POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI

1. INTRODUÇÃO

A Política de Segurança da Informação, também referida como PSI, é o documento utilizado para orientar e estabelecer diretrizes de segurança da COLOMBO PREVIDÊNCIA para a proteção dos ativos de informação e prevenção de incidentes que possam comprometer, integridades de dados tratados pela Autarquia e prevenção de responsabilidade legal para todos os colaboradores. Deve, portanto, ser cumprida e aplicada em todas as áreas da Autarquia.

É de responsabilidade da equipe de tecnologia da informação do RPPS avaliar, sempre que necessário, para que esta política seja atualizada e manter sua adequação e relevância em relação às necessidades e objetivos dos serviços desempenhados.

2. OBJETIVOS

Definir diretrizes de segurança baseada nas recomendações propostas pela norma ABNT NBR 27002:2005, que devem ser seguidas pelos servidores e fornecedores da Colombo Previdência afim de garantir que as tarefas desempenhadas no dia-a-dia sejam embasadas nas melhores práticas de segurança com a finalidade de proteger os ativos da Autarquia.

Preservar as informações do COLOMBO PREVIDÊNCIA quanto à:

- **Integridade:** garantir que a informação seja mantida em seu estado original, protegendo-a durante a guarda, transmissão, contra modificações indevidas, intencionais ou acidentais.

- **Confidencialidade:** Permitir que apenas pessoas autorizadas tenham acesso à informação.

- **Disponibilidade:** Acesso à informação pelas pessoas autorizadas sempre que necessário.

3. TERMOS E DEFINIÇÕES

Para os efeitos desta política, aplicam-se os seguintes termos e definições:

Ativo: Qualquer coisa que tenha valor para a organização, seja equipamento, serviço ou informação.

Controle: Método de gerenciamento do risco, contendo políticas, diretrizes, praticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, gestão ou legal.

Diretriz: Descrição utilizada para orientar quais ações de proteção devem ser executadas e como devem ser executadas.

Recurso de processamento da informação: Qualquer sistema de processamento de informação, serviço ou infraestrutura e as instalações que os abriguem.

Segurança da informação: Preservação da confidencialidade, integridade e disponibilidade da informação. Autenticidade, responsabilidade e confiabilidade também fazem parte da segurança da informação.

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 situação previamente desconhecida que possa ser relevante para a segurança da informação.

Incidente de segurança da informação: Evento ou série de eventos de segurança da informação indesejados ou inesperados que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

Política: Intenções ou diretrizes globais formalmente expressas pela direção ou setor responsável e documentadas formalmente.

Risco: Combinação da probabilidade de um evento ocorrer e suas consequências para a segurança da informação.

Análise de riscos: Avaliação de informações para identificar fontes e estimar risco.

Avalição de riscos: Processo completo de análise de riscos.

Gestão de riscos: Atividades coordenadas para direcionar e controlar a ocorrência de riscos como análise e avaliação de riscos, aceitação e comunicação de riscos.

Tratamento de risco: Processo de seleção e implementação de medidas para reduzir ou evitar riscos.

Ameaça: Potencial causa de um incidente indesejado que pode resultar em danos nos ativos da organização.

Vulnerabilidade: Fragilidade dos ativos ou grupo de ativos que pode ser explorada ou atingida por uma ameaça.

4. APLICAÇÕES

Todas as diretrizes estabelecidas nesta política de segurança da informação deverão ser seguidas por todos os servidores e prestadores de serviço. Esta política deve ser distribuída entre os colaboradores, que tem a obrigação de manter-se atualizados em relação a esta política, buscando orientação de seu gestor caso haja dúvida em como agir em situação que pode gerar algum tipo de incidente. Os prestadores de serviço devem receber uma cópia deste documento antes de iniciarem qualquer atividade, afim de garantir seu conhecimento sobre as diretrizes que regem este documento quando realizarem qualquer tarefa.

5. RESPONSABILIDADES ESPECÍFICAS

5.1 Dos Servidores e Fornecedores em Geral

Entende-se por servidor toda e qualquer pessoa física, nomeada por concurso público ou por livre nomeação e exoneração, que exerça alguma atividade dentro ou fora da instituição.

Entende-se por fornecedor o prestador de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

É de responsabilidade cada servidor ou fornecedor, todo prejuízo ou dano que possa ocorrer a COLOMBO PREVIDÊNCIA e/ou a terceiros, caso o mesmo não respeite ou siga as diretrizes ou normas descritas nesta política.

5.2 Dos Servidores em Regime de Exceção (Temporários e Estagiários)

Deve-se entender os riscos associados à sua condição especial e exigir o cumprimento das regras descritas nesta política.

Caso julgue-se necessário, deve-se restringir permissões de acesso à dados e serviços.

5.3 Dos Gestores de Pessoas ou Processos

Como líderes, devem ter postura de exemplo quanto ao uso e respeito às diretrizes da política de segurança da informação, como modelo de conduta para os servidores sob sua gestão.

Devem atribuir aos servidores, durante a fase de contratação e de formalização dos contratos individuais de trabalho ou de prestação de serviços ou de parceria, a responsabilidade do cumprimento e respeito da Política de Segurança da Informação.

Cabe também aos gestores, exigir dos servidores e fornecedores a assinatura do Termo de Compromisso e Ciência, localizado no fim desta PSI, assumindo o dever de seguir as normas estabelecidas e se comprometer a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da COLOMBO PREVIDÊNCIA.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta política.

5.4 Da Equipe de Tecnologia da Informação (Contratada/Terceirizada)

- Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.
- Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.
- Configurar os equipamentos, ferramentas e sistemas concedidos aos servidores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política de Segurança de Informações.

- Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários.
- Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para o COLOMBO PREVIDÊNCIA.
- Quando ocorrer movimentação interna dos ativos de tecnologia de informação, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.
- Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

a) Os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário;

b) Os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

- Realizar auditorias periódicas de configurações técnicas e análise de riscos. Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de exoneração de servidor, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da COLOMBO PREVIDÊNCIA.
- Promover a conscientização dos servidores em relação à relevância da segurança da informação para as atividades precípuas ao COLOMBO PREVIDÊNCIA.

- Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

6. REGRAS DE SEGURANÇA

As diretrizes listadas a seguir definem boas práticas de segurança utilizadas para reduzir a exposição dos ativos, minimizando a possibilidade de ocorrência de incidentes de segurança.

6.1 NÃO UTILIZAR SENHAS E PADRÕES DE CONFIGURAÇÃO DE FÁBRICA

Alterar nomes de usuários, senhas e configurações que seguem padrões de fábrica, inseridos em equipamentos ou serviços. Criar nomes de usuário diferentes de padrões conhecidos e utilizar senhas com sequência de caracteres alfanuméricos para ampliar a complexidade das palavras-chave. Alterar protocolos de serviço e números de portas, tanto em equipamentos físicos ou servidores virtuais.

Remover todas as contas padrão desnecessárias devem ser removidas ou desativadas.

6.2 DESENVOLVER E MANTER SISTEMAS E APLICATIVOS SEGUROS (TERCEIROS)

Deve-se utilizar boas práticas de programação para que o sistema não possua brechas de segurança que possam ser exploradas para acesso a dados. Funcionalidades que tratam dados sensíveis devem implementar técnicas de criptografia para evitar que os dados, caso sejam acessados por pessoas sem permissão ou haja vazamento de informação, não possam ser lidos e compreendidos.

Todos os componentes e softwares devem ter patches de segurança mais recentes fornecidos pelos fornecedores instalados. Patches críticos de segurança devem ser instalados em no máximo 30 dias após a liberação.

6.3 IDENTIFICAR E AUTENTICAR ACESSO AOS COMPONENTES CRÍTICOS DO SISTEMA

Necessário atribuir identificação exclusiva (ID) para cada pessoa com acesso a sistemas ou software críticos, garantindo que cada pessoa seja o único responsável por suas ações e assim, facilitando a rastreabilidade de cada ação tomada e o responsável pela ação. Sempre que um colaborador que possuir acesso a estes tipos de sistema for desligado da empresa, ou caso seja um prestador de serviço temporário e seu contrato de prestação de serviço chegar ao fim, deve-se revogar as permissões de acesso do usuário deste colaborador, ou caso seja possível, excluir o usuário.

6.3.1 MÉTODOS DE AUTENTICAÇÃO DO USUÁRIO

Além de uma identificação única, a autenticação de acesso aos sistemas deve exigir pelo menos um dos itens a seguir:

- Algo que o usuário saiba, como uma senha ou frase secreta.
- Algo que o usuário tenha, como um dispositivo token ou cartão inteligente.
- Algo que o usuário possa identificá-ló como leitor biométrico.

As senhas ou frases secretas devem possuir no mínimo 8 dígitos com caracteres alfanuméricos.

6.3.2 CONTAS E SENHAS EM GRUPO OU COMPARTILHADAS

Não utilizar contas ou senhas compartilhadas para administração de sistema e outras funções críticas. Não utilizar para administrar componente de sistema.

7. DA POLÍTICA DE ACESSO A INTERNET

7.1. FINALIDADE

Tem como finalidade definir as diretrizes para a utilização da internet da empresa afim de evitar o uso indevido para práticas que possam gerar prejuízos a organização, violação de políticas de segurança e prática de atos ilícitos, como consumo e transferência de material sem autorização de uso e

compartilhamento, transmissão de dados sem autorização, entre outros atos lícitos conhecidos.

7. 2. DEVERES DO SERVIDOR E PRESTADOR DE SERVIÇOS

1. Não repassar ou compartilhar senha de autenticação da conexão segura (VPN).

2. Caso o sigilo da senha ou chave de acesso seja comprometido, informar imediatamente o departamento de TI para que sejam tomadas as medidas de segurança cabíveis.

3. Não utilizar a conexão de internet da empresa para prática de atividades que violam as leis vigentes como consumo e distribuição de qualquer material sem autorização, violando direitos autorais (pirataria), comentários ofensivos ou de cunho pejorativo ou preconceituoso.

4. Utilizar a conectividade de forma segura, para fins lícitos afim de criar oportunidades que possam gerar incidentes de segurança e comprometer a integridade dos serviços e equipamentos.

5. Consultar o departamento de TI sempre que for notada alguma atividade estranha como solicitação para instalação de aplicativo não solicitado, recebimento de mensagens eletrônicas solicitando para acessar link no corpo da mensagem para algum procedimento, etc.

7. 3. DO CORREIO ELETRÔNICO

O objetivo é informar aos servidores do COLOMBO PREVIDÊNCIA quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico do COLOMBO PREVIDÊNCIA é para fins corporativos e relacionados às atividades do quanto à instituição.

A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique ao COLOMBO PREVIDÊNCIA e também não cause impacto no tráfego da rede.

É proibido aos servidores o uso do correio eletrônico do COLOMBO PREVIDÊNCIA para:

- ✓ enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;

- ✓ enviar mensagem por correio eletrônico pelo endereço de seu departamento ou 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 ao COLOMBO PREVIDÊNCIA ou suas unidades 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 ao COLOMBO PREVIDÊNCIA estiver sujeita a algum tipo de investigação;

- ✓ Utilizar o endereço de correio eletrônico corporativo para fins de cadastros pessoais e redes sociais;

- ✓ produzir, transmitir ou divulgar mensagem que:
    - o contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do COLOMBO PREVIDÊNCIA;

    - o contenha ameaças eletrônicas, como: spam, mail *bombing*, vírus de computador e etc.;

- 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 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;

- vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

- inclua imagens criptografadas ou de qualquer forma mascaradas;

- tenha conteúdo considerado impróprio, obsceno ou ilegal;

- seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

- contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;

- tenha fins políticos locais ou do país (propaganda política);

- inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

7. 4. Das páginas de Internet:

Todas as regras atuais da COLOMBO PREVIDÊNCIA visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, ao COLOMBO PREVIDÊNCIA, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A COLOMBO PREVIDÊNCIA, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer servidor, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

O uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Somente os servidores que estão devidamente autorizados a falar em nome do COLOMBO PREVIDÊNCIA para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os servidores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos, redes sociais ou qualquer outra tecnologia correlata que venha surgir na internet.

Os servidores com acesso à internet poderão fazer o download somente de programas ligados diretamente às suas atividades no COLOMBO PREVIDÊNCIA e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela área de tecnologia de informação.

Os servidores não poderão em hipótese alguma utilizar os recursos do COLOMBO PREVIDÊNCIA 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.

Servidores com acesso à internet não poderão efetuar upload de qualquer software licenciado ao COLOMBO PREVIDÊNCIA ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os servidores não poderão utilizar os recursos do COLOMBO PREVIDÊNCIA para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores. O acesso a softwares peer-to-peer (Kazaa, BitTorrente afins), sites de jogos e plataformas de filmes que não tenham relação com as atividades institucionais, não serão permitidas, bem como sites de jogos. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) e os serviços de comunicação instantânea (SKYPE, WHATSAPP, redes sociais e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor ou a área de tecnologia da informação julgue necessário.
Não é permitido acesso a sites de proxy.-

7. 5. É TERMINANTEMENTE PROIBIDO

1. O acesso a páginas com conteúdo inadequado com pornografia, incitação a violência e discurso de ódio.

2. Download de programas piratas.

3. Utilização da conectividade para publicar mensagens constrangedoras ou difamatórias contra colaboradores ou qualquer outro indivíduo.

4. Praticas atividades de hacker ativismo como tentativas de invasão a sistemas ou equipamentos.

5. Compartilhamento de informações confidências ou que possam gerar prejuízos financeiros a empresa.

6. Desinstalar ou desabilitar mecanismos de segurança como navegação protegida.

7. Coletar dados sem autorização e finalidade conhecida.

8. Acessar sites com conteúdo duvidoso e que possam expor a empresa a ataques de criminosos digitais.

9. Acessar sites que façam comércio ilegal de qualquer natureza.

7. 6. MONITORAMENTO DA REDE

Todo o tráfego da rede da empresa é monitorado através de firewall de rede e a limitação a determinados tipos de conteúdo é gerido pelas regras de acesso

configurados no serviço de firewall. Qualquer tipo de conteúdo classificado como indevido é identificado pelo firewall, e consequentemente, identificado o equipamento.

8. IDENTIFICAÇÃO_

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307–falsa identidade). Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os servidores.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal). Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante ao COLOMBO PREVIDÊNCIA e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Se for identificado conhecimento ou solicitação do gestor de uso compartilhado este deverá ser responsabilizado.

A área de tecnologia de informação responde pela criação de usuários dos servidores e na rede.

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.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados).

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.

Todos os servidores/estagiários que deixarem de integrar o quadro da Autarquia, devem ter seus acessos imediatamente bloqueados.

Caso o servidor esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

9. COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos servidores são de propriedade do COLOMBO PREVIDÊNCIA, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um servidor da área de tecnologia de informação, ou de quem este determinar.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes às atividades do COLOMBO PREVIDÊNCIA não deverão ser copiados movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente sem comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos servidores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os servidores do COLOMBO PREVIDÊNCIA e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da área de tecnologia da informação.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

a) Os servidores devem informar qualquer identificação de dispositivo estranho conectado ao seu computador;

b) É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado pela área de tecnologia de informação ou por terceiros devidamente contratados para o serviço;

c) Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de informática;

d) O servidor deverá manter a configuração do equipamento disponibilizado pelo COLOMBO PREVIDÊNCIA, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações;

e) Deverão ser protegidos por senha (bloqueados) todos os terminais de computador quando não estiverem sendo utilizados;

f) Todos os recursos tecnológicos adquiridos pelo COLOMBO PREVIDÊNCIA devem ter imediatamente suas senhas padrões (default) alteradas.

Situações em que é proibido o uso de computadores e recursos tecnológicos do COLOMBO PREVIDÊNCIA:

i. Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;

ii. Burlar quaisquer sistemas de segurança;

iii. Acessar informações confidenciais sem explícita autorização do proprietário;

iv. Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);

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

vi. Usar qualquer tipo de recurso tecnológico para 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;

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

viii. Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

10. PRIVACIDADE DA INFORMAÇÃO

Define-se como necessária a proteção da privacidade das informações, aquelas que pertencem aos seus segurados e/ou beneficiários e que são

manipuladas ou armazenadas nos meios às quais o COLOMBO PREVIDÊNCIA detém total controle administrativo, físico, lógico e legal.
As diretivas abaixo refletem os valores institucionais do COLOMBO PREVIDÊNCIA e reafirmam o seu compromisso com a melhoria contínua desse processo:

• As informações são coletadas de forma ética e legal, com o conhecimento do segurado / beneficiário, para propósitos específicos e devidamente informados;

• As informações são acessadas somente por pessoas autorizadas e capacitadas para seu uso adequado;

• 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;

• As informações somente são fornecidas a terceiros, mediante autorização prévia da Diretoria-Executiva ou para o atendimento de exigência legal ou regulamentar;

• 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.

11. DISPOSITIVOS MÓVEIS

O COLOMBO PREVIDÊNCIA deseja facilitar a mobilidade e o fluxo de informação entre seus servidores. Por isso, permite que eles usem equipamentos portáteis.

Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido pela área de tecnologia de informação, como: notebooks, smartphones e pendrives.

O objetivo é estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os servidores que utilizem tais equipamentos.

O COLOMBO PREVIDÊNCIA, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O servidor, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções no COLOMBO PREVIDÊNCIA, mesmo depois de terminado o vínculo contratual mantido com a instituição.

Todo servidor deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não carregá-los juntos.

O suporte técnico aos dispositivos móveis de propriedade do COLOMBO PREVIDÊNCIA e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação, autorização e sem a condução, auxílio ou presença de um servidor da área de tecnologia de informação.

O servidor deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pela área de tecnologia de informação.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante. É permitido o uso de rede banda larga

de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.

É responsabilidade do servidor, no caso de furto ou roubo de um dispositivo móvel fornecido pelo COLOMBO PREVIDÊNCIA, notificar imediatamente o seu gestor direto e a área de tecnologia de informação.

O servidor deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar ao COLOMBO PREVIDÊNCIA e/ou a terceiros.

12. RESTRINGIR ACESSO FÍSICO AOS DADOS

O acesso físico a dados ou sistemas que armazenam os dados deve ser restrito apenas ao colaborador que necessite do acesso para fins justificados. Qualquer tentativa de acesso de colaborador não autorizado deve ser identificado e analisado o motivo da tentativa de acesso para identificar possível violações de segurança.

13. PROTEJER FISICAMENTE TODAS A MÍDIAS

São considerados como mídias computadores, mídia eletrônica removível (pen drive e cartão de memória), recibos em papel e relatórios impressos. Os procedimentos a seguir devem ser seguidos para garantir a proteção de todas as mídias.

13.1 DISTRIBUIÇÃO DE MÍDIA

Toda distribuição, interna ou externa, necessária de mídia deve ter um controle rígido, contendo:

- Classificação da mídia para determinar a sensibilidade do conteúdo.
- O envio de mídia deve ser realizado por correio expresso ou outro método de entrega que possa ser rastreado com precisão. Deve-se emitir e reter logs de transferência de mídia.

- Antes de distribuir ou mover uma mídia de local, a gerência deve aprovar tal ação, inclusive quando a mídia é distribuída a indivíduos, como parceiros ou prestadores de serviço.

13.2 ARMAZENAMENTO E ACESSIBILIDADE DE MÍDIA

O acesso ao ambiente onde a mídia é armazenada deve ser controlado, sendo permitido apenas o acesso de pessoas autorizadas.

Deve-se anualmente realizar e manter inventário de todas as mídias armazenadas.

13.3 POLÍTICA E PROCEDIMENTO DE DESTRUIÇÃO DE MÍDIA

Mídias que possuírem dados e não forem mais necessárias devem ser destruídas. Caso a mídia seja impressa, ela deve ser triturada e posteriormente incinerada. Mídias digitais devem ter seu conteúdo apagado de modo que não haja possibilidade de recuperação de dados. O processo de destruição de mídia deve ser acompanhado pelo responsável da área de segurança da informação.

Deve-se ainda garantir o armazenamento seguro da mídia antes do processo de destruição a fim de garantir que pessoas não autorizadas possam ter acesso aos dados contidos nas mídias.

14. POLÍTICA PARA COMPARTILHAMENTO DE DADOS COM PROVEDORES DE SERVIÇO

Manter uma lista documentada de todos os provedores de serviços aplicáveis em uso.

Necessário um contrato de prestação de serviço por escrito com todos os provedores de serviço, incluindo reconhecimento da responsabilidade dos provedores de proteger os dados, ou na medida em que possam afetar a segurança de um ambiente de dados.

Além disto, o provedor de serviço deve concordar em fornecer evidências de validação de conformidade com o Padrão de Transmissão de Dados

anualmente. Antes de iniciar as operações com um provedor de serviço, deve-se seguir um processo completo de due diligence (auditoria).
Revisar anualmente as evidências fornecidas pelos provedores de serviço, demonstrando sua conformidade.

15.POLÍTICAS DO PLANO DE RESPOSTA A INCIDENTES

Os incidentes de segurança devem ser identificados e tratados rapidamente de forma controlada para evitar ou reduzir falhas ou danos nos serviços.
Atualmente a empresa conta com um monitoramento de rede e servidores afim de identificar possíveis incidente, porém essa vigilância passa por todos os colaboradores que ao identificar qualquer situação não típica deve comunicar imediatamente o setor de TI para tomar as devidas providências.

16. BACKUP

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.
Os servidores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.
Os backups imprescindíveis, críticos, para o bom funcionamento das atividades do COLOMBO PREVIDÊNCIA, exigem uma regra de retenção especial, seguindo assim as determinações fiscais e legais existentes no país.
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 e solucionado o problema.
Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade.

Os arquivos de backup devem estar disponíveis em servidores externos de arquivo, como segunda fonte.

17. PLANO DE GERENCIAMENTO DE INCIDENTES

17.1. FINALIDADE

Este Plano de Gerenciamento de Incidentes está alinhado com a Política de Segurança da Informação, sendo documento que define as diretrizes de tratamento de incidentes que possam ocorrer nos ambientes de TI, definindo quais processos devem ser seguidos para reestabelecer a operação normal dos serviços o mais rápido possível, de modo a minimizar o impacto nas operações da empresa e limitar as falhas de segurança que possam de alguma forma expor as informações tratadas pela empresa.

17.2. DEFINIÇÕES

Indisponibilidade à rede ou servidor.

Conjunto de informações com registros de todos os erros conhecidos.

TERMO DESCRIÇÃO	
Central de Serviços de TI	Ferramenta utilizada pelos colaboradores como ponto de contato único (abertura de chamados) com a equipe de suporte.
Erro Conhecido	Problema que possui causa raiz e solução documenta. Este problema pode ou não já ter ocorrido no ambiente da empresa.

Evento: Ocorrência anormal de qualquer serviço e que pode ser identificada.

Gerenciamento de Incidentes	Processo de gerenciamento do ciclo de vida dos incidentes, desde a sua detecção e/ou identificação, tratamento, correção de possíveis danos e reestabelecimento de serviços afetados.

Incidente	Um evento confirmado ou sob suspeita que possa causar interrupção de um ou mais serviços ou redução da qualidade do serviço prestado.
Incidente de Segurança	Um evento confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores,

Causa de um ou mais incidentes ou problema incidentes de segurança.
Funcionamento de um ou mais serviços operação normal de serviço atendendo a qualidade estabelecida.

17.3 DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta Política de Segurança da Informação, o COLOMBO PREVIDÊNCIA poderá:

• implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

• tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou solicitação dos Diretores;

• realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

• instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

17.4. DESCRIÇÃO DO PROCESSO DE GERENCIAMENTO DE INCIDENTES

A) ABERTURA DE CHAMADO

Os chamados devem ser registrados pelos usuários do sistema através da Central de Serviços de TI enviado um e-mail para suporte@vnsolution.com.br e se for o caso solicitar urgência no grupo de WhatsApp disponível.

Todos os problemas ou incidentes identificados pelos usuários, devem ser relatados através deste meio de comunicação. Durante o ciclo de vida do chamado, todas as informações relevantes como contato com usuário, atividades realizadas e afins, devem ser registradas no acompanhamento do chamado.

B) CLASSIFICAR E PRIORIZAR

Todos os chamados abertos pelos usuários serão filtrados e categorizados como requisições (melhorias, novas funcionalidades, etc), incidente operacional como falha em uma operação, erro ao requisitar uma função ou incidente de segurança da informação. Após a classificação, o chamado deve receber um nível de prioridade de atendimento, sendo considerado seu impacto nas operações e a urgência causada às operações. As prioridades dos incidentes são classificadas como ‘Baixa’, ‘Média’, ‘Alta’ e ‘Urgente’.

Os atendimentos aos incidentes de segurança terão prioridade considerando os riscos à integridade das informações tratadas. Os chamados relacionados à incidentes serão atendidos considerando a prioridade mais alta (Urgente), e consequentemente, as demais prioridades (Alta, Média e Baixa).

C) INVESTIGAÇÃO E DIAGNÓSTICO

Neste processo, a equipe de suporte deve analisar as informações registradas no chamado de forma que seja possível reproduzir ou diagnosticar o incidente de forma precisa. Para isto deve-se utilizar recursos como:

- Acesso ao colaborador que identificou o problema.
- Procedimentos técnicos da instituição, como simulação no ambiente.
- Consulta com especialistas (Analistas de Redes, Servidores e Segurança).
- Consulta a fornecedores externos de serviços.

D) RESOLUÇÃO E RESTAURAÇÃO DO AMBIENTE

Após identificação da causa do incidente e solução deve-se tomar a devidas medidas para a restauração do ambiente. Esta atividade pode ser executada diretamente pela equipe de suporte ou pelos especialistas da área afetada pelo incidente. É necessário certificar junto ao usuário responsável pela abertura do chamado se as ações tomadas foram eficazes na resolução do incidente e restauração do ambiente.

E) ENCERRAMENTO DO CHAMADO

Após confirmação da restauração do ambiente, a solução aplicada ao incidente deve ser registrada a fim de manter o banco de dados de erros conhecidos atualizado e encerrar o chamado. O usuário que abriu o chamado é informado que o chamado foi encerrado através de e-mail.

17.5. RESPOSANBILIDADESESPECÍFICAS

PAPEL	RESPONSABILIDADE
Equipe de suporte	- Recepcionar chamados - Classificar chamados - Analisar incidente descrito no chamado - Revolver incidente, caso tenha resolução ou conhecimento da causa do problema. - Buscar junto a especialista ou fornecedor externo resolução de incidente. - Registrar resolução do incidente. - Encerrar chamados.
Especialistas	- Auxiliar equipe de suporte em busca de resolução de chamados. - Implementar resolução para incidentes. - Implementar funcionalidades solicitadas pelo usuário que sejam pertinentes ao negócio.
Departamento de	- Manter a Política de Segurança da Informação

Segurança da Informação	atualizada, atualizando as diretrizes de segurança já definidas e inserindo novas. - Manter atualizado o Plano de Gerenciamento de Incidentes. - Atender demandas de segurança identificados através do processo de gerenciamento de incidentes.

17.6. MONITORAMENTO DE DESEMPENHO

O monitoramento dos indicadores de desempenho listados abaixo fará parte do relatório gerencial do processo de gerenciamento de incidentes. Estes dados serão utilizados para identificar quais rotinas ou processo do sistema podem e devem ser melhorados para minimizar a ocorrência de falhas, promovendo a melhora contínua dos serviços:

A) NÚMEROS DE INCIDENTES RELATADOS

Mensurar número mensal de incidentes relatados e quantidade de chamados abertos pelos usuários.

B) NÚMEROS DE CHAMADOS REABERTOS E REINCIDENTES

Quantidade de chamados reabertos pelos usuários e reincidência de incidentes relatados anteriormente.

C) NÚMEROS DE INCIDENTES ATENDIDOS

Total de chamados atendidos com sucesso pela equipe de suporte

17.7. CLASSIFICAÇÃO DE INCIDENTES

INCIDENTES	TIPO	DESCRIÇÃO

Acesso não autorizado	Incidente de segurança	Tentativa de acesso não autorizado.
Acesso bloqueado	Incidente de segurança	Falha de sistema impede acesso de usuário autorizado.
Uso indevido	Incidente de segurança	Violação das políticas de segurança no uso de serviços.
Tentativa de invasão	Incidente de segurança	Varredura da rede para identificar falhas de segurança como portas de serviço desprotegidas e acesso sem verificar autorização
Vírus	Incidente de segurança	Software malicioso com intuito de causar falhas ou indisponibilidade dos serviços
Falha de serviço	Incidente de TI	Indisponibilidade ou erro de sistema.
Requisição de melhorias	Requisição de TI	Usuário solicita melhoria em algum serviço ou implantação de nova funcionalidade.
Requisição de serviço	Requisição de TI	Solicitação para alterar permissão de acesso, alteração de senha, bloqueio ou exclusão de conta de usuário.

18. PENALIDADES

Ao ser identificada alguma infringência a esta Política de Segurança da Informação, será remetido o caso para apurações com sindicância e/ou Processo Administrativo Disciplinar nos termos legais. Em se tratando de prestadores de serviços/ terceirizados poderão também sofrer as penalidades impostas no contrato.

19. APROVAÇÃO E VIGÊNCIA

Esta Política de Segurança de Informação foi elaborada e revisada com apoio da equipe técnica de Tecnologia da Informação, entrará em vigência a partir da data de aprovação pela Diretoria Executiva, terá prazo indeterminado, devendo ser revisto sempre que necessário, com as devidas ciências aos servidores, colaboradores e fornecedores.

Colombo, 29 de fevereiro 2024

gov.br Documento assinado digitalmente
WILTON LUIZ CARRAO
Data: 08/04/2024 13:30:53-0300
Verifique em https://validar.iti.gov.br

Wilton Luiz Carrão
Diretor Superintendente

gov.br Documento assinado digitalmente
ALEKSANDRA DO CARMO ULLMANN
Data: 08/04/2024 16:37:40-0300
Verifique em https://validar.iti.gov.br

Aleksandra do Carmo Ullmann
Diretora de Benefícios

gov.br Documento assinado digitalmente
GIOVANI CORLETTO
Data: 09/04/2024 10:25:28-0300
Verifique em https://validar.iti.gov.br

Giovani Corletto
Diretor Financeiro

Colombo Previdência
PREVIDÊNCIA DOS SERVIDORES PÚBLICOS MUNICIPAIS DE COLOMBO

Termo de Ciência

TERMO DE RECEBIMENTO E COMPROMISSO COM A POLITICA DE SEGURANÇA DA INFORMAÇÃO DA COLOMBO PREVIDÊNCIA

Declaro que recebi e li a Política de Segurança da Informação da Colombo Previdência e estou ciente de seu conteúdo e da sua importância para o exercício de todas as atividades desta Autarquia.

A assinatura do presente Termo, é manifestação de minha concordância e do meu compromisso em cumpri-lo integralmente.

Colombo, _____ de _____ de 20____.

_____

Nome Completo e/ou Razão Social

CPF/CNPJ: _____/_____