CASSIND

CAIXA DE ASSISTÊNCIA DO SINDIFISCO - SE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Sumário

1 DISPOSIÇÕES INICIAIS

1.1 FINALIDADE

Estabelecer diretrizes para a proteção das informações da operadora, devendo ser aplicada em toda e qualquer atividade atribuindo responsabilidades e diretrizes bem como adequação às práticas no manuseio, tratamento, controle e proteção, a fim de evitar a disponibilidade, divulgação, acesso e modificação não autorizados de informações e dados. Durante todo o ciclo de vida da informação, desde a coleta, uso, compartilhamento, transporte, armazenamento até o descarte de tais informações.

1.2 ABRANGÊNCIA

Esta política se aplica, no que couber, às atividades realizadas pela CASSIND através de todo o seu corpo funcional, diretoria e conselhos, colaboradores, consultores externos, jovem aprendiz, estagiários e prestadores de serviço no exercício dos serviços contratadas com operadora para atender os fins a que essa se destina, inclusive no compartilhamento de dados e informações e dados protegidos por esse documento.

1.3 FREQUÊNCIA DE REVISÃO

Os normativos gerados a partir desta política devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 1(um) ano.

1.4 DISTRIBUIÇÃO E DISSEMINAÇÃO DA POLÍTICA

Deverá ser implementada e disponibilizada, de forma total, parcial ou através de medidas e ações com fins pedagógicos, com circularização através de recurso virtuais como: no portal da entidade, redes sociais; além de recursos físicos como folders, cartazes, quadro de avisos e em outros meios de comunicação, a fim de ampliar a divulgação das políticas a todos os interessados e envolvidos nas atividades da entidade observando os limites legais.

2 PRINCÍPIOS E DIRETIVAS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A presente política assim como a metodologia e ações práticas que permeiam a política de adequação e implementação da LGPD deverão estar alicerçadas nos princípios do normativo legal que regula os padrões de proteção de dados no Brasil.

2.1 Classificação da Informação

2.1.1 Classificação adequado da Informação

Tem o objetivo de assegurar **o nível adequado de proteção para a informação, de acordo com a ISO 27001**. De forma a coibir o vazamento de informações ou o acesso indevido decorrente de ato ilícito de terceiros, ou de forma acidental pelos operadores dos dados, com a definição **dos pontos críticos na organização** observando os requisitos legais.

2.1.2 Inventário de ativos

O propósito em desenvolver um inventário de ativos tem como finalidade: identificar e classificar as informações disponibilizadas, quem é responsável por elas, a quem se destinam, onde, como, e com quem essas informações são compartilhadas interna e externamente;

2.1.3 Rotulagem da informação

Tem o objetivo de rotular/classificar os ativos pela classificação em termos de confidencialidade, são eles:

- ✓ Confidencial (o mais alto nível de confidencialidade);
- ✓ Restrita (médio nível de confidencialidade);
- ✓ Uso interno (o mais baixo nível de confidencialidade);
- ✓ Pública (todos podem ver a informação).

O proprietário do ativo é o responsável **por classificar a informação**, quanto maior o valor da informação (maiores as consequências de uma quebra da confidencialidade), maior deve ser o nível de classificação, observando o sigilo requerido, relevância, criticidade e sensibilidade.

2.1.4 Manuseio de ativos

As informações criadas, armazenadas, manuseadas, transportadas, custodiadas ou descartadas, referentes aos ativos, são patrimônio da Operadora, classificadas e manipuladas de acordo com normas e legislação específica em vigor, mantendo a segurança durante todo o seu ciclo de vida.

Os Operadores tratarão de forma estritamente confidencial todas as informações levadas a seu conhecimento de acordo com o rótulo de cada ativo, durante a prestação dos serviços ou em função deles e somente as utilizarão no âmbito dos serviços ora pactuados.

Obrigam-se, portanto, a manter o sigilo e respeitar a confidencialidade de todos os dados e informações, verbais ou escritas, pormenores, inovações, segredos comerciais, marcas, criações, especificações técnicas e comerciais da instituição, entre outros, a que tiverem acesso, conhecimento ou que venha a lhes ser confiado, comprometendo-se, outrossim, a não revelar, reproduzir, utilizar ou dar conhecimento, em hipótese alguma e a qualquer tempo. O uso das informações deverá ser feito apenas para o desempenho das atividades laborais.

2.2 Utilização dos Recursos de Informação

Os recursos de tecnologia da informação vinculados a CASSIND colocados à disposição para uso como ferramenta de trabalho, devem ser utilizados em atividades primordialmente relacionadas às funções institucionais desempenhadas.

Apenas os equipamentos e softwares disponibilizados e/ou homologados pela CASSIND podem ser instalados e conectados à rede. Todos os ativos de informação devem ser

devidamente guardados, especialmente documentos em papel ou mídias removíveis. Documentos não devem ser abandonados após a sua cópia, impressão ou utilização.

É vedado o uso de recursos computacionais para armazenar ou transmitir conteúdo ilegal, difamatório, invasivo à privacidade, obsceno ou injurioso.

É vedada a utilização dos recursos de tecnologia da informação com o objetivo de praticar ações prejudiciais ao funcionamento e à utilização de quaisquer recursos da rede de computadores internas e/ou externas.

A CASSIND pode autorizar terceiros ou efetuar testes controlados de sistemas e de infraestrutura com o objetivo de identificar vulnerabilidades e mensurar riscos, adotando as medidas preventivas cabíveis a fim de evitar quaisquer efeitos danosos ou impactos indesejáveis ao ambiente computacional e ao trabalho dos usuários autorizados.

O uso dos recursos computacionais pelo corpo funcional, diretoria e conselhos, colaboradores, consultores externos, jovem aprendiz, estagiários e prestadores de serviço está sujeito à monitoração, respeitando-se os princípios constitucionais e legais aplicáveis e adotados pela CASSIND;

É vedado ao qualquer membro do corpo funcional, diretoria e conselhos, colaboradores, consultores externos, jovem aprendiz, estagiários e prestadores de serviço de forma deliberada e sem prévia autorização formal alterar, física ou logicamente, as estações de trabalho.

O uso de recursos criptográficos poderá ser considerado no trânsito e no armazenamento das informações, de acordo com a sua classificação.

2.2.1 SEGURANÇA DOS EQUIPAMENTOS

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento da Área de TI ou por quem está designada mediante endosso da Diretoria da CASSIND.

Os sistemas e computadores devem ter versões de software antivírus instalados, ativados e atualizados permanentemente. Em caso de suspeita de incidência de vírus ou problemas de funcionalidade de hardware ou software, o membro do corpo funcional, diretoria e conselhos, colaboradores, consultores externos, jovem aprendiz, estagiários e prestadores de serviço deverá acionar a Área de TI.

Os membros do corpo funcional, diretoria e conselhos, colaboradores, consultores externos, jovem aprendiz, estagiários e prestadores de serviço deverão proteger o acesso a seus computadores por meio de tela de bloqueio a ser liberada mediante senha, quando os mesmos não estiverem em uso. Ao final do expediente de trabalho diário, o computador deverá ser desligado.

2.2.2 UTILIZAÇÃO DA REDE

A CASSIND possui uma rede integrada de computadores com servidores e um microcomputador para cada operador. O acesso à rede da CASSIND exige prévio registro obrigatório de computador e usuário, de acordo com os sistemas de registro implementados.

O operador é responsável pelas atividades realizadas por intermédio de sua conta de usuário e senhas de acesso.

É vedado ao membro do corpo funcional, diretoria e conselhos, colaboradores, consultores externos, jovem aprendiz, estagiários e prestadores de serviço, extrair ou disponibilizar material sem a licença adequada através da rede.

Cada usuário/operador é responsável pela própria e devida autenticação nos sistemas de redes disponibilizados, não podendo fornecer e/ou compartilhar seu usuário, senha e/ou acesso à rede com outros usuários.

O usuário se compromete a utilizar as redes públicas e ou privadas para uso exclusivo de atividades relacionadas ao setor no qual o usuário pertence. É vedada a utilização de proxies que permitam o tráfego de informações a redes privadas externas.

Os usuários devem administrar suas pastas, excluindo arquivos desnecessários, sendo vedado o acesso a material de caráter sexual explícito ou não, contrário à legislação brasileira, a moral e bons costumes, sendo expressamente proibido: a exposição, impressão, armazenamentos, distribuição, edição ou gravação, através do uso dos recursos computacionais da rede corporativa ou redes sociais da entidade.

É expressamente proibido: a gravação de arquivos particulares (músicas, filmes, fotos etc.) nos drivers de rede, pois estes ocupam espaço comum limitado. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente, sem prévia comunicação;

2.2.3 UTILIZAÇÃO DA INTERNET

Sob o aspecto de proteção e integridade dos sistemas de informação, a Internet é classificada como conexão de alto risco.

Os usuários devem estar cientes, portanto, das peculiaridades da navegação na Internet, antes de acessá-la e de utilizar os seus recursos. A internet, via cabo ou Wi-fi, deverá ser utilizada para fins profissionais, como ferramenta de busca de informações, que contribuam para o desenvolvimento das atividades da CASSIND, obedecendo os limites de segurança e bloqueios aplicados pela entidade.

2.2.4 UTILIZAÇÃO DE MÍDIAS REMOVÍVEIS

O uso de mídias removíveis deve ser tratado como exceção à regra, pois a porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais.

Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que tais dispositivos possam vir a causar, uma vez que esse tipo de mídia pode conter vírus e softwares maliciosos, capazes de danificar e corromper dados.

2.2.5 ACESSO REMOTO

Onde existir a necessidade de acesso Remoto aos recursos de processamento da informação, uma avaliação dos riscos envolvidos deve ser feita para determinar as possíveis implicações na segurança e os controles necessários. Estes devem ser acordados e definidos através de instrumento assinado com os prestadores de serviços, quando evidenciarem o cumprimento as exigências da LGPD no tocante a segurança e controle das informações compartilhadas.

O acesso à informação e aos recursos de processamento da informação não deve ser permitido até que os controles apropriados sejam implementados e um documento definindo os termos para a conexão ou acesso seja assinado.

A boa utilização destes serviços é de responsabilidade de cada usuário, os que utilizam a rede da CASSIND e/ou terceiros autorizados a utilizar serviços de acesso remoto. Cabe enfatizar que os serviços estão disponibilizados para o uso estritamente profissional e de interesse da CASSIND.

- ✓ O usuário somente pode realizar acesso interativo entre redes onde a permissão esteja autorizada;
- ✓ O usuário externo deve configurar de forma adequada o firewall e a proteção antivírus na rede externa à rede da CASSIND;

2.3 Dos controles de acesso

As instalações, equipamentos, redes e sistemas de computadores, deverão possuir mecanismos adequados de controle de acesso físico e/ou lógico, que possibilitem a identificação das pessoas.

Para utilização dos recursos de TI da CASSIND será sempre necessária a autenticação, mediante credencial de acesso.

As credenciais de acesso deverão delegar a seu portador somente os níveis de privilégio mínimos ao exercício de sua função.

Os equipamentos e softwares utilizados na administração dos recursos de TI deverão ser protegidos por senha, que será de conhecimento exclusivo dos técnicos da TI e/ou terceiros responsáveis pela administração destes recursos.

Os administradores dos Ativos de TI da CASSIND são responsáveis pelo uso adequado dos recursos sob sua responsabilidade, devendo zelar pela integridade, disponibilidade e confidencialidade dos sistemas e dos dados sob seus cuidados.

Na ocorrência de afastamento, mudança de responsabilidades e de lotação ou atribuições dentro da empresa, faz-se necessária **a revisão imediata dos direitos de acesso e**

uso dos ativos. Na efetivação do desligamento do usuário, deverão ser extintos todos os direitos de acesso e uso dos ativos de informação a ele atribuídos.

A **senha de acesso é de uso pessoal e intransferível e sua divulgação é vedada sob qualquer hipótese**, devendo ser alterada pelo próprio usuário, a qualquer tempo, ou por determinação da TI, especialmente quando houver suspeita de sua violação.

Qualquer utilização dos sistemas e demais recursos de informática da CASSIND é de responsabilidade do Usuário ao qual estejam associadas as credenciais de acesso utilizadas.

A senha de rede valerá por prazo determinado. A TI divulgará as regras a serem seguidas na definição da senha de rede, além de recomendações que visem assegurar a maior privacidade possível da senha.

Os visitantes não poderão possuir credenciais de acesso a redes e sistemas de computadores da CASSIND, exceto nos casos de redes destinadas para tais pessoas, autorização expressa da TI e casos previstos em lei.

Cada senha de usuário é exclusiva. Nenhuma senha deve ser fornecida ou divulgada a terceira pessoa, ainda que pertencente ao corpo funcional, diretoria, conselho, colaborador, estagiário, prestador de serviço da organização, por qualquer razão ou argumento.

Em hipótese alguma, as informações relativas ao negócio da organização, incluindo, mas não se limitando a arquivos, programas, em especial aquelas ligadas às atividades financeiras, técnicas, comerciais, senhas, nomes de usuários ou outras informações relacionadas à rede de comunicação, devem ser trocadas através da internet com destinatários não autorizados, a menos que tenha sido aprovado expressamente.

O acesso físico a sala dos servidores é privativa à diretoria, gerencia e funcionários do setor de TI, ou pessoas acompanhadas por esses.

2.4 Direitos de Propriedade

Todo ativo resultante do trabalho da prestação de serviço direto ou indireto de tratamento da informação (coleta de dados e documentos, sistema, metodologia, dentre outros) é propriedade da CASSIND.

Em caso de extinção ou rescisão do contrato de trabalho ou prestação de serviços, por qualquer motivo, deverá o agente de tratamento devolver todas as informações confidenciais geradas e manuseadas em decorrência da prestação dos serviços, ou emitir declaração de que as destruiu.

2.5 Equipamentos particulares/privados

Equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio, nem devem ser conectados às redes da Organização.

Casos especiais, **expressamente autorizados** pela Diretoria / Gerência, serão respaldados por Termo de responsabilidade específico para essa finalidade.

2.6 Mesa Limpa e Tela Limpa

Essa prática tem como objetivo a redução dos riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente.

A adoção dessa prática "mesas limpas" para os papéis e mídias de armazenamento removível e, igualmente, uma política de "telas limpas", contra, por exemplo, o perigo de ter um usuário já autenticado/registrado, porém ausente e com sua sessão de trabalho aberta.

A **prática** de Mesa Limpa/Tela Limpa busca resguardar a Cassind bem como o próprio usuário contra o acesso não autorizado a informações. Assim, sinteticamente, entre outros:

a) Papéis, anotações e lembretes da sua mesa de trabalho devem ser mantidos sempre que possível fora da superfície da mesa (mesa limpa);
b) Informações restritas ou confidenciais devem ser trancadas em local separado (idealmente em um arquivo, armário ou gaveteiro) quando não necessárias, especialmente quando o ambiente fica vazio;
c) Computadores e notebooks não devem ser deixados autenticados/ registrados quando não houver um colaborador (operador) junto e devem ser protegidos por senhas e outros controles quando não estiverem em uso. (Tela limpa);
d) Informações restritas ou confidenciais, quando impressas, devem ser retiradas da impressora imediatamente;
e) Ao final do dia, ou no caso de ausência prolongada, limpar a mesa de trabalho;
f) Papéis, livros ou qualquer informação restrita ou confidencial não devem ser deixados na mesa;
g) Um protetor de tela que solicite uma senha para acesso deve ser usado;
h) Todos os documentos e meios eletrônicos no final do dia de trabalho devem ser devidamente guardados/organizados, com proteção adequada;
i) Documentos contendo informações pessoais devem ser mantidos trancados.

3 SEGURANÇA EM PESSOAS

3.1 Novos Colaboradores, estagiários e prestadores de serviço

As responsabilidades de segurança da informação devem ser atribuídas na fase de recrutamento, incluídas em contratos e monitoradas durante a permanência.

Todos que utilizam os ativos devem obedecer ás regras de segurança da informação.

3.2 Treinamento dos usuários

Deve ser elaborada uma política de capacitação em segurança da informação para usuários com o objetivo de assegurar que estejam cientes das ameaças e preocupações de segurança da informação e equipados para apoiar a política de segurança da instituição durante a execução normal do seu trabalho.

Os usuários devem ser treinados nos procedimentos de segurança da informação de forma a minimizar possíveis riscos de segurança.

3.3 Notificação de falhas e incidentes de segurança da informação e mau funcionamento

Devem ser estabelecidos procedimentos formais para notificação de falhas e incidentes de segurança da informação e mau funcionamento de equipamentos ou aplicativos, bem como procedimentos de resposta a incidentes.

A inobservância das proibições acima indicadas poderá implicar em aplicação de medidas disciplinares, sanções contratuais ou mesmo rescisão do contrato vigente, além de responder administrativa, civil e criminalmente pelos prejuízos causados a CASSIND ou a terceiros a ela vinculado.

4 TABELA DE CONTROLE DE REVISÕES

Responsável pela criação da política - Josué Esteves Araujo - email: comunicados@cassind.com.br			
REVISÃO	**DATA**	**MOTIVO**	**RESPONSÁVEL**

5 TERMOS E DEFINIÇÕES

- ✓ Ambiente Tecnológico: Compreende todos os sistemas, computadores e redes do Instituto.
- ✓ Antivírus: Programa de proteção do computador que detecta e elimina os vírus (programas danosos) nele existentes, assim como impede sua instalação e propagação.
- ✓ Aplicativos de comunicação: Programas de computador, geralmente instalados em dispositivos móveis, usados para troca rápida de mensagens, conteúdos e informações multimídia, a exemplo de Whatsapp, Telegram, Skype etc.

- ✓ Ativo: Qualquer coisa que tenha valor para o Instituto e precisa ser adequadamente protegida.
- ✓ Backup: É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.
- ✓ Clientes: Patrocinadores, instituidores, participantes e seus beneficiários.
- ✓ Data Center: Rede de computadores utilizados para armazenamento, processamento ou distribuição remota de grandes quantidades de dados.
- ✓ Dispositivos móveis: Equipamentos de pequena dimensão que têm como características a capacidade de registro, armazenamento ou processamento de informações, possibilidade de estabelecer conexões e interagir com outros sistemas ou redes. Exemplos: smartphone, notebook, tablet, equipamento reprodutor de MP3, câmeras de fotografia ou filmagem.
- ✓ Firewall: Dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.
- ✓ Hardware: conjunto dos componentes físicos (material eletrônico, placas, monitor, equipamentos periféricos etc.) de um computador.
- ✓ Informação: Conjunto de dados e conhecimentos organizados, que possam constituir referências sobre um determinado acontecimento, fato ou fenômeno.
- ✓ Log - Registro de eventos em um sistema de computadores.
- ✓ Mídias Removíveis: Dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Disquete, Pen Drive, cartão de memória entre outros.
- ✓ Patches: Programas criados para atualizar ou corrigir um software.
- ✓ Parceiros: Pessoas Físicas ou Jurídicas que possuem relação de negócios com o Instituto Peer-To-Peer (P2P) - Arquitetura de redes de computadores onde cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central.
- ✓ Perfil de Acesso: Grupo de acessos a um recurso tecnológico estratificado por função dentro do Instituto.
- ✓ Colaboradores: Corpo Diretivo, conselheiros, membros de comitê, empregados, estagiários e empregados terceirizados.
- ✓ Proxy: Em redes de computadores, um proxy é um servidor (um sistema de computador ou uma aplicação) que age como um intermediário para requisições de clientes solicitando recursos de outros servidores.
- ✓ RH: Recursos Humanos.
- ✓ Sites de proxy: Sites utilizados para acessar outros sites da web. Em redes corporativas que tem monitoramento ou bloqueio de sites, sites de proxy permitem a navegação anônima a sites proibidos.
- ✓ Servidor: é um software ou computador, com sistema de computação centralizada que fornece serviços a uma rede de computadores, chamada de cliente.
- ✓ Software: É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores.
- ✓ SPAM: Mensagem de e-mail publicada em massa com fins publicitários.

- ✓ TI: Tecnologia da Informação.
- ✓ USB: É um tipo de conexão "ligar e usar" que permite a conexão de periféricos sem a necessidade de desligar o computador.
- ✓ VDI (Virtual Desktop Infrastructure): É um tipo de virtualização de desktops, utilizado para possibilitar o acesso a uma máquina virtual, onde o colaborador terá pleno acesso a todos os aplicativos disponibilizados pelo Instituto.
- ✓ VPN (Virtual Private Network): Modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna. Comumente é utilizado por colaboradores autorizados em trânsito.
- ✓ Wi-Fi: Abreviação de Wireless Fidelity - é uma tecnologia de comunicação que não faz uso de cabos e, geralmente, é transmitida através de frequências de rádio, infravermelhos etc.

REFERÊNCIAS:

a) ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação — Requisitos;

b) ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação;

c) Normas da ANS;

d) Lei 9.609/98 - Lei do Software;

e) Lei 12.527/11 - Lei de Acesso à Informação;

f) Lei 12.737/12 - Lei Carolina Dieckmann;

g) Lei 12.965/14 - Marco Civil da Internet;

h) Lei 13.709/18 - Lei Geral de Proteção de Dados.