada e gerar danos à organização.

Malwares: O nome malwares vem do inglês malicious software (programa malicioso). Refere-se a qualquer tipo de programa indesejado, instalado sem seu consentimento e que pode trazer danos ao computador.

SPAM: É o termo usado para referir-se a e-mails não solicitados, que geralmente são enviados para um grande número de pessoas.

Phishing: Mensagens de e-mail que solicitam dados do usuário de forma direta ou através de redirecionamentos para sites ou números de telefone, a fim de roubar sua identidade.

Mail bombing: Envio de mensagens eletrônicas em massa para um determinado destinatário com o objetivo de sobrecarregar o serviço de e-mail e torná-lo inutilizável ou indisponível.

INTRODUÇÃO

A presente Política de Segurança da Informação – PSI está baseada nas recomendações da norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, além de estar de acordo com o DEC 9.637/2018 (DECRETO DO EXECUTIVO) 26/12/2018, que Institui a Política Nacional de Segurança da Informação. A informação é um ativo de grande valor para o Fundo Único de Previdência Social do Estado do Rio de Janeiro – AMPREV, por isso necessita ser adequadamente protegida. “Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio” (ABNT NBR ISO/IEC 17799:2005).

Por princípio, a Segurança da Informação deve abranger três propriedades básicas:

- Confidencialidade: Propriedade que estabelece que a informação deva estar acessível apenas para pessoas autorizadas;
- Integridade: Propriedade que estabelece que a informação esteja correta, confiável, sem a ocorrência de mudanças não autorizadas;
- Disponibilidade: Propriedade que estabelece que a informação esteja sempre acessível para uso legítimo de pessoas autorizadas.

OBJETIVO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

"A segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados" (ABNT NBR ISO/IEC 17799:2005).

A Política de Segurança da Informação tem como objetivo estabelecer normas, diretrizes e procedimentos que assegurem a segurança das informações, ao tempo que não impeçam e/ou dificultem o processo do negócio, mas que garantam:

• A confiabilidade das informações através da preservação da confidencialidade, integridade e disponibilidade dos dados da empresa;

• O compromisso da empresa com a proteção das informações de sua propriedade e/ou sob sua guarda;

• A participação e cumprimento por todos os colaboradores em todo o processo.

POR QUE OS COLABORADORES DEVEM SE PREOCUPAR COM SEGURANÇA?

"Uma corrente é tão forte quanto seu elo mais fraco".

Não adianta a área da Tecnologia da Informação impor controles e medidas técnicas se não existir a participação dos colaboradores, por exemplo, de nada vale a implantação de barreiras e portas de controle de acesso eletrônico se um funcionário que tem acesso legítimo a determinada área restrita, resolve divulgar informações confidenciais que estavam devidamente protegidas nesta área.

A área de Tecnologia da Informação é a responsável pela salvaguarda dos dados da organização, mas o processo de segurança da informação deve envolver todos os

colaboradores, independentemente do nível hierárquico, posto que, de posse de uma informação específica qualquer pessoa pode, por descuido e/ou com má intenção, se tornar um agente de divulgação não autorizada.

Diante do exposto, a Política da Segurança da Informação vem propor uma Gestão de Segurança da Informação baseada em controles e procedimentos técnicos, considerando e promovendo o comportamento dos colaboradores de forma que possa aplicar a tecnologia adequada em todo o processo e atingir efetividade em seu objetivo: entender o negócio e aplicar segurança a ele.

DIREÇÃO

A efetividade da Política de Segurança da Informação depende estritamente do comprometimento da alta direção.

É essencial que os responsáveis por liberar recursos, aplicar sanções, criar regras e portarias, apoiem a PSI e demonstrem seu comprometimento para que os colaboradores se sintam motivados a cumpri-la.

A ordem expressa e o exemplo de cumprimento das cláusulas da PSI pela alta direção possibilitarão: • A inexistência de exceções à regra;

• Que a PSI seja um ativo estratégico;

• Que a PSI componha a legislação interna do AMPREV;

• Conformidade com a LGPD. (Lei nº 14010 de 10/06/2020);

• Que a PSI tenha ampla divulgação nas palestras desenvolvidas pelo EDUCAPREVA e PODCAST'S da Amapá Previdência;

• Que a PSI seja incluída no processo de recrutamento de novos servidores e prestadores de serviços.

A Política de Segurança da Informação se tornará um documento, existente na teoria e adotada na prática.

CLASSIFICAÇÃO DAS INFORMAÇÕES

As informações devem ser classificadas e identificadas por rótulos, considerando os seguintes níveis:

• Pública;

• Interna;

• Confidencial;

• Confidencial restrita;

– Pública

São informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio e que, por isso, não necessitam de proteção efetiva ou tratamento específico. São exemplos de informação pública:

• Editais de licitação;

• Portal da transparência.

- Interna

São informações disponíveis aos colaboradores do AMPREV para a execução de suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo. São exemplos de informações internas:

• Memorandos, Oficio Internos, Ofícios Externos, Portarias, Padrões, Políticas e Procedimentos internos;

• E-mails e lista telefônica internos;

• Avisos e campanhas internas; intranet.

Confidencial

São informações de acesso restrito a um colaborador ou grupo de colaboradores. Sua revelação pode violar a privacidade de indivíduos, violar acordos de Confidencialidade, prejuízos financeiros, dentre outros.

São exemplos de informações confidenciais:

• Processos judiciais;

• Dados cadastrais de funcionários;

• Dados processuais previdenciários;

Confidencial restrita

São informações de acesso restrito a um colaborador ou grupo de colaboradores que obrigatoriamente contam como destinatários delas mesmas, em geral, associadas ao interesse estratégico da empresa e restritas ao superintende, gerentes e funcionários cujas funções requeiram conhecê-las. São exemplos de informações confidenciais restritas:

• Atas de reunião da governança com a presidência;

• Indicadores e estatísticas dos processos de negócio do AMPREV;

• Resultado de auditorias internas.

DAS RESPONSABILIDADES

Colaboradores

Será de inteira responsabilidade de servidores, funcionários, terceirizados e demais colaboradores da AMAPÁ PREVIDÊNCIA:

• Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação do Fundo de Previdência Social do Estado do Amapá;

• Buscar o DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO para esclarecimentos de dúvidas referentes à PSI;

• Proteger as informações contra acesso, divulgação, impressão, modificação ou destruição não autorizados pela AMPREV;

• Garantir que equipamentos e recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela AMPREV;

• Descarte adequado de documentos de acordo com seu grau de classificação;

• Comunicar prontamente à chefia imediata qualquer violação a esta política, suas normas e procedimentos.

Gestores de áreas

Em relação à segurança da Informação, cabe aos gestores de áreas:

• Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob sua gestão;

• Dar ciência, na fase de contratação e formalização dos contratos individuais de trabalho, à responsabilidade do cumprimento da PSI da AMPREV;

• Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;

• Exigir de parceiros, prestadores de serviços e outras entidades externas, a assinatura do termo de confidencialidade referente às informações às quais terão acesso;

• Elaborar, com o apoio do DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO, os procedimentos de segurança da informação relacionados às suas áreas, fornecendo as informações necessárias e mantendo-os atualizados;

• Informar, sempre que necessário, atualizações referentes a processos e/ou cadastros de funcionários para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade;

• Tomar as decisões administrativas referentes aos descumprimentos da PSI da AMPREV.

Comitê Gestor de Segurança da Informação

Cabe ao comitê Gestor de Segurança da Informação:

• Propor melhorias, alterações e ajustes da PSI;

• Propor investimentos relacionados à segurança da informação com o intuito de minimizar os riscos;

• Classificar e reclassificar o nível de acesso às informações sempre que necessário;

• Avaliar incidentes de segurança e propor ações corretivas;

O Setor de Segurança da Informação deverá ser composto por, no mínimo, um colaborador das seguintes áreas:

• Chefe de Gabinete (GAB);

• Unidade de Digitalização Documental - (UDID);

• Chefia de Tecnologia da Informação (DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO);

• Recursos Humanos (RH);

• Procuradoria Jurídica (PROJUR);

• Assessoria Da Presidência.

Remunerar-se-á, ordinariamente, uma vez a cada três meses e extraordinariamente sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a AMPREV.

SETOR DE GESTÃO DE PROCESSOS E TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO.

Cabe ao Setor de Tecnologia e Segurança da Informação:

• Definir as regras para instalação de software e hardware na AMPREV;

• Homologar os equipamentos pessoais (smartphones, tabletes e notebooks) para uso na rede da AMPREV;

• Monitorar os acessos às informações e aos ativos de tecnologia (sistemas, bancos de dados, recursos de rede), tendo como referência a Política e as Normas de Segurança da Informação;

• Mediante informações do RH, manter registro e controle atualizados de todas as liberações de acesso concedidas, providenciando, sempre que demandado formalmente, dentro do horário de expediente da instituição, a pronta suspensão ou

alteração de tais liberações (não somente, tais como: afastamento, contratação, admissão, férias, licença, alteração de lotação);

• Propor as metodologias e processos referentes à segurança da informação, como classificação da informação, avaliação de risco, análise de vulnerabilidades etc.;

• Promover, com o envolvimento da RH, palestras de conscientização dos colaboradores em relação à importância da segurança da informação para o negócio da AMPREV;

• Analisar criticamente incidentes de segurança em conjunto com o Setor de Segurança da Informação;

• Manter comunicação efetiva com o Setor de Segurança da Informação sobre possíveis ameaças e novas medidas de segurança;

• Buscar alinhamento com as diretrizes da organização.

UTILIZAÇÃO DA REDE

O ingresso à rede interna da AMPREV deve ser devidamente controlado para que os riscos de acessos não autorizados e/ou indisponibilidade das informações sejam minimizados.

Assim, é preciso que sejam instauradas algumas regras, listadas a seguir:

A Internet cabeada estará disponível apenas para máquinas e equipamentos de propriedade da AMPREV, com a finalidade restrita à realização de atividades inerentes ao desempenho de tarefas laborais dos colaboradores nesta autarquia;

A Internet sem fio deverá ser segregada, garantindo o isolamento da rede interna da autarquia, com o objetivo de fornecer acesso a sistemas e dados internos apenas para

os colaboradores desempenharem suas tarefas; poderá ter outras redes com acesso apenas à Internet para disponibilizar a visitantes e usuários que não precisam ter acesso aos dados internos. A definição de qual rede o usuário deverá ingressar ficará a cargo da DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO após análise dos requisitos de acesso;

A concessão de acesso à rede sem fio para acesso apenas à Internet se dará através abertura de Chamado no Sistema de Gestão de Demandas no endereço: https://amprev.ap.gov.br/admin/divisão_de_tecnologia_da_informação-calls, por onde passará por análise para aprovação.

O RH ficará responsável por notificar formalmente a DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO sobre desligamentos de colaboradores, para que os acessos deles sejam revogados;

A AMPREV reserva-se o direito de monitorar e registrar o acesso à Internet como forma de inibir a proliferação de programas maliciosos, garantindo a integridade da rede, sistemas e dados internos;

Os equipamentos, tecnologias e serviços fornecidos para o acesso à Internet são de propriedade da AMPREV, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A Internet disponibilizada pela AMPREV aos seus colaboradores, independentemente de sua relação contratual, não pode ser utilizada para fins pessoais, desde que seja autorizada pelo chefe imediato e pela DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO e não prejudique o andamento dos trabalhos nos setores;

Apenas colaboradores devidamente autorizados a falar em nome do AMPREV para meios de comunicação e/ou entidades externas poderão manifestar-se, seja por e-mail, entrevista on-line, documento físico, ligação telefônica etc.;

É proibida a divulgação e/ou o compartilhamento indevido de informações internas, confidenciais e confidenciais restritas em listas de discussão, sites, redes sociais, fóruns, comunicadores instantâneos ou qualquer outra tecnologia correlatada que use a internet como via, de forma deliberada ou inadvertidamente, sob a possibilidade de sofrer penalidades previstas nos procedimentos internos e/ou na forma da lei;

Os colaboradores com acesso à Internet só poderão fazer o download programas necessários às suas atividades no AMPREV e deverão providenciar a licença e o registro necessário desses programas, desde que autorizados pela DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO;

O uso, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente são expressamente proibidos. Qualquer software não autorizado será excluído pela DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO;

Os colaboradores não poderão em hipótese alguma utilizar os recursos da AMPREV para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional;

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Documentos digitais de condutas consideradas ilícitas, como por exemplo, apologia ao tráfico de drogas e pedofilia, são expressamente proibidos e não devem ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;

Os colaboradores não poderão usar os recursos da AMPREV para deliberada ou inadvertidamente propagar qualquer tipo vírus, worms, cavalos de troia, spam, ou programas de controle remoto de outros computadores;

Não serão permitidos os acessos a softwares peer-to-peer (BitTorrent, µtorrent e afins);

Não serão permitidos os acessos a sites de compartilhamento de arquivos, tais como: megaupload, uploaded, bitshare, depositfiles, etc;

Não serão permitidas tentativas de burlar os controles de acesso à rede, tais como utilização de proxy anônimos e estratégias de bypass de Firewall/Proxy;

Não serão permitidos o uso de aplicativos de reconhecimento de vulnerabilidades, análise de tráfego, ou qualquer outro que possa causar sobrecarga ou prejudicar o bom funcionamento e a segurança da rede interna, salvo os casos em que o objetivo for realizar auditorias de segurança, quando a DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO deverá estar devidamente ciente e concedido autorização para tal;

Os arquivos inerentes a AMPREV, obrigatoriamente, deverão ser armazenados na pasta compartilhada de cada setor, localizada no servidor de arquivos, para a garantia de backup destes documentos. É terminantemente proibido armazenar estes tipos de arquivos em equipamentos pessoais e/ou armazenamento em nuvem;

Não será permitida a alteração das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro;

Haverá geração de relatórios de sites e downloads acessados por usuário.

AUDITORIA E CONFIDENCIALIDADE POLÍTICA DE SENHAS

A senha é a forma mais convencional de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identidade do colaborador, evitando que uma pessoa se faça passar por outra.

O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Assim, com o objetivo de orientar a criação de senhas seguras, estabelecem-se as seguintes regras:

A senha é de total responsabilidade do colaborador, sendo expressamente proibida sua divulgação ou empréstimo, devendo a mesma, ser imediatamente alterada no caso de suspeita de sua divulgação;

A senha inicial só será fornecida via chamado, solicitado pelo gerente e/ou coordenador da área, que ficará responsável de transferir as credenciais. As credenciais não poderão ser fornecidas por telefone, comunicador instantâneo ou qualquer outra forma que não assegure a identidade do colaborador;

É proibido o compartilhamento de funções de administração de sistemas;

As senhas não devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor etc.);

As senhas deverão seguir os seguintes pré-requisitos:

• Tamanho mínimo de oito caracteres;

• Existência de caracteres pertencentes a, pelo menos, três dos seguintes grupos: letras maiúsculas, letras minúsculas, números e caracteres especiais;

• Não devem ser baseadas em informações pessoais de fácil dedução (aniversário, nome do cônjuge etc).

O acesso do usuário deverá ser imediatamente cancelado nas seguintes situações: • Desligamento do colaborador;

•. Quando, por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação.

Para os cancelamentos acima mencionados, do Recursos Humanos (RH) ficará responsável por informar prontamente a DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO acerca dos desligamentos e mudança de função dos colaboradores.

O usuário não poderá logar em mais de uma máquina simultaneamente dentro do domínio do AMPREV, somente em algumas exceções, com a devida aprovação do DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO.

E-MAIL

O e-mail é uma das principais formas de comunicação. No entanto, é, também, uma das principais vias de disseminação de malwares, phishing etc, por isso, surge a necessidade de normatização da utilização deste recurso.

O e-mail corporativo é destinado a fins profissionais, relacionados às atividades dos colaboradores;

Os e-mails enviados ou recebidos de endereços externos poderão ser monitorados com o intuito de bloquear spams, malwares ou outros conteúdos maliciosos que violem a Política de Segurança da Informação;

É proibido enviar, com endereço eletrônico corporativo, mensagens de cunho particular, propagandas, vídeos, fotografias, músicas, mensagens do tipo “corrente”, campanhas ou promoções etc.;

É proibido abrir arquivos com origens desconhecidas anexados a mensagens eletrônicas;

É proibido enviar qualquer mensagem por meios eletrônicos que torne o AMPREV vulnerável a ações civis ou criminais;

É proibido falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;

Produzir, transmitir ou divulgar mensagem que:

• Contenha ameaças eletrônicas, como: spam, phishing, mail bombing, malwares;

• Contenha arquivos com código executável (.exe, .cmd, .pif, .js, .hta, .src, cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;

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

• Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

• Vise burlar qualquer sistema de segurança;

• Vise vigiar secretamente ou assediar outro usuário;

• Vise acessar informações confidenciais sem explícita autorização do proprietário;

• Tenha conteúdo considerado impróprio, obsceno ou ilegal;

• Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

• Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

O uso de e-mails pessoais é aceitável, se usado com moderação, em caso de necessidade e quando:

• Não contrariar as normas aqui estabelecidas;

• Não interferir, negativamente, nas atividades profissionais individuais, ou de outros colaboradores;

• Não interferir, negativamente, na AMPREV e na sua imagem.

• Não redirecionar e-mail corporativos para e-mail pessoais, com qualquer objetivo.

DO USO DAS ESTAÇÕES DE TRABALHO

As estações de trabalho devem permanecer operáveis durante o maior tempo possível para que os colaboradores não tenham suas atividades prejudicadas. Assim, algumas medidas de segurança devem ser tomadas, são elas:

É de responsabilidade do colaborador do equipamento zelar por ele, mantendo-o em boas condições;

Não é permitido personalizar o equipamento por adesivos, fotos, riscos, raspar e retirar a etiqueta de patrimônio;

É vedada a abertura de computadores para qualquer tipo de reparo pelos colaboradores. Caso seja necessário, o reparo deverá ser feito pela equipe de suporte da DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO;

As estações de trabalho só estarão acessíveis aos colaboradores através de contas de usuário limitadas.

É proibida a instalação de softwares ou sistemas nas estações de trabalho pelos usuários finais. Este procedimento só poderá ser realizado pela equipe de suporte da DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO após análise e/ou aprovação da gerência;

É proibida a instalação de softwares que não possuam licença e/ou não sejam homologados pela equipe da DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO;

As estações de trabalho devem permanecer bloqueadas nos períodos de ausência do colaborador;

Os documentos e arquivos relativos à atividade desempenhada pelo colaborador deverão, sempre que possível, serem armazenados em local próprio no servidor da rede, o qual possui rotinas de backup e controle de acesso adequado;

Documentos críticos e/ou confidenciais só podem ser armazenados no servidor da rede local, nunca no disco local da máquina;

É proibido o uso de estações de trabalho para:

• Tentar ou obter acesso não autorizado a outro computador, servidor ou rede; exceto com pedido direto da Presidência.

• Burlar quaisquer sistemas de segurança;

• Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

• Cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

• Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

A divisão de tecnologia da informação não se responsabiliza por prestar manutenção ou instalar softwares em computadores pessoais;

As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário, que poderá ser acessada pela divisão de tecnologia da informação a pedido da Presidência.

DO USO DE EQUIPAMENTOS PARTICULARES E DISPOSITIVOS MÓVEIS

O objetivo da AMPREV é maximizar a agilidade e eficiência da realização das tarefas dos colaboradores, contando com todos os recursos de equipamentos disponíveis, mas não pode deixar de considerar os requisitos de segurança da informação, por isso estabelece algumas regras para o uso de equipamentos de propriedade particular e de dispositivos móveis.

Caracteriza-se por dispositivo móvel qualquer equipamento eletrônico com atribuições de mobilidade, seja de propriedade da AMPREV ou particular com prévia aprovação e permissão pela DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO, como: notebooks, smartphones, pen drives e outros.

Todas as regras do tópico “Estações de Trabalho” se enquadram nesta seção, adicionalmente a:

Só será autorizado o uso de notebooks e dispositivos móveis para acesso à internet do AMPREV mediante autorização do chefe imediato via CHAMADO e liberação da DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO;

O uso de notebooks e dispositivos móveis para fins de acesso à rede de Internet do AMPREV será realizado mediante cadastro de usuário através da abertura de CHAMADO no endereço https://amprev.ap.gov.br/admin/dinfo-calls e autorização do chefe imediato com aprovação da DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO.

A DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO tem o direito de, periodicamente, auditar os equipamentos utilizados no AMPREV, visando proteger suas informações bem como garantir que aplicativos ilegais não estejam sendo usados no AMPREV;

É de responsabilidade do proprietário a instalação do Sistema Operacional que será utilizado, bem como dos aplicativos a serem utilizados no notebook, celulares etc., salvo exceções de aplicativos específicos autorizados pelo DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO;

É de responsabilidade do proprietário usar somente aplicativos legalizados em seu notebook, celular etc.;

Não podem ser executados nos notebooks, celulares etc. Aplicativos de característica maliciosa, que visam comprometer o funcionamento da rede, acesso a informações sem a devida permissão ou informações confidenciais;

É proibido o armazenamento de informações proprietárias da AMPREV que não sejam de uso pessoal do proprietário do notebook. Todos os arquivos que pertençam ao

AMPREV não podem ser armazenados no disco rígido do notebook e/ou em dispositivos de armazenamento móvel, como exemplo: pen drive e/ou armazenamento em nuvem pessoal, sem a autorização da área responsável pelos dados. Estes arquivos devem sempre ser armazenados no servidor de arquivos local na pasta do seu setor disponibilizado na rede através do seu login de acesso;

Mesmo nos computadores portáteis fornecidos pelo AMPREV, é proibido o armazenamento de informações confidenciais e confidenciais restritas no disco rígido do equipamento;

É proibida a inclusão de smartphones na rede corporativa do AMPREV. Estes equipamentos deverão ter seu acesso restrito à rede de Internet;

HOME OFFICE / TELE TRABALHO

O colaborador deverá tomar ciência do documento do DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO - Minuta Trabalho Remoto". As dúvidas sobre diretrizes de trabalho remoto deverão ser sanadas com a Divisão de Tecnologia da Informação.

USO DE IMPRESSORAS / IMPLANTAÇÃO DO PAPEL ZERO

O uso de impressoras na AMPREV deve seguir algumas regras:

É proibida a impressão desnecessária e xerox de documentos de cunho pessoal e/ou ilegal;

A configuração e manutenção das impressoras só podem ser realizadas pela Equipe prestadora de Serviços contratadas pela DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO;

A instalação das impressoras deverá ser realizada através de CHAMADO;

O chefe de cada setor / unidade será o responsável pela forma de utilização da impressora localizada na sala, inclusive para responder a questionamentos como impressões/xerox excessivas;

As impressoras devem estar ligadas em tomadas específicas para elas, indicada pela GEAD;

DOS BACKUP'S

Um dos procedimentos mais básicos da Segurança da Informação é a implantação de uma Política de Backup (cópia de segurança).

Uma organização tem que estar preparada para recuperar ou restaurar, todos os seus dados de forma íntegra caso um incidente de perda de dados venha a ocorrer.

Assim, estabelecem-se as regras:

Todo sistema ou informação relevante para a operação dos negócios da AMPREV deve possuir cópia dos seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações da instituição;

A DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO ficará responsáveis por classificar os dados de acordo com a relevância e provocar a DIVISÃO DE TECNOLOGIA DA

INFORMAÇÃO sobre a necessidade de backup deles, sugerindo o tempo de retenção destas cópias;

Todos os backups devem ser automatizados por sistemas de agendamento para que sejam, preferencialmente, executados fora do horário comercial, períodos de pouco ou nenhum acesso de usuários ou processos aos sistemas de informática;

As mídias físicas de backup que não estão em uso devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e, preferencialmente, distantes o máximo possível do Datacenter;

Toda infraestrutura de suporte aos processos de backup e restauração deve possuir controles de segurança para prevenção contra acessos não autorizados, bem como mecanismos que assegurem seu correto funcionamento;

A divisão de tecnologia da informação prepara semestralmente um plano para execução de testes de restauração de dados, que deve ter escopo definido em conjunto com as áreas de negócio. Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos;

Na situação de erro de backup e/ou Restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado o problema. Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser executados apenas mediante justificativa de necessidade e aprovação da área de negócios, junto a DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO.

TABELA TEMPORALIDADE DE DADOS PROCESSOS ADMINISTRATIVOS E BENEFÍCIOS.

Classificação e Tabela de Temporalidade e Destinação de Documentos Relativos às atividades-meio efim do Regime Próprio de Previdência do estado do Amapá – AMPREV.

ÓDIGO	DESCRIÇÃO	PRAZOS DE GUARDA		DESTINAÇÃO FINAL	OBSERVAÇÕES
		FASE CORRENTE	FASE INTERMEDIÁRIA		
100	CONCESSÃO DE BENEFÍCIO PRECIDENCIÁRIO				
101	APOSENTADORIAS	ENQUANTO VIGORAR	10 ANOS	ELIMINAÇÃO	OS PROCESSO DE APOSENTADORIAS QUE DÃO ORIGEM AO BENEFÍCIO PODERÃO SER JUNTADOS AO PROCESSO E SEGUIR A TEMPORALIDADE DESTE. PROCESSOS INDEFERISOS PODERÃO SER ELIMINADOS APÓS 10 ANOS DO INDEFERIMENTO.
102	AUXÍLIOS	ENQUANTO VIGORAR	10 ANOS	ELIMINAÇÃO	PROCESSOS INDEFERIDOS PODERÃO SER ELIMINADOS APÓS

Rua Binga Uchoa, 10 - Centro - CEP 68900-090 - Macapá/AP - CNPJ 03.281.445/0001-85
Fone: (96) 4009-2400

					10 ANOS DO INDEFERIMENTO.
103	PENSÕES	ENQUANTO VIGORAR	10 ANOS	ELIMINAÇÃO	PROCESSOS INDEFERIDOS PODERÃO SER ELIMINADOS APÓS 10 ANOS DO INDEFERIMENTO.
104	CONCESSÃO DE ENEFÍCIOS ASSISTENCIAIS	ENQUANTO VIGORAR	10 ANOS	ELIMINAÇÃO	PROCESSOS INDEFERIDOS PODERÃO SER ELIMINADOS APÓS 10 ANOS DO INDEFERIMENTO.
200	ATIVIDADE MÉDICO PERICIAL				
201	AVALIAÇÃO MÉDICO PERICIAL	ENQUANTO VIGORAR	10 ANOS	ELIMINAÇÃO	PROCESSOS INDEFERIDOS PODERÃO SER ELIMINADOS APÓS 10 ANOS DO INDEFERIMENTO.
202	CREDENCIAMENTO E DESCREDENCIAMENTO DE MÉDICOS E ENTIDADES DE SAÚDE	ATÉ A APROVAÇÃ O DE CONTAS OU APRESENT AÇÃO DO RELATÓRIO DE GESTÃO	10 ANOS APÓS A APROVAÇÃO DE CONTAS OU APRESENTAÇÃ O DO RELATÓRIO DE GESTÃO	ELIMINAÇÃO	PARA OS CASOS NÃO EFETIVADOS, ELIMINAR DEPOIS DE 5 ANOS.
300	GERENCIAMENTO FINANCEIRO DOS BENEFÍCIOS E RECURSOS				
301	PAGAMENTO DE BENEFÍCIOS PREVIDENCIÁRIOS E ASSISTENCIAIS	5 ANOS	5 ANOS	ELIMINAÇÃO	
302	EMPRÉSTIMO CONSIGNADO				

Rua Binga Uchoa, 10 - Centro - CEP 68900-090 - Macapá/AP - CNPJ 03.281.445/0001-85
Fone: (96) 4009-2400

302.1	HABILITAÇÃO DE INSTITUIÇÕES FINANCEIRAS	ENQUANTO VIGORA	5 ANOS	GUARDA PERMAN ENTE	
302.2	DEVOLUÇÃO AO ERÁRIO	5 ANOS	10 ANOS	ELIMINAÇÃO	OS PROCESSOS DE RECOLHIMENTO DE DESCONTOS INDEVIDOS, PODEM SER ELIMINADOS APÓS 10 ANOS DO RECOLHIMENTO DO RECURSO PARA O ERÁRIO.
310	COMPENSAÇÃO PREVIDENCIÁRIA	ENQUANTO ESTIVER SENDO PAGO	10 ANOS	ELIMINAÇÃO	
320	GERENCIAMENTO E FISCALIZAÇÃO DO BENEFÍCIO				
321	ATUALIZAÇÃO DE BENEFÍCIO	ENQUANTO ESTIVER SENDO PAGO	10 ANOS	ELIMINAÇÃO	
322	RECURSO ADMINISTRATIVO DE BENEFÍCIO	ATÉ DECISÃO DO RECURSO	10 ANOS	ELIMINAÇÃO	
323	REVISÃO E CORREÇÃO POR INDÍCIOS DE IRREGULARIDADE	ATÉ A DECISÃO DA REVISÃO OU CORREÇÃO	10 ANOS	ELIMINAÇÃO	
330	PRESTAÇÃO DE SERVIÇOS ASSISTENCIAIS				
331	ESTUDO SOCIAL	ENQUANTO O BENEFÍCIO ORIGINÁRIO ESTIVER SENDO PAGO	10 ANOS	ELIMINAÇÃO	
332	PESQUISA SOCIAL	5 ANOS	10 ANOS	PERMANENTE	
333	ORIENTAÇÃO, ASSESSORIA E CONSULTORIA	1 ANO	5 ANOS	ELIMINAÇÃO	
334	HABILITAÇÃO E REABILITAÇÃO PROFISSIONAL	ENQUANTO DURAR A RELAÇÃO DO SEGURADO COM A	10 ANOS	ELIMINAÇÃO	

		PREVIDÊNCIA SOCIAL			
400	PROMOÇÃO DA EDUCAÇÃO PREVIDENCIÁRIA				
401	DIVULGAÇÃO DA INFORMAÇÃO PREVIDENCIÁRIA	2 ANOS	3 ANOS	GUARDA PERMANENTE	DEVE SER MANTIDO UM EXEMPLAR DO MATERIAL DE DIVULGAÇÃO.
402	ACOMPANHAMENTO E AVALIAÇÃO DA EDUCAÇÃO PREVIDENCIÁRIA	2 ANOS	3 ANOS	ELIMINAÇÃO	FICHA DE INSCRIÇÃO E OS CONJUNTOS DOCUMENTAIS REFERENTES A ORÇAMENTO E FINANÇAS DEVERÃO SER MANTIDOS ATÉ A PRESTAÇÃO DE CONTAS OU APRESENTAÇÃO DO RELATÓRIO DE GESTÃO NA FASE CORRENTE E 5 ANOS APÓS A PRESTAÇÃO DE CONTAS OU 10 ANOS APÓS A APRESENTAÇÃO DO RELATÓRIO DE

					GESTÃO NA FASE INTERMEDIÁRIA.
403	FORMAÇÃO DE DISSEMINADORES EM EDUCAÇÃO PREVIDENCIÁRIA	2 ANOS	3 ANOS	GUARDA PERMANENTE	
500	ADMINISTRAÇÃO GERAL				
501	MODERNIZAÇÃO E REFORMA ADMINISTRATIVA - INCLUEM-SE DOCUMENTOS REFERENTES AOS PROJETOS, ESTUDOS E NORMAS RELATIVOS À ORGANIZAÇÃO E MÉTODOS, REFORMA ADMINISTRATIVA E OUTROS PROCEDIMENTOS QUE VISEM À MODERNIZAÇÃO DAS ATIVIDADES DA AMPREV	ENQUANTO VIGORA	5 ANOS	GUARDA PERMANENTE	
502	PLANO INSTITUCIONAL - INCLUEM-SE DOCUMENTOS REFERENTES AO PLANEJAMENTO E AOS PLANOS, PROGRAMAS E PROJETOS DE TRABALHO GERAIS.	ENQANTO VIGORA	5 ANOS	GUARDA PERMANENTE	PROGRAMAS E/OU PROJETOS DE TRABALHO, CLASSIFICAR NO ASSUNTO ESPECÍFICO.
503	RELATÓRIO DE ATIVIDADES	ENQANTO VIGORA	GUARDA PERMANENTE	GUARDA PERMANENTE	SÃO PASSÍVEIS DE DESCARTE OS RELATÓRIOS CUJAS INFORMAÇÕES ENCONTRAM-SE RECAPITULADAS EM OUTROS.
504	ACORDO. AJUSTE. CONTRATO. CONVÊNIO - INCLUEM-SE DOCUMENTOS REFERENTES A UM	ENQUANTO VIGORA	5 ANOS	GUARDA PERMANENTE	QUANTO AOS DEMAIS ACORDOS,

	ACORDO, AJUSTE, CONTRATO E/OU CONVÊNIO, IMPLEMENTADOS OU NÃO, TAIS COMO PROJETOS, RELATÓRIOS TÉCNICOS, PRESTAÇÕES DE CONTAS E ADITAMENTOS, QUE ABRANJAM A EXECUÇÃO DE VÁRIAS ATIVIDADES AO MESMO TEMPO.				AJUSTES, CONTRATOS E/OU CONVÊNIOS, CLASSIFICAR NO ASSUNTO ESPECÍFICO.
505	OUTROS DOCUMENTOS REFERENTES À COMUNICAÇÃO COM A IMPRENSA	1 ANO		DESCARTE	
506	DIVULGAÇÃO INTERNA DE POLÍTICAS E ATOS ADMINISTRATIVOS E OUTROS	2 ANOS		DESCARTE	
507	LEGISLAÇÃO - INCLUEM-SE NORMAS, REGULAMENTAÇÕES, DIRETRIZES, ESTATUTOS, REGULAMENTOS, PROCEDIMENTOS, ESTUDOS E DECISÕES DE CARÁTER GERAL.	ENQUANTO VIGORA	5 ANOS	GUARDA PERMANENTE	
508	BOLETIM - INCLUEM-SE BOLETINS ADMINISTRATIVOS, DE PESSOAL E DE SERVIÇO.	10 ANOS	10 ANOS	GUARDA PERMANENTE	
509	IDENTIFICAÇÃO FUNCIONAL - INCLUEM-SE CARTEIRAS, CARTÕES, CRACHÁS E CREDENCIAIS.	ENQUANTO O SERVIDOR PERMANECER		DESCARTE	
510	DIVULGAÇÃO RELAÇÃO COM ÓRGÃO NORMALIZADOR DA ADMINISTRAÇÃO PÚBLICA - INCLUEM-SE OBRIGAÇÕES TRABALHISTAS E ESTATUTÁRIAS.	5 ANOS	5 ANOS	DESCARTE	
511	CURSO PROMOVIDO POR OUTRA INSTITUIÇÃO NO BRASIL.	5 ANOS		DESCARTE	
512	FOLHA DE PAGAMENTO	5 ANOS	95 ANOS	DESCARTE	
600	ORGANIZAÇÃO E FUNCIONAMENTO				

Rua Binga Uchoa, 10 - Centro - CEP 68900-090 - Macapá/AP - CNPJ 03.281.445/0001-85
Fone: (96) 4009-2400

601	NORMA, REGULAMENTO, DIRETRIZ, PROCEDIMENTO, ESTUDO OU DECISÃO DE CARÁTER GERAL REFERENTE À ORGANIZAÇÃO E FUNCIONAMENTO	ENQUANTO VIGORA	5 ANOS	GUARDA PERMANENTE	
602	REGISTRO NOS ÓRGÃOS COMPETENTES	ENQUANTO VIGORA	GUARDA PERMANENTE	GUARDA PERMANENTE	
603	REGIMENTO. REGULAMENTO. ESTATUTO. ORGANOGRAMA. ESTRUTURA	ENQUANTO VIGORA	5 ANOS	GUARDA PERMANENTE	
700	COMISSÃO. CONSELHO. GRUPO DE TRABALHO. COMITÊ				
701	ATO DE CRIAÇÃO, ATA E RELATÓRIO DE COMISSÃO, CONSELHO, GRUPO DE TRABALHO OU COMITÊ - INCLUEM-SE DOCUMENTOS REFERENTES À CRIAÇÃO DE COMISSÕES, CONSELHOS, GRUPOS DE TRABALHO E COMITÊS, NA RIOPRETOPREV OU EM ÓRGÃOS COLEGIADOS E DE DELIBERAÇÃO COLETIVA, BEM COMO AQUELES RELATIVOS AO EXERCÍCIO DE SUAS FUNÇÕES, TAIS COMO: ATAS E RELATÓRIOS TÉCNICOS.	4 ANOS	5 ANOS	GUARDA PERMANENTE	
702	OUTROS DOCUMENTOS REFERENTES À COMISSÃO, CONSELHO, GRUPO DE TRABALHO OU COMITÊ	4 ANOS	5 ANOS	GUARDA PERMANENTE	

Rua Binga Uchoa, 10 - Centro - CEP 68900-090 - Macapá/AP - CNPJ 03.281.445/0001-85
Fone: (96) 4009-2400

SEGURANÇA DO AMBIENTE DE TI ESTRUTURA FÍSICA DO DATA CENTER

Os equipamentos (servidores) que armazenam sistemas da AMPREV estão em área protegida – Data Centers localizados na sede da autarquia.

Todos os sistemas ou equipamentos classificados como críticos devem ser mantidos em áreas seguras do Data Center;

A entrada aos Data Centers tem acesso devidamente controlado e monitorado;

As permissões de acesso físico às áreas restritas de TIC por outras áreas e terceiros, devem ter previamente autorização da gerência de informática;

As áreas do Data Center devem ser protegidas com barreiras de segurança ou mecanismos de acesso, de forma a impedir o acesso não autorizado;

A porta do Data Center deve permanecer fechada, com mecanismo de autenticação individual quando possível.

O acesso às dependências dos Data Centers com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir de autorização da equipe de Segurança e mediante supervisão;

O acesso ao Datacenter sem as devidas identificações à DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO, só poderá ocorrer em emergências, quando a segurança física do Datacenter for comprometida, como por incêndio, inundação, abalo da estrutura predial, temperatura fora do padrão ou quando o sistema de autenticação não estiver funcionando;

Caso haja necessidade do acesso não emergencial, o requisitante deve solicitar autorização com antecedência de no mínimo 24 horas à DIVISÃO DE TECNOLOGIA

DA INFORMAÇÃO através de CHAMADO no endereço: https://amprev.ap.gov.br/admin/divisão de tecnologia da informação-calls;

O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente, somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a mesma deve ser autorizada pela DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO.

ESTRUTURA LÓGICA DO DATA CENTER

Na política de segurança da Informação estabelecida pela AMPREV, define-se que os analistas de TI, devem ser os únicos a terem permissão para ler/editar as informações, obedecendo as atribuições de sua área de atuação.

O objetivo da segurança lógica no Data Center é proteger os ativos de informações, sistemas ou programas de acesso indevidos e não autorizados;

Somente os colaboradores de outras áreas, credenciados e autorizados pela DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO e pelo Setor Segurança da Informação podem ter acesso aos dados armazenados, de outras áreas;

Os logs dos ativos de rede são monitorados pelo sistema ids pelo firewall constantemente a fim de evitar acessos indevidos.

VIOLAÇÃO DA POLÍTICA E PENALIDADES

No caso de não cumprimento das normas estabelecidas nesta Política de Segurança, o funcionário ou colaborador poderá sofrer as seguintes penalidades:

• Advertência verbal: O colaborador será comunicado verbalmente pela Gerência de Informática de que ele está infringindo as normas da Política de Segurança da Informação da AMPREV e será recomendado à leitura desta norma.

• Advertência formal A primeira notificação será enviada ao colaborador informando o descumprimento da norma, com a indicação precisa da violação cometida. A segunda notificação será encaminhada para a chefia imediata do infrator e a Presidência.

• Penalidades As penalidades aplicadas ao colaborador, será definida pela DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO em conjunto com a Presidência, de acordo com a Lei nº 14010 de 10/06/2020 (LGPD);

ADEQUAÇÃO À LEI Nº 13.709, DE 14 DE AGOSTO DE 2018

A Lei nº 13.709, de 14 de agosto de 2018, foi promulgada com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. A LGPD fala sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais, conferida através do link: https://amprev.ap.gov.br/lei-geral-de-protecao-de-dados-lgpd

CONSIDERAÇÕES FINAIS

As dúvidas decorrentes de fatos não descritos nesta Política de Segurança da Informação deverão ser encaminhadas a GEAD para avaliação e decisão.

Esta PSI entra em vigor a partir da data de publicação e pode ser alterada a qualquer tempo, por decisão da Governança, mediante o surgimento de fatos relevantes que apareçam ou não tenham sido contemplados neste documento.

3. REFERÊNCIAS

As referências utilizadas para concepção desta Política foram:

- ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação – Técnicas de segurança – Código deprática para controles de segurança da informação.
- Instrução Normativa GSI/PR Nº 1 – 13/06/2008.
- Normas Complementares da IN GSI/PR Nº 1, DSIC/GSIPR Nº 1 e Nº 5.
- Política de Segurança da Informação e Comunicações da DATAPREV.
- Resolução Nº 1.168/2017-GP do Tribunal de Justiça do Estado do Amapá – TJAP
- Política de Segurança da Informação (13/08/2013) do Instituto Federal de Educação, Ciência eTecnologia Farroupilha.
- PORTARIA Nº 486/2017 – Política de Segurança da Informação do Instituto de Previdência Socialdos Servidores Públicos Municipais de Santos.
- Lei nº 13.709, de 14.08.2018- Lei Geral de Proteção de Dados – LGPD;
- ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança da Informação – Sistemas de Gestão de Segurança de TIC;
- ABNT NBR ISO/IEC 27002:2013 - Tecnologia da Informação — Técnicas de Segurança;