POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SERGIPEPREVIDÊNCIA

SERGIPE PREVIDÊNCIA

SECRETARIA DE ESTADO DA ADMINISTRAÇÃO

SERGIPE GOVERNO DO ESTADO

Sumário

Introdução

Conforme definição da norma ABNT NBR ISO/IEC 27002:2005**,** "*A **informação** é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida. [...] A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente."*

De acordo com a mesma norma, *"**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."*

Os princípios da segurança da informação abrangem, basicamente, os seguintes aspectos:

Integridade: somente alterações, supressões e adições que forem autorizadas pela instituição devem ser realizadas nas informações;

Confidencialidade: somente pessoas devidamente autorizadas pela instituição devem ter acesso à informação;

Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

Ainda de acordo com a norma ABNT NBR ISO/IEC 27002:2005, *"A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio."*

A violação desta política de segurança é qualquer ato que:

- Exponha o Instituto a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados /ou de informações ou ainda da perda de equipamento.
- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.
- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

Termos e Definições

Acesso: Ato de ingressa, transitar, conhecer ou consultar a informação, bem como a acessibilidade de usar os ativos de informação de um órgão ou entidade.

Informação: Conjunto de dados, textos, imagens, métodos, sistemas ou quais quer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado.

Usuário Interno: O empregado, o servidor, o contratado, o estagiário ou o conveniado da Administração Pública, que no exercício de suas funções, tenham acesso a informações produzidas ou recebidas pelo instituto, fazendo uso de recursos computacionais.

Usuário Externo: A pessoa física ou pessoa jurídica, contrata direta ou indiretamente, que tenha acesso concedido a informações produzidas ou recebidas pelo instituto, e que não seja caracterizado como Usuário Interno, que fazem uso de recursos computacionais.

Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização. [ISO/IEC 13335-1:2004]

Ativo: qualquer coisa que tenha valor para a organização. [ISO/IEC 13335- 1:2004]

Ativo de Informação: qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio.

Controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. [ABNT NBR ISO/IEC 27002:2005]

Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação. [ISO/IEC TR 18044:2004]

Incidente de segurança da informação: indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação. [ISO/IEC TR 18044:2004]

Risco: combinação da probabilidade de um evento e de suas consequências. [ABNT ISO/IEC Guia 73:2005]

Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. [ABNT NBR ISO/IEC 27002:2005

Ativos: São equipamentos específicos que permitem estruturar uma rede de computadores, conectando as máquinas da empresa umas às outras e também conectando a organização à internet. Tecnicamente, eles são responsáveis por gerar e receber dados, além de converter sinais eletrônicos ou ópticos. São esses dispositivos que geram todo o tráfego de dados que passa pelos equipamentos passivos da rede.

Login: identificação de usuário dentro do sistema. Deve ser único para cada usuário do sistema

Token: equipamento utilizado para armazenar a chave privada do usuário, certificado privado do usuário, realizar a assinatura digital do usuário, ou fornecer código de acesso específico, visando a autenticação de um usuário no sistema.

Active Directory: Serviço de diretório do Windows que permite o controle de autenticação de usuários de forma integrada. Dentre outras funções, gerencia os *logins*, senhas e grupos.

Classificação da Informação

Informação Pública: É toda informação que pode ser acessada por servidores da entidade, usuários, fornecedores, prestadores de serviços e cidadão em geral, com linguagem e formato dedicado à divulgação, sendo seu caráter informativo.

Informação Interna: É uma informação a qual não tem interesse em divulgar. É toda informação que só pode ser acessada por servidores, órgãos públicos e prestadores de serviços. São informações que, possuem um grau de confidencialidade que pode comprometer a imagem do instituto, mas não com a mesma magnitude de uma informação confidencial ou restrita.

Informação Confidencial: É toda informação considerada crítica e que pode ser acessada apenas por servidores. A divulgação não autorizada dessa informação pode causar impacto financeiro, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais aos seus servidores e segurados. É sempre restrita a um grupo específico de pessoas, podendo ser este composto por servidores, segurados e/ou fornecedores.

Informação Restrita: É toda informação que pode ser acessada somente por servidores da entidade explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos a entidade e/ou comprometer a gestão da empresa.

É de responsabilidade do Gestor/Diretor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação geradas por sua área.

Todo Gestor/Diretor deve orientar seus subordinados a não circularem informações, mídias de armazenamento e relatórios, considerados confidenciais e/ou restritas, em locais de fácil acesso, a exemplo de relatórios deixados nas impressoras, bem como sobre suas mesas.

Objetivo

Estabelecer os conceitos e diretrizes de segurança da informação, visando à utilização da infraestrutura tecnológica do SERGIPEPREVIDENCIA, de acordo com princípios éticos e legais, bem como atitudes adequadas para proteger as informações do instituto e de seus segurados. A política busca preservar os seus ativos de informação, assim como a sua imagem institucional.

São objetivos da Política de Segurança da Informação do SERGIPEPREVIDENCIA:

a) Estabelecer diretrizes que permitam aos colaboradores e fornecedores do RPPS seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da Autarquia e do indivíduo;
b) Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento;
c) Preservar as informações do RPPS quanto à integridade, confidencialidade e disponibilidade;
d) Definir ações e responsabilidades por partes dos servidores;

Abrangência

Os objetivos e diretrizes estabelecidos nesta Política de Segurança da Informação serão aplicados em todo o instituto e deverão ser observados por todos os servidores, órgão, colaboradores e também por fornecedores e prestadores de serviço quando pertinente ou aplicável a área da informação, em qualquer meio ou suporte, incluindo trabalhos executados remotamente, que utilizam o ambiente de processamento do SERGIPEPREVIDENCIA.

Este documento, dentre outros que possam estar vinculados, dá ciência a cada envolvido de que os ambientes, sistemas, recursos computacionais e redes informacionais do instituto poderão ser monitorados e gravados, com prévia informação, conforme previsto na legislação brasileira.

É obrigação de cada colaborador se manter atualizado em relação a esta Política de Segurança da Informação, buscando orientação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Diretrizes

Considerando a informação como sendo um bem do instituto, um dos recursos críticos para a realização das atividades, as diretrizes a seguir, constituem os principais pilares do sistema de segurança da informação do SERGIPEPREVIDENCIA.

Proteção da Informação

Define-se como necessária a proteção das informações da instituição ou sob sua custódia como fator primordial nas atividades profissionais de cada servidor, segurado, estagiário ou prestador de serviços, sendo que:

a) Os servidores devem assumir uma postura proativa no que diz respeito à proteção das informações do SERGIPEPREVIDENCIA e devem estar atentos a ameaças externas, bem como fraudes, roubo de

informações, e acesso indevido a sistemas de informação sob responsabilidade do SERGIPEPREVIDENCIA;

b) As informações não podem ser transportadas em qualquer meio físico, sem as devidas proteções;
c) Assuntos confidenciais não devem ser expostos publicamente;
d) Senhas, contas de usuário e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados;
e) Somente softwares homologados podem ser utilizados no ambiente computacional do SERGIPEPREVIDENCIA;
f) Documentos impressos e arquivos contendo informações confidenciais devem ser armazenados e protegidos. O descarte deve ser feito na forma da legislação pertinente;
g) Todo usuário, para poder acessar dados das redes de computadores do SERGIPEPREVIDENCIA, deverá possuir uma conta de usuário atrelado à uma senha previamente cadastrada, sendo este pessoal e intransferível, ficando vedada a utilização de conta de acesso genéricos ou comunitários;
h) Não é permitido o compartilhamento de pastas nos computadores de servidores da instituição. Os dados que necessitam de compartilhamento devem ser alocados nos servidores apropriados, atentando às permissões de acesso aplicáveis aos referidos dados;
i) Todos os dados considerados como imprescindíveis aos objetivos do SERGIPEPREVIDENCIA devem ser protegidos através de rotinas sistemáticas e documentadas de cópia de segurança, devendo ser submetidos à testes periódicos de recuperação;

Privacidade da Informação

Define-se como necessária a proteção da privacidade das informações, aquelas que pertencem aos seus segurados e que são manipuladas ou armazenadas nos meios às quais o SERGIPEPREVIDENCIA detém total controle administrativo, físico, lógico e legal. As diretivas abaixo refletem os valores institucionais do SERGIPEPREVIDENCIA e reafirmam o seu compromisso com a melhoria contínua desse processo:

a) As informações são coletadas de forma ética e legal, com o conhecimento do segurado, para propósitos específicos e devidamente informados;
b) As informações são acessadas somente por pessoas autorizadas e capacitadas para seu uso adequado;
c) As informações podem ser disponibilizadas a empresas contratadas para prestação de serviços, sendo exigido de tais organizações o cumprimento de nossa política e diretivas de segurança e privacidade de dados;
d) As informações somente são fornecidas a terceiros, mediante autorização prévia da diretoria executiva ou para o atendimento de exigência legal ou regulamentar;
e) As informações e dados constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais só são fornecidos aos próprios interessados, mediante solicitação formal, seguindo os requisitos legais vigentes.

Permissões e Senhas

Para o acesso aos recursos tecnológicos do SERGIPEPREVIDENCIA será exigido, identificação e senha exclusiva de cada colaborador, permitindo assim o controle dos acessos a rede de computares e sistemas.

É proibido o compartilhamento de login entre os colaboradores. O uso de login e senha de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade)

As permissões de cada usuário devem ser concedidas de forma que o usuário tenha somente o privilégio necessário para desempenhar suas funções.

É proibido o compartilhamento de login e senha com funções de administração da rede, computadores ou sistemas, bem como conceder tais privilégios à conta de usuário.

Recomenda-se como boa prática de segurança que, ao realizar o primeiro acesso ao ambiente de rede local, o usuário seja direcionado a trocar imediatamente a sua senha.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados (tokens).

A senha de acesso a rede de computadores segue requisitos de complexibilidade de tamanho e considera caracteres de três categorias:

- Letras maiúsculas de A a Z;
- Letras minúsculas de a a z;
- Base 10 dígitos (0 a 9)
- Caracteres especiais (não alfanuméricos): (~!@#$%^&*_-+='|\() {} []:;' <>,.? /);
- Qualquer caractere Unicode categorizado como um caractere alfabético, mas não em maiúsculas ou minúsculas.

As contas de usuários (login) e as senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (word, excel, bloco de notas, etc.), compreensíveis por linguagem humana (não criptografados) ou sem uso de senha que possa protege-los. As senhas não devem ser baseadas em informações pessoais, como nome próprio, nome de familiares, data de nascimento, endereço, placa de veículo, nome do departamento ou combinações óbvias de teclado, como, “abcdef”, “123456”, entre outras.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

Caso o usuário esqueça sua senha, ele deverá requisitar formalmente a criação de uma nova senha provisória, onde o sistema solicitará a redefinição da senha provisória no primeiro acesso, imediatamente após a redefinição da senha. Pode ainda o usuário comparecer ao setor de informática para realizar o cadastro da nova senha.

Todos os acessos de um usuário podem ser bloqueados pelo setor de informática caso seja identificado uso suspeito do login/senha ou se tornarem desnecessários. O mesmo se aplica em caso de desligamento do usuário ou período de férias, previamente comunicado pelo setor de recursos humanos.

O setor de informática é responsável pela definição e pela divulgação das regras de formação da conta de usuário e da senha.

Cabe ainda ao setor de informática a emissão de termo de responsabilidade de uso dos recursos de tecnologia da informação para usuários interno e externo.

Acesso aos Sistemas

Sempre que possível, o acesso aos sistemas do SERGIPEPREVIDENCIA será feito de forma integrada ao AD (Active Directory) para que o usuário possa utilizar um único login e senha de acesso. Quando não for possível tal integração, será criado um login e senha para acesso ao determinado sistema, e a senha utilizada pelo usuário deverá seguir as normas de uso de senhas desta política

Auditoria de Acessos

Procedimentos de Auditoria de Acesso são práticas e verificações realizadas para garantir a segurança e a conformidade com políticas e regulamentos em sistemas de informação. Esses procedimentos são essenciais para monitorar e controlar o acesso a dados e recursos, bem como para detectar atividades suspeitas ou não autorizadas.

- **Aqui estão alguns passos comuns em procedimentos de auditoria de acesso:**

Autenticação e Autorização:

É verificado, na criação dos acessos, se os usuários são autenticados corretamente antes de acessar sistemas ou aplicativos. Garantindo que os usuários tenham as permissões adequadas para acessar os recursos específicos.

Registro de Acesso:

O sistema registra todas as tentativas de acesso, incluindo data, hora, usuário e ação realizada.

Analisamos, quando necessário, os registros para identificar padrões incomuns ou atividades suspeitas.

Revisão Periódica de Acesso:

É revisado regularmente as permissões de acesso para garantir que estejam atualizadas e alinhadas com as necessidades do usuário. É removido ou ajustado permissões conforme necessário.

Monitoramento Contínuo:

Monitoramento de acesso em tempo real para detectar atividades anômalas.

Auditorias de Segurança:

É realizado auditorias regulares para avaliar a eficácia dos controles de acesso.

Verificando se as políticas e procedimentos estão sendo seguidos.

Transferências de Servidores

Quando um Servidor for promovido ou transferido de setor ou gerência, o setor de Recursos Humanos comunica o fato a AGIN, para que sejam feitas as adequações necessárias para o acesso do referido Servidor ao sistema informatizado do SERGIPEPREVIDENCIA.

Cópias de Segurança de Arquivos Pessoais

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de textos, planilhas, mensagens eletrônicas, desenhos e outros arquivos ou documentos, desenvolvidos pelos Servidores, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios do SERGIPEPREVIDENCIA.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios do SERGIPEPREVIDENCIA, o setor de Informática disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações. Estas informações serão incluídas na rotina diária de backup da Informática.

Uso do Ambiente WEB (Internet)

O acesso à Internet será autorizado para os usuários que necessitarem do mesmo para o desempenho das suas atividades no SERGIPEPREVIDENCIA. Pode ser utilizada para fins pessoais, desde que não prejudique o andamento das atividades ou causem prejuízo ao instituto.

Todo acesso à internet é identificado através da conta e senha do usuário.

O ambiente de internet é monitorado e possui regras de acesso de acordo com o grupo que o usuário faz parte.

O acesso à internet se dará, exclusivamente, através dos computadores do SERGIPEPREVIDENCIA. É proibido o uso de computadores pessoais para esse tipo de acesso, salvo situações com autorização do Gestor da Informação. O instituto, até a presenta data, não possui pontos de acesso sem fio para acesso à internet.

O acesso disponibilizado pelo SERGIPEPREVIDENCIA se caracteriza como uma ferramenta de trabalho, sendo seu uso destinado às funções relativas as atribuições de cada Servidor, estagiário ou prestador de serviço. Será permitido o acesso à internet para uso com fins particulares nas seguintes condições, cumulativamente:

- Seja utilizado para acesso à *Internet Bank* e a sites cujo conteúdo proporcionem desenvolvimento pessoal;
- O tempo de acesso e conteúdo acessado não interfiram no cumprimento das funções;
- O acesso não interfira no bom funcionamento da rede e dos sistemas do Instituto;
- Não seja contabilizado para justificar a necessidade de aumento da capacidade de acesso;
- Todas as conexões feitas e conteúdos transmitidos estão sujeitos à monitoração e auditoria, mesmo que para uso particular e de conteúdo privado;
- O acesso não coloque em risco a segurança da rede e dos sistemas do instituto;

O acesso poderá ser bloqueado a qualquer momento devido a critérios técnicos ou requerimento de qualquer um dos membros da Diretoria Executiva, sem que o instituto seja responsabilizado por qualquer perda ou dano decorrente do bloqueio do acesso;

É proibida a divulgação e/ou compartilhamento indevido de informações do SERGIPEPREVIDENCIA em listas de discussão, sites ou comunidades de relacionamentos, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Não é permitido instalar programas provenientes da Internet nos computadores do SERGIPEPREVIDENCIA, sem expressa anuência do setor de Informática, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais. Os programas que necessitem de Licença ou Registro, devem ter sua regularização autorizada pela Diretoria e adquirida de forma legal. Qualquer software não licenciado que esteja em uso nos computadores do instituto poderá ser excluído.

Não é permitido, em hipótese alguma, utilizar os recursos do SERGIPEPREVIDENCIA para fazer download (baixar) de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional. O mesmo se aplica a uploads (subir) de qualquer software

licenciado pelo SERGIPEPREVIDENCIA ou de dados de sua propriedade, sem expressa autorização.

Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

Quando navegando na Internet, é proibido a visualização, transferência (download/upload), cópia, distribuição ou qualquer outro tipo de sites que:

- Possuam conteúdo pornográfico ou relacionado a sexo;
- Que defendam atividades ilegais;
- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
- Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios do SERGIPEPREVIDENCIA;
- Que promovam discussão pública sobre os negócios do SERGIPEPREVIDENCIA, a menos que autorizado pela Diretoria;
- Que possibilitem a distribuição de informações de nível “Confidencial”.

Uso do Correio Eletrônico – (E-Mail)

O correio eletrônico (e-mail) fornecido ao usuário pelo SERGIPEPREVIDENCIA é um instrumento de comunicação interna e externa do instituto, pessoal e intransferível.

As mensagens devem ser escritas em linguagem compatível com a comunicação oficial, não devem comprometer a imagem do SERGIPEPREVIDENCIA, não podem ser contrárias à legislação vigente e nem aos princípios éticos. Ver Anexo I com recomendações em como compor uma mensagem oficial.

O usuário é responsável por toda mensagem enviada pelo seu endereço de e-mail, ficando o mesmo terminantemente proibido de:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Autarquia;
- Enviar mensagem por correio eletrônico usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o instituto vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando o instituto estiver sujeito a algum tipo de investigação.
- Produzir, transmitir ou divulgar mensagem, seja entre usuários do instituto ou externos que:
    - Contenha conteúdo difamatório, calunioso, ofensivo, infame, violento, racista, especulativo, obsceno, degradante, ameaçador, pornográfico, bullying, correntes, indução religiosa, comércio, propaganda, com fins políticos, incentivos a atos terroristas, ou de qualquer natureza similar, que vier a instigar, ameaçar, invadir a privacidade ou prejudicar pessoas, organizações privadas ou públicas.
    - Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do SERGIPEPREVIDENCIA;
    - Contenha ameaças eletrônicas, como: vírus de computador e Spam; ○ Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .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 burlar qualquer sistema de segurança;
    - Contenha anexo(s) superior(es) a 40 MB para envio ou recebimento; ○ Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

Para incluir um novo usuário no correio eletrônico, o setor de recursos humanos deverá fazer um pedido formal ao setor de informática, informando nome completo, CPF, setor e cargo, que providenciará a inclusão do mesmo.

Havendo o desligamento de um servidor ou colaborador, fica o setor de recursos humano responsável em comunicar o desligamento para que a conta de e-mail seja encerrada. Uma cópia da caixa de e-mail pode ser solicitada no comunicado, sendo está cópia entregue ao gerente do setor em que o servidor ou colaborador era vinculado.

Acesso a Contas de E-mail Particular (Webmail)

Caso o usuário tenha acesso a sites de e-mail gratuitos ou pagos, que disponibilizem o envio e recebimento de e-mails através da tecnologia webmail, o usuário fica ciente que tais acessos podem comprometer a segurança das informações do SERGIPEPREVIDENCIA, motivo pelo qual tais acessos devem ser extremamente cautelosos e fetos de forma moderada.

Considerando que os e-mails pessoais acessados através da infraestrutura tecnológica do SERGIPEPREVIDENCIA, serão, via de regra, realizados através da conexão à internet pertencente ao instituto e, considerando que o endereço IP (internet protocol) de tais conexões será vinculado ao SERGIPEPREVIDENCIA, a utilização de e-mails pessoais poderá gerar responsabilidades ao instituto, o que justifica a necessidade de cautela par parte dos usuários.

Nesse sentido, caso o acesso à conta de e-mail do usuário cause qualquer tipo de dano ao SERGIPEPREVIDENCIA, este será integralmente responsável por seus atos, respondendo civil e criminalmente.

É vedado o envio de informações, dados ou arquivos relacionados, direta ou indiretamente, aos interesses do SERGIPEPREVIDENCIA via e-mail pessoal.

Necessidades de Novos Sistemas, Aplicativos e/ou Equipamentos

O setor de Informática é responsável pela aplicação da Política do SERGIPEPREVIDENCIA em relação à definição de compra e substituição de “software” e “hardware”.

Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardware) deverá ser discutida com o responsável pelo setor de Informática.

Não é permitido a compra ou o desenvolvimento de “softwares” ou “hardware” diretamente pelos servidores do instituto.

Uso de Computadores

Os servidores que tiverem direito ao uso de computadores (desktop ou notebook), ou qualquer outro equipamento computacional, de propriedade do SERGIPEPREVIDENCIA, devem estar cientes de que:

- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades voltadas ao instituto;
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo, reportando à área competente qualquer incidente que tenha conhecimento;
- É proibida a instalação e uso de Softwares (programa) ilegais (não licenciados) ou que sejam considerados inseguros;
- O usuário não deve alterar a configuração (hardware ou software), desabilitar ou desinstalar programas de segurança e interromper serviços essenciais do equipamento recebido;

- É vedado ao usuário o privilégio de administração e o acesso à senha do administrador local da estação de trabalho, exceto nos casos autorizados pelo setor de informática, em que seja necessário para o desempenho das funções;
- É vedada ao usuário a abertura física ou a desmontagem da estação de trabalho, ficando essa atividade de exclusividade do setor de informática, quando necessário;
- É proibido o uso de dispositivos ou softwares de vigia, monitoramento, acesso remoto e analisadores de pacotes com o intuito de monitorar outros usuários ou a rede de computadores;
- É vedada a conexão de computadores pessoais, de propriedade do usuário, na rede de computadores do SERGIPEPREVIDENCIA, exceto se autorizado pelo setor de informática, acompanhada de justificativa e registro da necessidade, ficando este equipamento sujeito às regras de segurança e auditoria;
- Arquivos pessoais e/ou não pertinentes ao negócio do SERGIPEPREVIDENCIA (fotos, vídeos, música, etc.) não devem ser copiados ou movidos para as pastas da rede. Caso identificado tais arquivos, os mesmos poderão ser excluídos definitivamente;
- Documentos imprescindíveis para o negócio do SERGIPEPREVIDENCIA devem ser salvos nas pastas da rede. Arquivos salvos nas pastas locais do computador (Unidade (C:), Meus Documentos, Área de Trabalho, etc.), não terão garantia de backup e poderão ser perdidos caso ocorra falha do HD (Hard Disk) do computador, sendo, portanto, de responsabilidade do usuário;
- Os usuários devem bloquear sua estação de trabalho ao se ausentarem das suas salas através da combinação de teclas CRTL + ALT + DEL e escolher a opção BLOQUEAR no menu de opções que será apresentado.

Em caso de mau uso, ou uso em desacordo com as instruções desta norma, o usuário poderá ser responsabilizado.

Fica o Servidor, usuário de computador, ciente de que a qualquer momento o setor de informática pode realizar auditoria visando garantir a correta aplicação desta diretriz.

Alguns cuidados que devem ser observados:

Fora do Instituto:

- Mantenha o equipamento sempre com você;
- Atenção em hall de hotéis, aeroportos, aviões, táxi e etc.
- Quando transportar o equipamento em automóvel utilize sempre o porta malas ou lugar não visível;
- Atenção ao transportar o equipamento na rua.

Em caso de furto

- Registre a ocorrência em uma delegacia de polícia;
- Comunique ao seu superior imediato e ao setor de Informática;
- Envie uma cópia da ocorrência para o setor de Informática.

Home Office

- Mantenha a integridade do equipamento
- Não utilize o equipamento para atividades particulares ou de terceiros
- Não faça instalação de programas
- Comunique imediatamente qualquer incidente que venha ocorrer com o equipamento ao setor de informática

Uso de Anti-Vìrus

Todo arquivo em mídia proveniente de entidade externa ao SERGIPEPREVIDENCIA deve ser verificado por programa antivírus.

Todo arquivo recebido/obtido através do ambiente Internet deve ser verificado por programa antivírus. Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de Informática, via rede.

O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

Rotinas de Recuperação de Desastres

Desastres específicos que podem ocorrer no âmbito da segurança da informação e que exigem a implementação de planos de recuperação de desastres eficazes para garantir a resiliência e a continuidade das operações:

1. **Ataques Cibernéticos:** Incluem uma variedade de ataques, como malware, ransomware, phishing, ataques de negação de serviço (DDoS), injeção de SQL, entre outros, que visam comprometer a confidencialidade, integridade ou disponibilidade dos sistemas e dados.

2. **Falhas de Segurança:**

• Vulnerabilidades de software: Falhas de segurança em aplicativos, sistemas operacionais ou outros softwares utilizados pela organização.

• Brechas de segurança: Acesso não autorizado a sistemas, redes ou dados devido a falhas na configuração, autenticação fraca ou outras vulnerabilidades.

- Perda de dados: Exposição, corrupção ou exclusão não autorizada de dados sensíveis ou críticos.

3. **Desastres Físicos:**

- Incêndios: Danos a equipamentos de hardware e infraestrutura devido a incêndios.

- Inundações: Danos causados pela água a servidores, dispositivos de armazenamento e outros equipamentos.

- Desastres Naturais: Eventos como terremotos, tempestades e furacões que podem interromper operações de TI e comprometer a segurança da informação.

4. **Erros Humanos:**

- Exclusão acidental de dados: Ações inadvertidas que resultam na perda irreversível de informações.

- Configurações incorretas: Erros na configuração de sistemas, firewalls, permissões de acesso, etc., que podem levar a violações de segurança.

5. **Falta de Conformidade:**

- Violações de regulamentos: Descumprimento de leis, regulamentos ou políticas internas de segurança da informação, o que pode resultar em penalidades legais e perda de confiança dos clientes.

6. **Desastres de Terceiros:**

- Falhas de fornecedores: Interrupções causadas por falhas de fornecedores de serviços de nuvem, provedores de serviços de Internet, entre outros.

- Vazamento de dados de terceiros: Exposição de dados sensíveis devido a violações de segurança em sistemas de terceiros com os quais a organização compartilha informações.

Procedimentos de Recuperação (“Backup”)

O serviço de backup compreende a realização de cópias de segurança dos arquivos com o objetivo de restaurá-los no menor tempo possível caso haja necessidade.

Para garantir a segurança da informação, são realizadas cópias de segurança dos arquivos mantidos em servidores, sistemas e respectivos bancos de dados utilizados pelo SERGIPEPREVIDENCIA.

As rotinas de cópia de segurança são realizadas de forma automatizada, em horários prédefinidos, fora do horário de funcionamento do instituto, denominadas de “Janelas de Backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processamento sendo realizado nos sistemas informatizados.

São realizadas verificações periódicas dos backups realizados e testes de restauração com o intuito de averiguar a integridade dos arquivos ou banco de dados, executados aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup. Quando identificado erro, seja na execução do backup e/ou no processo de restauração, é realizado um novo backup no primeiro horário disponível, após identificado e solucionado o problema.

O armazenamento das cópias de segurança é feito no CPD, onde o acesso é controlado pelo setor de informática impedindo o acesso de pessoas não autorizadas. No caso do banco de dados do sistema de gestão previdenciária SISPREV, além do backup local é realizado um backup off-site no data center da Empresa Sergipana de Tecnologia da Informação – EMGETIS.

As solicitações de restauração de arquivos deverão ser feitas formalmente por e-mail ou através de ferramenta de abertura de chamados contendo o nome do(s) arquivo(s), o caminho completo da(s) pasta(s) que deverão ser recuperados e a data do arquivo que ser quer ter acesso.

É adotada o seguinte esquema para a realização do backup:

Tipo	Periodicidade	Retenção	Discriminação
Arquivos	Diário	30 Dias FULL 30 Dias Incremental	Arquivos utilizados pelos usuários salvos nas pastas da rede.
Bancos de Dados	Diário	16 Dias FULL 30 Dias Incremental 30 Dias LOG	Backup de todos os bancos de dados vinculados ao SISPREV

É vedado o armazenamento de informações nos servidores do SERGIPEPREVIDENCIA que estejam em desacordo com as atividades do instituto, tais como, arquivos de imagem, apresentações, arquivos de áudio ou vídeo, programas não homologados ou licenciados ou de conteúdo potencialmente prejudicial à Segurança da Informação. Caso identificado esses tipos de arquivos, o fato será considerado como incidente de segurança da informação e os arquivos serão excluídos para não comprometer os recursos destinados ao backup.

É terminantemente proibido cópia de segurança de arquivos pessoais dos usuários ou cópia imagem das estações de trabalho.

Rotina de Backup Servidor de arquivos

Para garantir a segurança e a integridade dos dados da rede, o servidor de arquivos de rede possui duas modalidades de backups automáticos. Esses backups são realizados

periodicamente e permitem a recuperação dos arquivos, pastas de trabalhos e demais documentos armazenados no servidor em caso de falhas ou perdas.

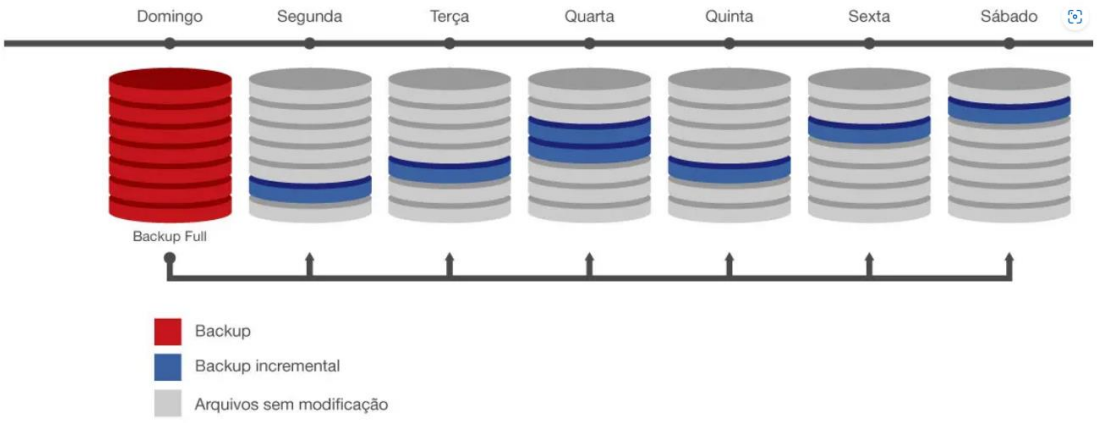
Modalidades de backups automáticos:

- FULL – Esse método de backup salva todos os dados para o destino estabelecido.

Observação:

O backup FULL ocorre todos os domingos, de forma automática, às 01:00Hrs.

- INCREMENTAL – Esse método de backup salva apenas as alterações feitas nos arquivos, desde o último backup realizado. Ao invés de copiar todos os arquivos novamente, ele identifica e armazena apenas os dados modificados ou adicionados desde o último backup. Isso permite que os backups subsequentes sejam rápidos em termos de espaço de armazenamento necessário.



Observação:

O backup Incremental ocorre de segunda a sábado, de forma automática, às 20:00Hrs.

LOCALIZAÇÃO FÍSICA / TEMPO DE RETENÇÃO

- Localização Física: Servidor IPESPREVI-S006
- Tempo de Retenção: 3 meses

Rotina de Backup Servidor Hyper-V (Sistemas)

Para garantir a segurança e a integridade dos dados armazenados nas máquinas virtuais do Hyper-V, estabelecemos rotinas automáticas de backup com o objetivo de resguardar os dados contidos nas máquinas virtuais. Essas rotinas são planejadas de acordo com a criticidade e a frequência de atualização dos dados. Para esse processo, é levado em consideração não apenas a rotina de backup, mas também a localização física onde ficarão contidos os backups e o tempo de retenção. Esses backups são realizados periodicamente e permitem a recuperação completa e parcial dos dados em caso de falhas ou perdas.

Observação:

O backup dos sistemas e máquinas virtuais é realizado todos os dias às 21:00Hrs.

4.3.1.1 LOCALIZAÇÃO FÍSICA / TEMPO DE RETENÇÃO

- Localização Física: Servidor IPESPREVI-S004
- Tempo de Retenção: Para esse tipo de backup preservamos apenas a versão mais recente dos dados, pois o objetivo, em caso de algum problema, é restaurar a versão mais recente do sistema.

Data Center

O Data center, também conhecido como C.P.D ou sala de servidores, é uma instalação física centralizada onde estão os computadores corporativos, rede, armazenamento e outros equipamentos de TI que dão suporte às operações do instituto. Os computadores contidos no data center armazenam ou manipulam aplicativos, serviços e dados importantes para o SERGIPEPREVIDENCIA.

O acesso ao data center é controlado pelo setor de informática e apenas técnicos responsáveis pela infraestrutura devem ter acesso. Visitantes, parceiros ou prestadores de serviço devem ser acompanhados durante toda sua permanência no data center por um técnico responsável, ou na ausência do mesmo, por um membro da equipe de informática.

O data center deverá ser mantido limpo. Qualquer procedimento que gere lixo ou sujeira deve ser retirado com o auxílio do departamento de serviços gerais, acompanhado por um técnico responsável, ou na ausência do mesmo, por um membro da equipe de informática.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno[1] ou inflamável.

[1] Concebido para produzir fumaça (para camuflagem, sinalização, fumigação etc.).

A entrada ou saída de equipamento do data center somente se dará com autorização do Gestor da Informação.

Papéis e Responsabilidades

Servidores, Segurados, Estagiários, e Prestadores de Serviços

Cabe aos Servidores, estagiários e prestadores de serviços, que exercem alguma atividade dentro ou foram do SERGIPEPREVIDENCIA as seguintes obrigações:

- Manter sigilo das informações do instituto;
- Zelar continuamente pela proteção das informações da instituição ou de seus segurados contra acesso, modificação, destruição ou divulgação não autorizada;
- Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados apenas para as finalidades da Instituição;
- Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;
- Comunicar imediatamente ao setor de Informática qualquer descumprimento da Política de Segurança da Informação e/ou das Normas de Segurança da Informação;
- Seguir as diretrizes e recomendações quanto ao uso, divulgação e descarte de dados e informações.

Os servidores com papel de gestão ou coordenação devem ter postura exemplar em relação à segurança da informação, diante, sobretudo, dos usuários sob sua gestão. Cada gestor ou coordenador deverá manter os processos sob sua responsabilidade aderentes às políticas de segurança, normas e procedimentos específicos de segurança da informação do SERGIPEPREVIDENCIA, tomando as ações necessárias para cumprir tal responsabilidade.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar ao SERGIPEPREVIDENCIA e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

Gestor da Informação

Compete à gestão da segurança da informação:

a) Classificar a informação sob sua responsabilidade, inclusive aquela gerada por Servidores, fornecedores ou outras entidades externas, que devem participar do processo de definição do nível de sigilo da informação;
b) Inventariar todos os ativos de informação sob sua responsabilidade;

c) Sugerir procedimentos para proteger os ativos de informação;
d) Manter um controle efetivo do acesso à informação, estabelecendo, documentando e fiscalizando a política de acesso à mesma. Tal política deve definir quais usuários ou grupos de usuários têm real necessidade de acesso à informação, identificando os perfis de acesso;
e) Reavaliar, periodicamente, as autorizações dos usuários que acessam as informações sob sua responsabilidade, solicitando o cancelamento do acesso dos usuários que não tenham mais necessidade de acessar a informação;
f) Participar da investigação dos incidentes de segurança relacionados às informações sob sua responsabilidade.

Gerências

Compete aos gestores:

g) Cumprir e fazer cumprir a política, as normas e procedimentos de segurança da informação;
h) Assegurar que suas equipes possuam acesso e entendimento da política, das normas e dos procedimentos de Segurança da Informação;
i) Sugerir ao Gesto da Informação, de maneira proativa, procedimentos de segurança da informação relacionados às suas áreas;
j) Redigir e detalhar, técnica e operacionalmente, as normas e procedimentos de segurança da informação relacionados às suas áreas, quando solicitado pelo Gestor da Informação;
k) Comunicar imediatamente ao Gestor da Informação eventuais casos de violação da política, de normas ou de procedimentos de segurança da informação.

Auditoria

Todo ativo de informação sob responsabilidade do setor de informática é passível de auditoria em data e horários determinados pelo Gestor, podendo esta, também, ocorrer sem aviso prévio.

A realização de uma auditoria deverá ser obrigatoriamente aprovada pela Diretoria e, durante a sua execução, deverão ser resguardados os direitos quanto a privacidade de informações pessoais, desde que estas não estejam dispostas em ambiente físico ou lógico de propriedade do SERGIPEPREVIDENCIA.

Com o objetivo de detectar atividades anômalas de processamento da informação e violações da política, das normas ou dos procedimentos de segurança da informação, a área de

Segurança da Informação poderá realizar monitoramento e controle proativos, mantendo a confidencialidade do processo e das informações obtidas.

As informações obtidas poderão servir como indício ou evidência em processo administrativo e/ou legal.

Violações

São consideradas violações à política, às normas ou aos procedimentos de segurança da informação as seguintes situações, não se limitando às mesmas:

a) Quaisquer ações ou situações que possam expor o SERGIPEPREVIDENCIA ou seus segurados à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;
b) Utilização indevida de dados da Instituição, divulgação não autorizada de informações, sem a permissão expressa do Gestor da Informação;
c) Uso de dados, informações, equipamentos, software, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação do SERGIPEPREVIDENCIA ou de seus segurados;
d) A não comunicação imediata à área de Gerencia da Informação de quaisquer descumprimentos da política, de normas ou de procedimentos de Segurança da Informação, que porventura um servidor, segurado, estagiário ou prestador de serviços venha a tomar conhecimento ou chegue a presenciar

Sanções

O não cumprimento desta Política de Segurança da Informação do SERGIPEPREVIDENCIA é considerada falta grave, podendo ser aplicadas penalidades previstas em lei.

Base Legal

Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal

Art. 138	Calúnia
Art. 139	Difamação
Art. 140	Injúria
Art. 147	Ameaça
Art. 153	Divulgação de segredo
Art. 154	Violação do segredo profissional
Art. 154-A e B	Invasão de dispositivo informático (incluindo distribuição de vírus)
Art. 184	Violar direitos de autor e os que lhe são conexos
Art. 266	Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento
Art. 297	Falsificação de documento público
Art. 307	Falsa Identidade
Art. 313 A	Inserção de dados falsos em sistema de informações
Art. 313 B	Modificação ou alteração não autorizada de sistema de informações
Art. 314	Extravio, sonegação ou inutilização de livro ou documento
Art. 320	Condescendência criminosa
Art. 325	Violação de sigilo funcional
Art. 326	Violação do sigilo de proposta de concorrência

Lei Federal 3.129, de 14 de outubro de 1982 - Regula a Concessão de Patentes aos autores de invenção ou descoberta industrial

Lei Federal 7.716, de 5 janeiro de 1989

Art. 20 Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional

Lei Federal 8.069, de 13 de julho de 1990 – Estatuto da Criança e do Adolescente Art. 241 Pornografia envolvendo criança ou adolescente

Lei Federal 8.159, de 08 de janeiro de 1991 - Dispõe sobre a Política Nacional de Arquivos Públicos e Privados

Lei Federal 9.609, de 19 de fevereiro de 1998 - Lei do Software

Lei Federal 9.610, de 19 de fevereiro de 1998- Dispõe sobre o Direito Autoral

Lei Federal 9.279, de 14 de maio de 1996 - Dispõe sobre Marcas e Patentes

Lei 9.296, de 24 de julho de 1996

Art. 10 Interceptação de comunicações telefônicas, de informática ou telemática

Lei 9.504, de 30 de setembro de 1997 – Lei Eleitoral

Art. 73 Proibições aos agentes públicos

Lei Federal 10.406, de 10 de janeiro de 2002 - Código Civil

Lei 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação

Art. 32 Divulgação de informação sigilosa ou informação pessoal

Recomenda-se a leitura integral da base legal citada.

Anexo I – Padrão de Comunicação por Correio Eletrônico

Um dos atrativos de comunicação por correio eletrônico é sua flexibilidade. Assim, não interessa definir padronização da mensagem comunicada. No entanto, devem-se observar algumas orientações quanto à sua estrutura.

Campo "Assunto"

O assunto deve ser o mais claro e específico possível, relacionado ao conteúdo global da mensagem. Assim, quem irá receber a mensagem identificará rapidamente do que se trata; quem a envia poderá, posteriormente, localizar a mensagem na caixa do correio eletrônico.

Deve-se assegurar que o assunto reflita claramente o conteúdo completo da mensagem para que não pareça, ao receptor, que se trata de mensagem não solicitada/lixo eletrônico. Em vez de "Reunião", um assunto mais preciso seria "Agendamento de reunião sobre a Reforma da Previdência"

Local e data

São desnecessários no corpo da mensagem, uma vez que o próprio sistema apresenta essa informação.

Saudação inicial/vocativo

O texto dos correios eletrônicos deve ser iniciado por uma saudação. Quando endereçado para outras instituições, para receptores desconhecidos ou para particulares, deve-se utilizar o vocativo conforme os demais documentos oficiais, ou seja, "Senhor" ou "Senhora", seguido do cargo respectivo, ou "Prezado Senhor", "Prezada Senhora".

Exemplos:

Senhor Coordenador,

Prezada Senhora,

Fecho

Atenciosamente é o fecho padrão em comunicações oficiais. Com o uso do e-mail, popularizou-se o uso de abreviações como "Att.", e de outros fechos, como "Abraços",

“Saudações”, que, apesar de amplamente usados, não são fechos oficiais e, portanto, não devem ser utilizados em e-mails profissionais.

O correio eletrônico, em algumas situações, aceita uma saudação inicial e um fecho menos formais. No entanto, a linguagem do texto dos correios eletrônicos deve ser formal, como a que se usaria em qualquer outro documento oficial.

Bloco de texto da assinatura

Sugere-se que todas as instituições da administração pública adotem um padrão de texto de assinatura. A assinatura do e-mail deve conter o nome completo, o cargo, a unidade, o órgão e o telefone do remetente.

Exemplo:

Maria da Silva Assessora

Subchefia para Assuntos Jurídicos da Casa Civil

(61)XXXX-XXXX

OBS: Devemos adotar o modelo recomendado pelo Manual do Governo/ SECOM.

Anexos

A possibilidade de anexar documentos, planilhas e imagens de diversos formatos é uma das vantagens do e-mail. A mensagem que encaminha algum arquivo deve trazer informações mínimas sobre o conteúdo do anexo.

Antes de enviar um anexo, é preciso avaliar se ele é realmente indispensável e se seria possível colocá-lo no corpo do correio eletrônico.

Deve-se evitar o tamanho excessivo e o reencaminhamento de anexos nas mensagens de resposta.

Os arquivos anexados devem estar em formatos usuais e que apresentem poucos riscos de segurança. Quando se tratar de documento ainda em discussão, os arquivos devem, necessariamente, ser enviados, em formato que possa ser editado.

Recomendações:

- Sempre que necessário, deve-se utilizar recurso de **confirmação de leitura**. Caso não esteja disponível, **deve constar da mensagem pedido de confirmação de recebimento**;

- Apesar da imensa lista de fontes disponíveis nos computadores, mantêm-se a recomendação de tipo de fonte, tamanho e cor dos documentos oficiais: **Calibri ou Carlito, tamanho 12, cor preta;**
- Fundo ou papéis de parede eletrônicos não devem ser utilizados, pois não são apropriados para mensagens profissionais, além de sobrecarregar o tamanho da mensagem eletrônica;
- A mensagem do correio eletrônico deve ser revisada com o mesmo cuidado com que se revisam outros documentos oficiais;
- O texto profissional dispensa manifestações emocionais. Por isso, ícones e emoticons não devem ser utilizados;
- Os textos das mensagens eletrônicas não podem ser redigidos com abreviações como "vc", "pq", usuais das conversas na internet, ou neologismos, como "naum", "eh", "aki";
- Não se deve utilizar texto em caixa alta para destaques de palavras ou trechos da mensagem pois denota agressividade de parte do emissor da comunicação.
- Evite-se o uso de imagens no corpo do e-mail, inclusive das Armas da República Federativa do Brasil e de logotipos do ente público junto ao texto da assinatura.
- Não devem ser remetidas mensagem com tamanho total que possa exceder a capacidade do servidor do destinatário.

FONTE: Manual de Redação da Presidência da Republicada, 3° Edição, 2018.

Anexo II - Termo de Responsabilidade e Sigilo

Termo de Responsabilidade e Sigilo

Prelo presente instrumento, eu _____,
CPF _____, DECLARO, sob pena das sanções cabíveis, estou comprometido com as práticas, responsabilidades e obrigações normativas referentes à Política de Segurança da Informação do SERGIPEPREVIDENCIA e à suas Regras de Uso dos Recursos Tecnologia da Informação.

Que tenho pleno conhecimento das minhas responsabilidades no que concerne ao sigilo a ser mantido sobre as atividades desenvolvidas ou ações realizadas, bem como, sobre informações que eventualmente ou por força da minha função venha a tomar conhecimento.

Aracaju (SE), _____ de _____ de _____

_____ Assinatura
por Extenso

_____ Cargo/Função

Anexo III - Termo de Responsabilidade Senha de Acesso

Termo de Responsabilidade

Senha para acesso aos sistemas, rede e internet

Prelo presente instrumento, eu _____,
CPF _____, DECLARO estar ciente de que:

- Devo alterar a senha inicialmente fornecida pelo SERGIPEPREVIDENCIA em meu primeiro acesso ao sistema;
- A senha para acesso aos sistemas é pessoal, sigilosa e de minha responsabilidade, que, em hipótese alguma poderei divulgá-la e/ou compartilhá-la;
- Serei responsável pelo uso correto de minha senha perante o SERGIPEPREVIDENCIA e a legislação (cível e criminal).

Declaro estar ciente e de acordo com a Política de Segurança de Informação do SERGIPEPREVIDENCIA, disponível no endereço eletrônico www.sergipeprevidenica.se.gov.br, e me comprometo a verificar futuras alterações desta política, me comprometendo a comunicar ao setor de T.I. qualquer desacordo com atualizações desta.

Aracaju (SE), _____ de _____ de _____

_____ Assinatura
por Extenso

_____
Cargo/Função

Anexo IV – Termo de Responsabilidade de Uso do Sistema de Gestão Previdenciária

TERMO DE RESPONSABILIDADE

USO DO SISTEMA DE GESTÃO PREVIDENCIÁRIA – SISPREV

SECRETARIA/ÓRGÃO:

DADOS DO USUÁRIO

Nome:		Sexo: ( ) M ( ) F
CPF:	E-mail corporativo:	
Cargo:		
Telefone Corporativo:	Celular:	

Perfil de Acesso

- ☐ Consulta dados pessoais e funcionais.
- ☐ Consulta dados pessoais, funcionais e informações financeiras.
- ☐ Consulta dados pessoais, funcionais, informações financeiras e acessa relatórios.
- ☐ Consulta e altera dados pessoais e funcionais.
- ☐ Consulta e altera dados pessoais e funcionais e informações financeiras. Assina processos.
- ☐ Consulta e altera dados pessoais, funcionais, informações financeiras e acessa relatórios. (exclusivo do instituto)
- ☐ Consulta e altera informações financeiras das aplicações. (exclusivo do instituto)
- ☐ Consulta e altera dados no módulo de Perícia. (exclusivo do instituto)
- ☐ Consulta e altera dados no módulo de Arrecadação. (exclusivo do instituto)
- ☐ Acesso irrestrito a todas as funcionalidades do sistema. (administradores – exclusivo do instituto)

Horário de trabalho

☐	Das 07:00h às 13:00h de segunda à sexta.
☐	Das 07:00h às 18:00h de segunda à quinta e das 07:00 às 13:00h às sextas.
☐	Das 07:00h às 22:00h de segunda a sexta (gerentes – exclusivo do instituto)
☐	Sem controle de horário (exclusivo do instituto)
☐	Horário especial para estagiários. Favor descrever: _____

Eu, **.....**, declaro possuir perfil de acesso ao SISPREV**,** tendo-o sob minha responsabilidade e comprometendo-me a:

I. Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial;

II. Utilizar os dados do SISPREV de acesso restrito com a necessária cautela, quando de sua exibição em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

III. Não me ausentar da estação de trabalho sem encerrar a sessão de uso do sistema, garantindo assim a impossibilidade de acesso indevido por terceiros;

IV. Não revelar minha senha de acesso ao sistema a terceiros e tomar o máximo de cuidado para que ela permaneça sendo somente de meu conhecimento;

V. Alterar minha senha, sempre que for obrigatório ou que haja suposição de ter sido descoberta por terceiros, redefinindo-a sem fazer uso de combinações simples que possam ser facilmente reveladas;

VI. Responder, em todas as instâncias, pelas consequências das ações ou omissões de minha parte, que possam por em risco ou comprometer a exclusividade de conhecimento de minha senha, ou das transações a que tenha acesso.

Declaro, ainda, estar plenamente esclarecido e consciente que:

a) São minha responsabilidade cuidar da integridade, confidencialidade e disponibilidade dos dados e informações contidas no sistema, bem como comunicar por escrito ao SERGIPEPREVIDÊNCIA e à minha chefia imediata quaisquer indícios ou possibilidades de irregularidades, de desvios ou de falhas

identificadas no sistema, sendo proibida a exploração de inconsistências ou vulnerabilidades porventura existentes;

b) Constitui descumprimento de normas legais, regulamentares e quebra de sigilo funcional divulgar dados obtidos do sistema para outros servidores não envolvidos nos trabalhos executados;

c) Sem prejuízo da responsabilidade penal e civil e de outras infrações disciplinares, representam falta de zelo e dedicação às atribuições do cargo e descumprimento de normas legais e regulamentares não proceder com cuidado na guarda e utilização de senha ou emprestá-la a outro servidor, ainda que seja usuário habilitado;

d) Constitui infração funcional e penal inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos do sistema ou bancos de dados do SERGIPEPREVIDÊNCIA (administração pública), com o fim de obter vantagem indevida para si ou para outrem ou para causar dano, bem como modificar ou alterar o sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente, ficando o infrator sujeito às punições previstas no Código Penal Brasileiro, conforme responsabilização por crime contra a Administração Pública, tipificado nos artigos 313-A e 313B.

Declaro, nesta data, ter ciência e estar de acordo com os procedimentos acima descritos, comprometendo-me a respeitá-los e cumpri-los plena e integralmente, além de manter sempre verossímeis os dados da instituição e da minha área de competência.

Aracaju (SE), _____ de _____ de _____

_____

(Assinatura do usuário)

_____

(Assinatura do dirigente ou gestor do RH da secretaria/órgão)

Obs.: Quando o usuário sair desta atividade, solicitamos informar em até 48h ao SERGIPEPREVIDÊNCIA para exclusão de seu acesso ao SISPREV.