Política de Segurança da Informação Facsenac-DF

SILVERS PRATAS

Emerson Jesus

Lucas Vanique

Renato da silva

Orientador: Prof. Clemilson Oliveira

Palavras-chave: Política; Segurança; Informação; Desenvolvimento.

PSI - Política de Segurança da Informação

1. Sobre a Política de Segurança da Informação (PSI)

A SILVERS PRATAS tem na informação um dos seus principais ativos, devendo ele ser adequadamente utilizado e protegido contra riscos, ameaças, violações, acessos não autorizados e danos. É imprescindível, portanto, a adoção de condutas, normas e procedimentos padronizados que tenham como objetivo garantir a proteção dos três aspectos básicos da segurança da informação: confidencialidade, integridade e disponibilidade.

Uma política de segurança da informação tem por objetivo possibilitar o gerenciamento da segurança em uma organização, estabelecendo regras e padrões para proteção da informação. A política possibilita manter a confidencialidade, garantir que a informação não seja alterada ou perdida e permitir que a informação esteja disponível quando for necessário.

- **O que é integridade de informações?** Consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados. Sinaliza, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário.

- **O que é confidencialidade de informações?** Consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação. Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento.

- **O que é autenticidade de informações?** Consiste na garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações.

- **O que é disponibilidade de informações?** Consiste na garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática. Manter a disponibilidade de informações pressupõe garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações.

- **Por que é importante zelar pela segurança de informações?** A informação é um ativo muito importante para qualquer empresa, podendo ser considerada, atualmente, o recurso patrimonial mais crítico. Informações adulteradas, não disponíveis, sob conhecimento de pessoas de má-fé ou de concorrentes podem comprometer significativamente, não apenas a imagem da instituição perante terceiros, como também o andamento dos próprios processos empresariais. É possível inviabilizar a continuidade de uma empresa se não for dada a devida atenção à segurança de suas informações.

- **Quem são os responsáveis por elaborar a PSI?** É recomendável que na estrutura da empresa exista uma área responsável pela segurança de informações, a qual deve iniciar o processo de elaboração da política de segurança de informações, bem como coordenar sua implantação, aprová-la e revisá-la, além de designar funções de segurança. Entretanto as pessoas de áreas críticas da instituição devem participar do processo de elaboração da PSI, como a alta administração e os diversos gerentes e proprietários dos sistemas informatizados. Além disso, é recomendável que a PSI seja aprovada pelo mais alto dirigente da empresa.

- **O que fazer quando a PSI for violada?** A própria Política de Segurança de Informação deve prever os procedimentos a serem adotados para cada caso de violação, de acordo com a severidade, a amplitude e o tipo de infrator. A punição pode ser desde uma simples advertência verbal ou escrita até uma ação judicial.

- **Uma vez definida, a PSI pode ser alterada?** A PSI não só pode ser alterada, como deve passar por processo de revisão definido e periódico que garanta a reavaliação a qualquer mudança que venha afetar a análise de risco original, tais como: incidente de segurança significativo, novas vulnerabilidades, mudanças organizacionais ou na infraestrutura tecnológica. Além disso, deve haver análise periódica da efetividade da política, demonstrada pelo tipo, volume e impacto dos incidentes de segurança.

2. Escopo

Os objetivos e diretrizes aqui estabelecidos serão desenvolvidos para toda a organização da SILVERS PRATAS, devendo ser observados por todos empregados, colaboradores, fornecedores e prestadores de serviço, e se aplicam à informação em qualquer forma (arquivos eletrônicos, mensagens eletrônicas, dados de intranet e internet, bancos de dados, arquivos impressos, informações expressadas verbalmente, mídias de áudio e vídeo, dentre outros) e em qualquer meio ou suporte, durante todo o seu ciclo de vida (criação, manuseio, divulgação, armazenamento, transporte e descarte).

3. Conceitos e Definições

Abaixo os principais conceitos referidos neste documento, de forma a evitar dificuldades de interpretação ou ambiguidades:

1. **Algoritmo:** conjunto das regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número finito de etapas;
2. **Ameaça:** causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou empresa.
3. **Antispyware**: software de segurança que tem o objetivo de detectar e remover softwares maliciosos;
4. **Assinatura Digital:** mecanismo criptográfico que tem por objetivo assinar documentos digitalmente;
5. **Ativo de Informação:** os meios de armazenamento, transmissão e processamento, os sistemas de informação, como os locais onde se encontram esses meios e as pessoas que têm acesso a eles;
6. **Backup**: é o processo de cópia de dados de um dispositivo de armazenamento para outro com o objetivo de proporcionar a proteção contra a perda dos originais;
7. **Certificação Digital:** é um arquivo eletrônico que serve como identidade virtual para uma pessoa física ou jurídica, e por ele podem ser feitas transações online com garantia de autenticidade e proteção das informações trocadas;
8. **Classificação da informação:** processo que tem como objetivo identificar e definir níveis e critérios adequados para a proteção das informações, de acordo sua importância para as organizações;
9. **Continuidade de Negócios:** Capacidade estratégica e tática da empresa de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação de atividades críticas, de forma a manter suas operações em um nível aceitável;
10. **Controle de Acesso:** processo por meio do qual os acessos aos sistemas e a seus respectivos dados são autorizados ou negados; os acessos autorizados e, em alguns casos, também os negados ficam registrados para posterior auditoria;
11. **Criptografia:** mecanismo de segurança e privacidade que torna determinada comunicação (textos,

imagens, vídeos, entre outros) ininteligível para quem não tem acesso aos códigos de tradução da mensagem;

12. **Dispositivos Móveis:** equipamentos portáteis dotados de capacidade computacional ou dispositivos removíveis de memória para armazenamento;

13. **Gestão de Segurança de Informação e Comunicação**: processo que visa a proteção dos ativos de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão e a modificação desautorizada de dados armazenados ou em trânsito;

14. **Incidente**: qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança dos sistemas, das informações ou das redes de computadores;

15. **Impacto:** mudança adversa no nível obtido dos objetivos do negócio;

16. **Plano de Continuidade de Negócio (PCN):** documento que estabelece mecanismos para restabelecer a atividade da empresa, em caso de interrupção;

17. **Programas Antivírus:** programas usados para proteger e prevenir computadores e outros aparelhos de códigos ou vírus, a fim de dar mais segurança ao usuário;

18. **Termo de Responsabilidade e Sigilo:** documento pelo qual o empregado ou colaborador se compromete a não revelar as informações de caráter secreto, sigiloso e confidencial da empresa;

19. **Wireless:** tecnologia que significa “sem fio”, e possibilita a transmissão da conexão entre pontos distantes sem precisar usar fios (como ocorrem em telefones sem fio, rádios ou celular).

4. Objetivos da Política de Segurança da Informação

- Estabelecer diretrizes que permitam aos colaboradores, fornecedores e prestadores de serviços da SILVERS PRATAS, seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades operacionais e de proteção legal da empresa e dos seus colaboradores.

- Garantir que os recursos computacionais e serviços de Tecnologia da Informação - TI serão utilizados de maneira adequada. O usuário deve conhecer as regras para utilização da informação de maneira segura, evitando exposição que possa prejudicar a SILVERS PRATAS, colaboradores e terceiros.

- A definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento. Deve implementar controles para preservar os interesses da empresa, contra danos que possam ser consideradas como violação ao uso dos serviços, considerados proibidos.

5. Aplicação da Política de Segurança da Informação

A Política e os Enunciados Normativos de Segurança da Informação devem ser divulgados a todos os empregados da SILVERS PRATAS e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

Os Procedimentos de Segurança da Informação ficarão disponíveis na rede interna da empresa, e devem ser divulgados às áreas diretamente relacionadas à sua aplicação.

6. Princípios da Política de Segurança da Informação

As diretrizes estabelecidas deverão ser seguidas por todos os colaboradores, bem como os fornecedores e prestadores de serviço que se aplicam à informação em qualquer meio ou suporte.
Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela SILVERS PRATAS.

É também obrigação de cada colaborador se manter atualizado em relação a esta política e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da área de tecnologia de informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações. Portanto, o conjunto de documentos que compõe esta PSI guiar-se-á pelos seguintes princípios gerais:

1. **Menor privilégio**: Usuários e sistemas devem ter a menor autoridade e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

2. **Segregação de função:** Funções de planejamento, execução e controle devem ser segregadas de forma a reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos.

3. **Auditabilidade:** Todos os eventos significantes de sistemas e processos devem ser rastreáveis até o evento inicial.

4. **Mínima dependência de segredos**: Os controles deverão ser efetivos ainda que a ameaça saiba de suas existências e como eles funcionam.

5. **Controles automáticos:** Sempre que possível, controles de segurança automáticos deverão ser utilizados.

6. **Defesa em profundidade:** Controles devem ser desenhados em camadas de forma que quando uma camada de controle falhar, haja um tipo diferente de controle em outra camada para prevenir a brecha de segurança.

7. **Exceção aprovada:** Exceções à PSI deverão sempre ter aprovação superior.

8. **Substituição da segurança em situações de emergência:** Controles somente devem ser desconsiderados de formas predeterminadas e seguras. Devem sempre existir procedimentos e controles alternativos para minimizar o nível de risco em situações de emergência.

7. Requisitos da Política de Segurança da Informação

PSI - Política de Segurança da Informação

A Política e os Enunciados Normativos de Segurança da Informação devem ser divulgados a todos os empregados da SILVERS PRATAS e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

Os Procedimentos de Segurança da Informação ficarão disponíveis na rede interna da desta empresa, e devem ser divulgados às áreas diretamente relacionadas à sua aplicação.

8. Monitoramento e Auditoria

A rede, os sistemas, as informações e os serviços utilizados pelos usuários são de exclusiva propriedade da SILVERS PRATAS, não podendo ser interpretados como de uso pessoal. Todos os empregados da empresa devem ter ciência de que o uso da rede, das informações e dos sistemas de informação da empresa pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política e dos Enunciados Normativos de Segurança da Informação e, conforme o caso, servir como **evidência em processos administrativos e/ou legais**. Visando efetivar esse controle, a SILVERS PRATAS poderá:

I. Implantar sistemas de monitoramento em estações de trabalho, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, de forma que a informação gerada ou trafegada por eles permita a sua rastreabilidade, identificando usuários e respectivos acessos efetuados;

II. Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria no caso de exigência judicial;

III. Realizar, a qualquer tempo, inspeção física nos equipamentos de sua propriedade;

IV. Instalar sistemas de proteção, preventivos e/ou repressivos, para garantir segurança das informações e dos perímetros de acesso;

V. Desinstalar, a qualquer tempo, qualquer software ou sistema que represente risco ou esteja em desconformidade com políticas, normas, procedimentos e princípios vigentes.

9. Responsabilidades Específicas

a) Cabe a todos os empregados, diretores, supervisores e estagiários, prestadores de serviço e terceirizados da SILVERS PRATAS:

b) Cumprir fielmente a Política, os Enunciados Normativos e os Procedimentos de Segurança da Informação da SILVERS PRATAS;

c) Manter-se atualizado em relação a esta Política, demais normas e procedimentos relacionados, buscando informação junto a seu superior ou junto à autoridade competente sempre que não estiver absolutamente seguro quanto a obtenção, uso e/ou descarte de informações;

d) Promover a segurança de seu usuário da empresa, departamental ou de rede local, bem como de seus respectivos dados, credenciais de acesso e quaisquer informações a que tenha acesso em virtude do cargo que ocupa;

e) Utilizar de forma ética, legal e consciente os recursos computacionais e informacionais, estando ciente de que sua estrutura não poderá ser utilizada para fins particulares e que ações que tramitem em sua rede poderão ser auditadas;

f) Os colaboradores, terceiros e passantes assumem inteiramente a responsabilidade pelo usuário fornecido para acesso a rede, aplicações internas, externas, aplicativos móveis, internet e sistemas de forma individual e intransferível.

g) Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados;

h) Cumprir as leis e as normas que regulamentam os aspectos da propriedade intelectual;

Controle de Acesso

Devem ser instituídas normas ou procedimentos que garantam o controle de acesso às informações e instalações.

Considerando que ambientes de computação móvel e de trabalho remoto são necessários para as atividades da empresa e que podem consistir em pontos fracos do sistema de gestão de segurança, devem ser instituídas normas e procedimentos que garantam a segurança da informação em ambientes de computação móvel e de trabalho remoto.

No caso de ambientes físicos de armazenamento de informações, deve haver, quando necessário, um sistema de controle de acesso que o registre. Se possível, deve ser usado um método de autenticação baseado em cartão de identificação/biometria ou MFA.

No caso particular de recursos de TI, deve haver uma política estabelecida de criação e manutenção de senhas. Deve haver um sistema único de autenticação e a autenticação deve ser de caráter pessoal (cada pessoa com uma única identificação, vinculada a ela e não ao cargo que ocupa). As informações para autenticação devem ser consideradas pessoais e intransferíveis.

8.1. Política de Senhas

As senhas são um aspecto crítico da segurança do computador. Uma senha fraca ou comprometida pode resultar no acesso não autorizado aos nossos dados mais confidenciais e/ou na exploração dos nossos recursos. Todos os funcionários, incluindo prestadores de serviços e fornecedores com acesso aos sistemas da SILVERAS PRATAS são responsáveis por tomar as medidas apropriadas, conforme descrito abaixo, para selecionar e proteger suas senhas.

Propósito

O objetivo desta política é estabelecer um padrão para o uso seguro e proteção de todas as senhas relacionadas ao trabalho.

Criação e uso de senha

Todas as senhas de nível de usuário e de sistema devem estar em conformidade com as Diretrizes de Construção de Senhas.

Os usuários devem usar uma senha separada e exclusiva para cada uma de suas contas relacionadas ao trabalho. Os usuários não podem usar nenhuma senha relacionada ao trabalho para suas próprias contas pessoais.

Os funcionários estão autorizados a usar gerenciadores de senhas autorizados e aprovados para armazenar e gerenciar com segurança todas as suas senhas relacionadas ao trabalho.

As contas de usuário que possuem privilégios de nível de sistema concedidos por meio de associações a

grupos ou programas como **SUDO** devem ter uma senha exclusiva de todas as outras contas mantidas por esse usuário para acessar privilégios de nível de sistema. Além disso, é altamente recomendável que alguma forma de autenticação multifator seja usada para quaisquer contas privilegiadas.

Proteção de senha

As senhas não devem ser compartilhadas com ninguém, incluindo supervisores e colegas de trabalho. Todas as senhas devem ser tratadas como informações confidenciais e confidenciais da SILVERS PRATAS. A Segurança da Informação da empresa reconhece que os aplicativos legados não suportam sistemas proxy em vigor.

As senhas não devem ser inseridas em mensagens de e-mail ou outras formas de comunicação eletrônica, nem reveladas por telefone a ninguém.

As senhas podem ser armazenadas apenas em gerenciadores de senhas autorizados pela organização.

Não use o recurso **"Lembrar senha"** de aplicativos (por exemplo, navegadores da web).
Qualquer indivíduo que suspeite que sua senha possa ter sido comprometida deverá relatar o incidente e alterar todas as senhas relevantes.

Autenticação multifator

A autenticação multifator é altamente recomendada e deve ser usada sempre que possível, não apenas para contas relacionadas ao trabalho, mas também para contas pessoais.

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

A EMPRESA deverá realizar, de forma sistemática, a avaliação dos riscos relacionados à segurança da informação, que servirá como base, entre outros, para o Plano de Continuidade de Negócios (PCN).

8.3 Redes sem fio

Objetivo

Definir as diretrizes relacionadas à utilização da rede sem fio da SILVERS PRATAS.

Definições

Conforme descrito no anexo Definições relacionadas à Política de Segurança da Informação.

Abrangência

Esta norma aplica-se a todos os usuários que utilizam redes sem fio da empresa.

- ✓ O acesso à rede sem fio da empresa é de uso exclusivo de usuários com credenciais de acesso e que utilizem estações de trabalho corporativas.
- ✓ A SILVERS PRATAS disponibiliza uma rede sem fio para visitantes para o exclusivo acesso à Internet e com as mesmas regras corporativas de controle de conteúdo. Este ambiente será segregado do ambiente corporativo, e seus usuários utilizarão credenciais de acesso temporárias;

- ✓ A SILVERS PRATAS disponibiliza uma rede sem fio para dispositivos móveis apenas para usuários elegíveis. Este ambiente será segregado, e o acesso será validado através da utilização de certificados digitais vigentes previamente implementados em equipamentos homologados;

- ✓ A utilização da rede sem fio é uma concessão da SILVERS PRATAS aos usuários que necessitem deste recurso para desempenhar suas funções e poderá ser suspensa, a qualquer momento, caso sejam identificadas situações que possam comprometer a rede de dados da empresa.

Papéis e Responsabilidades

- ✓ Usuário:

- o Solicitar credenciais de acesso temporárias para a utilização da rede sem fio de visitantes caso necessário o acesso a internet; o Comunicar imediatamente a área de informática, caso dispositivos móveis com acesso autorizados à rede sem fio sejam substituídos, roubados ou furtados;

- ✓ Gestor:

- o Comunicar a área de informática, caso identifique o mal uso dos recursos disponíveis.

- ✓ Área de informática:

  - o Administrar os acessos à rede sem fio; o Revogar a concessão de acesso à rede sem fio, caso identificado mau uso ou ameaça ao ambiente.

8.4 Dos Gestores/Gerentes

Cabe a todo gestor de área:

A. Cumprir e fazer cumprir esta Política, os Enunciados Normativos e os Procedimentos de Segurança da Informação;

B. Assegurar que suas equipes possuam acesso e conhecimento desta Política, dos Enunciados Normativos e dos Procedimentos de Segurança da Informação aplicáveis;

C. Ajudar a redigir os Procedimentos de Segurança da Informação relacionados às suas áreas;

D. Comunicar imediatamente eventuais casos de violação de segurança da informação.

E. Gerentes do mais alto nível – Estão envolvidos com toda a responsabilidade da segurança da informação. Podem delegar a função de segurança, mas são vistos como o principal foco quando são considerados os eventos relacionados com a segurança.

8.5 Descarte seguro para ativos de informação

Mídia é um meio de armazenamento ou tecnicamente um suporte para informação e inclui desde discos rígidos a registros em papel. O descarte de mídia não é descarte de informação, pois é objeto de legislação especifica. Informação somente pode ser descartada depois de devido processo e autorização. Mídias

somente podem ser descartadas se a informação armazenada puder ser descartada ou tiver sido preservada em outro meio.

Portanto, o descarte de mídias deve compreender, entre outros:

- métodos de controle de classificação de documentos que permitam identificar mídias contendo informações sensíveis, de maneira que sejam guardadas e destruídas de maneira segura;
- procedimentos de autorização de descarte;
- métodos e procedimentos de coleta e descarte para cada tipo de mídia;
- métodos e procedimentos para o controle do descarte de mídias sensíveis de maneira a manter, sempre que possível, uma trilha de auditoria.

8.6 Da Gerência de Tecnologia da Informação

A Gerência de Tecnologia da Informação será responsável pela gestão do uso de tecnologias necessárias ao bom andamento dos negócios DA EMPRESA e de ações preventivas.

a) Propor normas relativas à segurança da informação e de comunicações;

b) Assessorar a implementação das ações de segurança da informação e comunicações da empresa;

c) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e de comunicações;

d) Analisar os casos de violação da Política e dos Enunciados Normativos de Segurança da Informação, encaminhando à autoridade competente, quando for o caso;

e) Propor o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação;

f) Determinar a elaboração de relatórios, levantamentos e análises que deem suporte à gestão de segurança da informação e à tomada de decisão;

g) Acompanhar o andamento dos principais projetos e iniciativas relacionados à segurança da informação;

h) Propor a relação de “responsáveis” pelas informações da SILVRES PRATAS.

Da Gerência de Pessoal

Cabe à Coordenação Geral de Gestão de Pessoas:

a) Colher assinatura do Termo de Sigilo e Responsabilidade de todos os empregados da SILVERS PRATAS, arquivando-o nos respectivos prontuários;

b) Informar a Área de Tecnologia Da Informação sobre desligamentos, licenças, afastamentos e modificações no quadro funcional, para que sejam tomadas as medidas cabíveis em relação à segurança da informação.

BACKUP (CÓPIA DE SEGURANÇA)

Os procedimentos próprios ao serviço de backup (cópia de segurança) deverão ser fixados em Enunciado Normativo complementar, considerando as seguintes diretrizes gerais:

a) A realização do backup desta empresa consistirá no armazenamento da cópia dos dados contidos nos computadores servidores da SILVERS PRATAS. A realização de backup dos dados contidos nas estações de trabalho é de responsabilidade de cada usuário. A empresa não se responsabiliza por nenhum conteúdo presente nas máquinas utilizadas pelos usuários;

b) Todos os documentos pertinentes às atividades da empresa deverão ser armazenados nos servidores da própria empresa. Tais arquivos, se gravados apenas localmente nos computadores dos usuários, não serão incluídos na rotina de backup e poderão ser perdidos caso ocorra uma falha na máquina, situação em que a responsabilidade será inteiramente do usuário, podendo ele ser responsabilizado por quaisquer prejuízos à SILVERS PRATAS;

c) Arquivos pessoais ou não pertinentes às atividades da empresa como: (fotos, músicas, vídeos, entre outros) não deverão ser copiados ou movidos para os drives de rede. Caso identificados, esses arquivos poderão ser excluídos sem a necessidade de comunicação prévia ao usuário;

d) É proibido o armazenamento de informações corporativas, tais como bases de dados, arquivos, ou demais documentos em locais inadequados, tais como serviços de armazenamento em nuvem, computadores pessoais ou servidores de prestadores de serviço, salvo com a autorização.

10. Das Disposições Finais

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da SILVERS PRATAS. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes.

Sua elaboração e revisão deverão ser precedidos pelo responsável de TI, sendo posteriormente aprovado por dirigentes superiores competente.

As normas aqui descritas deverão sofrer alterações sempre que necessário, sendo que deverão ser registradas pelos responsáveis de TI, aprovada por pessoas competente e divulgadas pelo próprio setor responsável da TI, dentro da estrutura organizacional da SILVERS PRATAS, considerando-se do o tempo hábil para eventuais providências sejam tomadas.

TERMO DE CIÊNCIA E CONHECIMENTO

TERMO DE CIÊNCIA E CONHECIMENTO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI da Silvers Pratas.

Declaro que recebi a Política de Segurança da Informação - PSI da Silvers Pratas estando ciente de seu conteúdo e da sua importância para o bom exercício funcional do próprio (**NOME DO EMPREGADO**).

A assinatura do presente Termo, anexo a referida Política de Segurança da Informação, é manifestação de minha concordância e do meu compromisso em cumpri-lo integralmente.

PSI - Política de Segurança da Informação

Brasília-DF, _____ de _____ de 20____.

11. Referencias

Normas ABNT NBR ISO/IEC 27001:2013;
ABNT NBR ISO/IEC 27002:2013;
Lei Federal nº 12.965/2014, que instituiu o Marco Civil da Internet;
Artigo 482 do Decreto-Lei nº 5.452/1943 (Consolidação das Leis Trabalhistas - CLT);
https://www.meupositivo.com.br/panoramapositivo/plano-de-seguranca-da-informacao/#:~:text=Como%20elaborar%20um%20plano%20de%20seguran%C3%A7a%20da%20informa%C3%A7%C3%A3o%3F,...%206%20Revise%20e%20atualize%20o%20plano%20 ;
https://blog.binario.cloud/politica-de-seguranca-da-informacao-5-passos-para-criar-e-implementar/ ;
https://www.gov.br/gsi/pt-br/ssic;
FERREIRA, F. N. F.; ARAÚJO, M. T. D. **Políticas de Segurança da Informação - Guia Prático para elaboração e implementação**. Rio de Janeiro: Ciência Moderna, 2008;

https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros;
https://www.gov.br/gsi/pt-br/ssic/legislacao;