MAIO | 2022

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO 2022 - 2024

IPREV DF
Instituto de Previdência dos Servidores do Distrito Federal

GDF
É tempo de ação.

INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO DISTRITO FEDERAL

Governador do Distrito Federal
Ibaneis Rocha

Vice-Governador do Distrito Federal
Marcus Vinícius Britto

Presidente do Instituto de Previdência dos Servidores do Distrito Federal
Ney Ferraz Junior

Diretora de Previdência
Ledamar Sousa Resende

Diretor de Administração e Finanças
Paulo Ricardo Andrade Moita

Diretor de Investimentos
Jefferson Nepomuceno Dutra

Diretor Jurídico
Raquel Galvão Rodrigues da Silva

Diretoria de Governança, Projetos e Compliance
Sylvia Neves Alves (interina)

Elaboração
Rômulo Rodrigues de Paiva
Karoliny Pires Matias
Cleiton Cavalcante Ferreira

Diagramação
Unidade de Comunicação Social - UCS

SUMÁRIO

SUMÁRIO

1. INTRODUÇÃO

A informação é um elemento essencial para todos os processos de negócio de qualquer organização, por tanto à informação é o ativo mais valioso da organização, e deve ser protegido e cuidado, esse cuidado se dá por meio de regras, normas, procedimentos e políticas, essas informações podem ser alvo de uma série de ameaças com a finalidade de explorar as vulnerabilidades e causar prejuízos consideráveis.

O Instituto de Previdência dos Servidores do Distrito Federal – Iprev/DF, sendo a autarquia do regime especial responsável pela gestão do Regime de Próprio de Previdência Social do Distrito Federal, é uma instituição onde se circula um grande número de informações sensíveis, sejam de cunho pessoal de servidores e pensionistas, ou até movimentações financeiras internas e externas, faz necessário implementar uma Política de Segurança da Informação de modo a reduzir as chances de perda de dados, fraudes ou invasões indevidas.

2. OBJETIVO

Art. 1° A Política de Segurança da Informação do Iprev/DF, tem por finalidade definir diretrizes estratégicas no manuseio, tratamento, controle dos dados, informações classificadas e sensíveis, e conhecimentos produzidos, armazenados ou transmitidos por qualquer meio no âmbito do Iprev/DF, com o propósito de garantir à confidencialidade, integridade, disponibilidade e autenticidade.

3. ABRANGÊNCIA

Art. 2° Ficam submetidos à Política de Segurança da Informação do Iprev/DF, todos os servidores, estagiários, prestadores de serviços e demais agentes públicos ou privados que tenha qualquer tipo de acesso aos dados ou informações, sob pena de responsabilidade, conforme previsto na legislação brasileira.

4. PRINCÍPIO

Art. 3° Garantir que à Política de Segurança da Informação do Iprev/DF, seja conhecida e compreendida por todos, conscientizando-os sobre os riscos e responsabilidades existentes e quais medidas devem ser adotadas na ocorrência de algum incidente de segurança da informação de forma a atingir a melhor proteção à informação.

5. CLASSIFICAÇÃO DAS INFORMAÇÕES

Art. 4° As informações são classificadas conforme sua sensibilidade e criticidade, naquilo que diz respeito a estabelecer o grau de sigilo adequado a sua proteção e identificação nos seguintes níveis:

- Pública – Informações que podem ser disponibilizadas e acessíveis a consulta irrestrita a qualquer pessoa.

Exemplo:
- Portal da Transparência;
- Editais de licitações, portarias.

- Interna – Informações que podem ser acessadas apenas por servidores do Iprev/DF.

Exemplo:
- Memorandos, Políticas, Procedimento internos;
- Lista de telefones internos, lista de e-mails;
- Intranet, campanhas internas e avisos.

- Confidencial – Informações que estão acessíveis apenas a um grupo de servidores autorizados do Iprev/DF;

Exemplo:
- Dados cadastrais dos servidores;
- Processos judiciais.

- Restrita – Dados acessíveis apenas a servidores previamente definidos, sempre associados aos interesses estratégicos do Iprev/DF.

Exemplo:
- Resultado de auditorias internas;

6. NORMAS DE SEGURANÇA DA INFORMAÇÃO

Art. 5° As normas e procedimentos que complementam está Política de Segurança da Informação, abordam os seguintes aspectos: segurança física e logica:

- Segurança Física;
- Política de Senhas;
- Acesso à Rede;
- Estação de Trabalho;
- Equipamentos Particulares e Dispositivos Móveis;
- Home Office/Teletrabalho;
- E-mail Corporativo;
- Gestão de Contas de Usuários;
- Back-up;
- Gestão de Mudanças;
- Privacidade;
- Gestão de Incidentes;
- Criptografia;
- Gestão de incidentes;

7. SEGURANÇA FÍSICA

Art. 6° A segurança física se baseia no acesso físico das pessoas aos ambientes que tenham equipamentos de tecnologia da informação, garantindo a proteção de equipamento de acessos não autorizados, limitando assim a circulação apenas de pessoas treinadas, capacitadas e autorizadas para manuseio desses equipamentos, com propósito principal prevenir os danos e possíveis interferências nos recursos de processamento das informações devido ao acesso físico não autorizado.

Art. 7° Toda e qualquer pessoa que necessitar ingressar no Iprev/DF, além da área destinada para o atendimento ao público e do setor de protocolo, deverá ser devidamente identificada, nas áreas de recepção e devem receber um selo de identificação para ser colocado em local visível, e somente sejam concedidas para finalidades específicas e autorizadas.

Art. 8° O controle e monitoramento do acesso físico, bem como a proteção contra ameaças externas e do meio-ambiente nas dependências do prédio até a porta do Iprev/DF é de total responsabilidade da administração predial onde a instituição está instalada.

Art. 9° O controle de entrada e saída dos servidores e colaboradores nas dependências internas do Iprev/DF, se dá mediante ao uso de senha de acesso a fechadura eletrônica, limitando assim a circulação de pessoas não autorizadas.

Parágrafo único: Toda e qualquer acesso de terceiros que adentrar nas dependências internas do Iprev/DF deverá ser acompanhada durante toda sua permanência, por um servidor do instituto.

Art. 10° É vetada a entrada de qualquer pessoa não autorizada nas dependências internas do Iprev/DF.

Art. 11° O acesso às áreas em que são processadas ou armazenadas informações sensíveis é restrito apenas ao pessoal técnico autorizado e a equipe técnica do Iprev/DF.

Art. 12° As instalações de armazenagem de dados tecnologia da Informação deve ser protegidas de forma a evitar acesso não autorizado.

Art. 13° É obrigatório que todos os servidores, estagiários, fornecedores e todos os visitantes, tenham alguma forma visível de identificação.

Art. 14° As instalações-chave de Tecnologia da Informação devem ser localizadas de maneira a evitar acesso do público.

Art. 15° É vedado o uso de máquinas fotográficas, gravadores de vídeo ou áudio ou outros equipamentos de gravação, tais como câmeras em dispositivos móveis, salvo autorização prévia justificada.

Art. 16° Compete a Administração Predial onde o Iprev/DF está instalado:

I. Zelar pelas condições ambientais, como temperatura e umidade, e sejam monitoradas a fim de detectar com antecedência condições que podem afetar negativamente as instalações de processamentos da informação.

II. O edifício deve ser dotado de proteção contra raios.

III. Assegurar o funcionamento adequado do suprimento de energia elétrica, telecomunicações e ar-condicionado.

IV. Disponibilizar toda estrutura de rede física de computadores. Exceto “ativos de rede” switch, roteadores e concentradores.

Art. 17° Compete à Gerência de Suporte ao Usuário e Telecomunicação do Iprev/DF:

I. A instalação, manutenção e configuração das estações de trabalho;

II. A instalação dos ramais telefônicos;

III. A instalação e configuração de impressoras, datashow, Tvs e outros equipamentos de tecnologia da informação;

IV. Instalação e configuração de anti-virus e anti-spam;

8. POLÍTICA DE SENHAS

Art. 18 °: A senha é a forma mais convencional de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identidade do servidor, evitando que uma pessoa, se faça passar por outra. O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 - falsa identidade). Com o objetivo de orientar a criação de senhas seguras, ficam estabelecidas as seguintes regras:

I. A senha é de total responsabilidade do servidor, sendo proibida a sua divulgação ou empréstimo, devendo a mesma, ser imediatamente alterada no caso de suspeita de uso indevido;

II. A senha inicial será fornecida pela Gerencia de Redes e Monitoramento via e-mail institucional no ato da posse do servidor, solicitado pela Gestão de Pessoas – Iprev/DF, o servidor empossado será informado via correio eletrônico das credências e forma de acesso;

III. As credenciais não poderão ser fornecidas por telefone, comunicador instantâneo ou outra forma que não assegure a identidade do servidor;

IV. É obrigatório aos servidores, zelarem pela confidencialidade de sua senha de acesso, podendo ser responsabilizados pelas operações realizadas com a utilização de suas credenciais;

V. A equipe técnica do Iprev/DF deverá possuir contas e senhas individualizadas com privilégios administrativos e somente deverão utilizar essas contas para o desempenho de suas atividades;

VI. As senhas de acesso à rede de computadores e aos sistemas informatizados devem ser alteradas, à cada 75(setenta e cinco) dias;

VII. Fica proibido o compartilhamento de “login” para funções de administração de sistemas;

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

IX. As senhas deverão seguir os seguintes pré-requisitos:

- Tamanho mínimo de 08 (oito) caracteres;
- Existência de caracteres pertencentes a, pelo menos, três dos seguintes grupos: letras maiúsculas, letras minúsculas, números e caracteres especiais.

9. ACESSO À REDE

Art. 19° Todos os servidores, membros de conselhos e colaboradores (estagiários) estão autorizados e poderão fazer uso dos recursos da rede corporativa GDFNet dentro do domínio iprev.gdfnet.df, tais como:

I - Correio eletrônico (e-mail);
II - Internet, intranet;
III - compartilhamento e armazenamento de arquivos;
IV - Estações de trabalho;
V - Softwares e sistemas de informação; e
VI – Serviços de impressão.

Art. 20° Os servidores, membros de conselho e colaboradores terão acesso unicamente e exclusivamente àqueles recursos da rede corporativa GDFnet que lhe forem indispensáveis à realização de suas atividades.

Art. 21° Os serviços e sistemas autenticados serão disponibilizados para os usuários registrados e identificados pelo seu login e senha.

Art. 22° Cada unidade de lotação terá uma unidade de armazenamento em rede (p:) para os usuários lotados na respectiva área de atuação, com acesso de leitura e gravação.

Art.23° Manter, obrigatoriamente, os dados críticos da sua Unidade Administrativa em compartilhamentos de rede disponibilizados pela área de TIC;

Art. 24°.A inclusão de acesso será realizada automaticamente quando houver novo usuário na unidade de lotação;

Art. 25° Sob nenhuma hipótese os servidores que utilizam os recursos de rede disponibilizados pelo Iprev/DF poderão utilizá-los para fazer o download ou distribuição de software pirateados, atividade considerada delituosa de acordo com a legislação nacional vigente;

Art. 26° É proibida a instalação de softwares ou sistemas nas estações de trabalho pelos usuários finais. Este procedimento só poderá ser realizado pela Gerência de suporte ao usuário e telecomunicação.

Art. 27° O Iprev/DF, disponibilizará o acesso à rede de internet sem fio (wi-fi) a seus visitantes e colaboradores, o ingresso a rede se dará mediante cadastro quando solicitado o acesso. A rede de internet sem fio (wi-fi) será segregada, garantido assim o isolamento da rede interna GDFnet.

10. ESTAÇÕES DE TRABALHO

Art. 28°: Constituem estações de trabalho os computadores e notebooks registrados como patrimônio do Iprev/DF, e utilizados pelos servidores no desempenho de suas atividades funcionais. Assim recomendamos algumas medidas de segurança que devem ser adotadas quanto à utilização das estações de trabalho:

I. Não sejam instalados softwares sem a autorização;

II. Só sejam utilizados softwares devidamente licenciados;

III. A utilização de software não licenciado ou considerado "pirata" constitui infração prevista na Lei no 9.609/1998 (http://www.planalto.gov.br/ccivil_03/Leis/L9609.htm);

IV. Fica proibido remover ou modificar qualquer software, ou hardware sem a autorização da área de Tecnologia do Iprev/DF, pois, tal atitude pode comprometer a segurança e o desempenho da estação de trabalho;

V. Ao se ausentar da estação de trabalho, efetue o bloqueio ou "logoff" da mesma, evitando assim os acessos indevidos de outra pessoa a estação de trabalho através do seu usuário (login);

VI. A liberação do dispositivo móvel (notebook) será permitida após os solicitantes assinarem o acordo de conhecimento das suas responsabilidades (quanto a proteção física, atualização do software, entre outros), renunciando direitos autorais dos dados, que permita a exclusão remota dos dados pela Iprev/DF;

VII. Em caso de furto/roubo ou perda do dispositivo móvel, o servidor deverá comunicar imediatamente as autoridades policiais registrando, assim um boletim de ocorrência e deverá ainda comunicar a equipe de TI do Iprev/DF;

VIII. Utilização da estação somente para fins profissionais.

11. EQUIPAMENTOS PARTICULARES E DISPOSITIVOS MÓVEIS

Art. 29°: Ficam estabelecidas as seguintes regras para o uso de equipamentos particulares e de dispositivos moveis no âmbito do Iprev/DF:

I. A liberação para utilização de notebooks e para acesso à internet do Iprev/DF se dará mediante solicitação justificada e assinatura do termo de compromisso, vide anexo I;

II. O uso de notebooks particulares para fins de acesso à rede de Internet do Iprev/DF, será realizado pela Gerência de Suporte ao Usuário e Telecomunicações do Iprev/DF, mediante a verificação se tal equipamento possui proteção apropriada para uso autorizado.

III. Sob hipótese alguma poderão ser executados nos notebooks, software de característica maliciosa, que visam comprometer o funcionamento da rede;

IV. É de responsabilidade do proprietário usar somente software legalizados em seu notebook.;

V. É proibido o armazenamento de informações de proprietárias do Iprev/DF;

VI. Todos os arquivos que pertençam ao Iprev/DF não poderão ser armazenados no disco rígido do notebook e/ou em dispositivos de armazenamento móvel, como exemplo: pendrive e/ou armazenamento em nuvem pessoal;

VII. É proibida a inclusão de smartphones na rede corporativa GDFnet, a inclusão desses equipamentos se dará conforme o art. 27° desta política.

12. HOME OFFICE/TELETRABALHO

Art. 30°: A execução do teletrabalho ou home office se dará nos termos e orientações estabelecidos no decreto nº 42.462 de 30 de agosto de 2021.

13. E-MAIL CORPORATIVO

Art. 31°: O serviço de correio eletrônico (e-mail corporativo) é permitido somente para as atividades profissionais de seus usuários, não sendo permitido enviar ou arquivar mensagens que não estejam relacionadas as atividades deste Iprev/DF, e que contenham:

I. Assuntos que provoquem assédio, perturbação a outras pessoas ou que prejudiquem a imagem do Iprev/DF;

II. Temas difamatórios, discriminatórios, calunioso, degradante, ofensivo, violento, ameaçador, material obsceno, material pornográfico, ilegal ou antiético;

III. Fotos, imagens, sons ou vídeos que não tenham relação com as atividades profissionais do Iprev/DF;

IV. Compartilhar arquivos com códigos executáveis (.exe, .cmd, .pif, .js, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que possa apresentar risco a segurança da informação do Iprev/DF;

14. GESTÃO DE CONTAS DE USUÁRIOS

Art. 32° Todas as contas de usuários e senhas, estão armazenadas num servidor controlador de domínio (Active Directory), alocado fisicamente na Subsecretaria da Tecnologia da Informação e Comunicação – SUTIC/DF, o gerenciamento das contas de usuários e senhas do domínio iprev.gdfnet.df, pela Gerência de Redes e Monitoramento do Iprev/DF.

Art. 33° Poderá desfrutar de acesso à rede corporativa GDFnet, o servidor que obtiver a sua nomeação publicada no Diário Oficial do Distrito Federal, e os membros de conselhos e colaboradores que obtiverem contratos vigentes com Iprev/DF.

15. BACK-UP

Art. 34° Backup e restore são cópias de segurança, tendo por objetivo que os usuários se resguardem de uma ocasional perda de arquivos originais, seja por ações mau funcionamento dos sistemas ou ainda despropositadas pelo próprio usuário, permitindo assim a restauração das informações ou dados eventualmente perdidos. Desta forma o Iprev/DF, segue as orientações estabelecidas no Decreto nº 40.015, de 14 de agosto de 2019.

16. GESTÃO DE MUDANÇAS

Art. 35° Todas as mudanças devem ser constituídas, no mínimo, pelas fases de identificação, registro, planejamento, teste preliminar, aprovação, implementação e verificação dos potenciais impactos das mesmas por tanto:

I. Toda e qualquer proposta de mudança deve ser aprovada formalmente pela alta gestão juntamente com a equipe técnica competente;

II. Toda mudança realizada no Iprev/DF deverá ser devidamente comunicada à todas as partes interessadas;

III. Deverá ser amplamente divulgada, visando a redução de eventuais resistências e dificuldades de implementação das mesmas;

IV. Toda mudança, antes de ser implementada, deve contar com um plano de recuperação emergencial, incluindo procedimentos e responsabilidades para interrupção e recuperação, em caso de insucesso ou na ocorrência de eventos inesperados.

17. PRIVACIDADE

Art. 36° A privacidade está diretamente ligada com a classificação das informações a privacidade e proteção das informações devem ser asseguradas conforme requerido em legislação e regulamentação pertinente, quando aplicável:

I. Qualquer informação pessoal, mensagem eletrônica ou arquivo de computador só poderá ser acessada com a permissão do remetente, destinatário ou dono da mensagem ou arquivo, salvo por ordem judicial;

II. É determinantemente proibida a divulgação de informações institucionais do Iprev/DF sem a previa ciência e anuência da alta gestão;

III. Toda e qualquer divulgação de dados de funcionários, aposentados ou pensionistas é determinantemente proibida, salvo em casos em que a identificação do indivíduo seja excluída.

18. CRIPTOGRAFIA

Art. 37° A criptografia objetiva a proteção da confidencialidade, autenticidade e a integridade da informação. Nesse quesito orienta-se:

I. Os controles criptográficos serão utilizados para assegurar confidencialidade, a integridade e a autenticidade de informações confidenciais e restritas que se encontrem armazenadas ou sob processo de transporte físico ou de transmissão eletrônica;

II.O não-repúdio vira a provar a ocorrência de um evento ou ação alegados e suas entidades originárias, de forma a resolver disputas sobre a ocorrência ou não ocorrência do evento ou ação e do envolvimento das entidades no evento;

III. A autenticação: confirmar a identidade de usuários ou de sistemas automatizados;

Parágrafo único: A utilização de um sistema de gerenciamento de chaves criptográficas e baseado em procedimentos, normas e métodos seguros o qual realize minimamente as seguintes funcionalidades:

- Geração de chaves para diferentes sistemas criptográficos e diferentes aplicações;
- Geração e obtenção de certificados de chaves públicas;
- Distribuição de chaves para os usuários devidos, incluindo a forma como as chaves são ativadas, quando recebidas;
- Armazenamento de chaves, incluindo a forma como os usuários autorizados obtêm acesso a elas;
- Mudança ou atualização de chaves, incluindo regras quando as chaves são mudadas e como isto deve ser conduzido;
- Desativação e destruição de chaves;
- Recuperação de chaves perdidas ou corrompidas;
- Geração de cópias de segurança ou guardar as chaves;
- Manutenção de registro e auditoria das atividades relacionadas com o gerenciamento de chaves;

19. GESTÃO DE INCIDENTES

Art. 41° A continuidade da segurança da informação em situações adversas, e baseada no gerenciamento continuo e normal dos negócios ou na análise do impacto ao negócio no gerenciamento da recuperação de um possível desastre.

Parágrafo único: Planejar e assegurando a continuidade da segurança da informação:

I. O Iprev/DF deve avaliar se a continuidade da segurança da informação está contida dentro do processo de gestão da continuidade do negócio ou no processo de gestão de recuperação de desastre fatores determinantes do planejamento para continuidade do negócio e da recuperação de desastre;

II. Deve-se estabelecer, documentar, implementar e manter os processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação, durante uma situação adversa.

III. Os controles de segurança da informação devem continuar e operar durante uma condição de situação adversa. Se os controles de segurança não são capazes de manter a informação segura, recomenda-se que outros controles sejam estabelecidos, implementados e mantidos para garantir um nível aceitável da segurança da informação.

IV. A estrutura de gerenciamento adequada deverá estar implementada para mitigar e responder a um evento de interrupção, usando pessoal com a necessária autoridade, experiência e competência.

V. O Iprev/DF deve verificar os controles de continuidade da segurança da informação, estabelecidos e implementados, a intervalos regulares, para garantir que eles são válidos e eficazes em situações adversas.

VI. Os recursos de processamento da informação devem ser implementados com redundância suficiente para atender aos requisitos de disponibilidade.

VII. O Iprev/DF deve identificar os requisitos do negócio quanto à disponibilidade de sistemas de informação. Quando a disponibilidade não puder ser assegurada usando a arquitetura de sistemas existentes, componentes redundantes ou arquiteturas sejam considerados.

20. CONTINUIDADE DA SEGURANÇA DA INFORMAÇÃO

Art. 38° Incidentes de Segurança da Informação são todos e quaisquer eventos adversos, sob suspeita ou confirmados que possam comprometer as informações ou um ativo de informação ou serviços, que tem sua integridade, confidencialidade ou disponibilidade comprometida. Como incidentes de segurança, podemos citar:

I. mau funcionamento de sistemas ou serviços;

II. ataques (como os de engenharia social ou de negação de serviço);

III. acesso não autorizado;

IV. envio ou recebimento de códigos maliciosos;

V. alterações em um sistema sem a aprovação do proprietário e perda;

VI. extravio ou roubo de dados ou equipamentos que contenham informações críticas.

Art. 39° Toda e qualquer ação que for contra a Política de Segurança da Informação do Iprev/DF, também deve ser tratada como um incidente de segurança.

Art. 40° As diretrizes para o gerenciamento de responsabilidades e procedimentos com relação à gestão de incidentes de segurança da informação devem ser consideradas:

I. Procedimentos para preparação e planejamento a respostas a incidentes.

II. Procedimentos de monitoramento, detecção, análise e notificação de incidentes e eventos de segurança da informação.

III. A avaliação e decisão dos eventos de segurança da informação e avaliação de fragilidades de segurança da informação;

IV. Ponto de contato para notificação e detecção de incidentes de segurança.

V. Relato de todos os detalhes (tipo de não conformidade ou violação, mau funcionamento, mensagens na tela, comportamento estranho) informa imediatamente; e não tomar nenhuma ação sozinho, porém notificar imediatamente ao ponto de contato, tomando apenas ações coordenadas.

VI. O mau funcionamento ou outro comportamento anômalo do sistema pode ser um indicador de um ataque de segurança ou violação na segurança atual e, portanto, convém que sempre seja reportado como um evento de incidente na segurança da informação.

21. PROTEÇÃO À PROPRIEDADE INTELECTUAL

Art. 42° Todos os procedimentos apropriados devem ser implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados com os direitos de propriedade intelectual, e sobre o uso de produtos de softwares. Incluído os direitos de propriedade intelectual os direitos autorais de software ou documento, direitos de projetos, marcas, patentes e licenças de código fonte.

Produtos de softwares proprietários são normalmente fornecidos sob um contrato de licenciamento que especifica os termos e condições da licença, como por exemplo, limitar o uso dos produtos em máquinas especificadas ou limitar a reprodução apenas para a criação de cópias de backup. É recomendado que a importância e a conscientização dos direitos de propriedade intelectual de software sejam comunicadas aos responsáveis pelo desenvolvimento de software na organização.

Requisitos legais, regulamentares e contratuais podem colocar restrições sobre a cópia de material proprietário. Em particular, eles podem exigir que apenas o material que é desenvolvido pela organização ou que está licenciado ou fornecido pelo desenvolvedor para a organização, pode ser utilizado. Violação de direitos autorais pode levar a ação judicial e pode envolver multas e processos criminais.

Parágrafo Único: Recomendado que as seguintes diretrizes sejam consideradas para proteger qualquer material que possa ser considerado como propriedade intelectual:

I. Divulgar uma política de conformidade com os direitos de propriedade intelectual que defina o uso legal de produtos de software e de informação;
II. Adquirir software somente por meio de fontes conhecidas e de reputação, para assegurar que o direito autoral não está sendo violado;
III. Manter conscientização das políticas para proteger os direitos de propriedade intelectual e notificar a intenção de tomar ações disciplinares contra pessoas que violarem essas políticas;
IV. Manter de forma adequada os registros de ativos, e identificar todos os ativos com requisitos para proteger os direitos de propriedade intelectual;
V. Manter provas e evidências da propriedade de licenças, discos-mestres, manuais etc.;
VI. Implementar controles para assegurar que o número máximo de usuários permitidos, dentro da licença concedida, não está excedido;
VII. Conduzir verificações para que somente produtos de software autorizados e licenciados sejam instalados;
VIII. Estabelecer uma política para a manutenção das condições adequadas de licenças;
IX. Estabelecer uma política para disposição ou transferência de software para outros;
X. Cumprir termos e condições para software e informação obtidos a partir de redes públicas;
XI. Não duplicar, converter para outro formato ou extrair de registros comerciais (filme, áudio) outros que não os permitidos pela lei de direito autoral;
XII. Não copiar no todo ou em partes, livros, artigos, relatórios ou outros documentos, além daqueles permitidos pela lei de direito autoral.

22. SENSIBILIZAÇÃO E TREINAMENTO PARA SEGURANÇA

Art. 43° Todos os servidores do Iprev/DF, deveram receber treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas, normas e procedimentos institucionais relevantes para a realização de suas funções.

Parágrafo Único: Recomenda-se que o treinamento e educação em segurança da informação deve contemplar aspectos gerais, como:

I. O comprometimento da alta gestão com a segurança da informação;

II. Tornar conhecido e estar em conformidade com as obrigações e regras de segurança da informação aplicáveis, conforme definido nas políticas, normas, leis, regulamentações, contratos e acordos.

III. Responsabilidade pessoal por seus próprios atos e omissões, e compromissos gerais para manter seguro ou para proteger a informação que pertença a organização e partes externas.

IV. O treinamento e a educação em segurança da informação devem ser realizados periodicamente. Treinamento e educação iniciais se aplicam aqueles que são transferidos para novas posições ou atribuições com requisitos de segurança da informação completamente diferentes, e não apenas para os novos iniciantes e deve ser realizado antes das pessoas assumirem os seus papéis, ou o mais rápido que possível.

V. Procedimentos de segurança da informação básicos (tais como, notificação de incidente de segurança da informação) e controles básicos (tais como, segurança da senha, controles contra códigos maliciosos e política de mesa limpa e tela limpa).

VI. A organização deve desenvolver o programa de treinamento e educação com o objetivo de conduzir a educação e treinamento de forma eficaz. O programa deve estar alinhado com as políticas e procedimentos relevantes de segurança da informação da organização, levando em consideração as informações da organização a serem protegidas e os controles que devem ser implementados para proteger a informação. Recomenda-se que o programa considere diferentes formas de educação e treinamento, tais como, leituras ou auto estudos.

23. ATUALIZAÇÃO

Art. 44° A Política de Segurança da Informação – diretrizes, normas e procedimentos, deverá ser revisada com intervalos planejados, não superiores a 2 (dois) anos, a partir de sua data de publicação, ou em caso de condições obrigatórias de atualização do documento, tais como:

I. Mudanças estratégicas do instituto;
II. Alteração ou edição de leis;
III. Expiração da validade da política de segurança;
IV. Mudanças de tecnologias.
V. A partir dos resultados das análises de risco que estabeleçam a necessidade de mudança da norma para readequação da instituição aos riscos (mitigação);

24. REFERÊNCIAS LEGAIS E NORMATIVAS

I. Lei Complementar n° 840, de 23.11.2011 - Dispõe sobre o regime jurídicos dos servidores públicos civis do Distrito Federal, das autarquias e das fundações públicas distritais;

II. Resolução n° 03, de 06.11.2018, Política de Segurança da Informação e Comunicação – POSIC- Distrito Federal;

III. Decreto Distrital nº 40.015, de 14.08.2019- Dispõe sobre a obrigatoriedade de elaboração e publicação dos Planos Diretores de Tecnologia da Informação e Comunicação e sobre a centralização e utilização da rede GDFNet, da infraestrutura do Centro de Tecnologia da Informação e Comunicação do Distrito Federal - CeTIC-DF e dos sistemas de informação no âmbito da Administração Direta e Indireta do Distrito Federal, e dá outras providências.

IV. Decreto Distrital nº 35.382, de 29.04.2014 - Regulamenta o art. 42, da Lei nº 4.990, de 12.12.2012, dispõe sobre os procedimentos para credenciamento de segurança, sobre o Núcleo de Segurança e Credenciamento, institui o Comitê Gestor de Credenciamento de Segurança, e dá outras providências;

V. Decreto Distrital nº 37.574 de 26.08.2016 – Aprova a Estratégia Geral de Tecnologia da Informação – EGTI;

VI. Lei nº 13.709, de 14.08.2018- Lei Geral de Proteção de Dados – LGPD;

VII. Lei Distrital nº 4.990, de 12.12.2012 - Regula o acesso a informações no Distrito Federal previsto no art. 5º, XXXIII, no art. 37, § 3º, II, e no art. 216, § 2º, da Constituição Federal e nos termos do art. 45, da Lei federal nº 12.527, de 18.11.2011, e dá outras providências;

VIII. Lei Federal nº 12.965, de 23.04.2014 - Estabelece princípios, garantias, direitos e deveres para uso da Internet no Brasil;

IX. Lei Federal nº 12.737, de 30.11.2012 - Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7.12.1940 - Código Penal; e dá outras providências;

X. ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança da Informação – Sistemas de Gestão de Segurança de TIC;

XI. ABNT NBR ISO/IEC 27002:2013 - Tecnologia da Informação — Técnicas de Segurança;

XII. ABNT NBR ISO/IEC 22313:2020 – Sistema de Gestão de Continuidade de Negócios;

25. ANEXO I

TERMO DE COMPROMISSO PARA UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS

Nome do Solicitante:	
Lotação:	Cargo:
Matrícula:	Ramal:
Descrição do equipamento a ser liberado (notebook/computador,marca):	
Número de patrimônio:	
Descrição do dispositivo móvel:	
Motivo do uso do dispositivo móvel:	
Observações:	

Nome do responsável pelo dispositivo
Cargo

Nome do chefe imediato
Cargo

IPREV DF

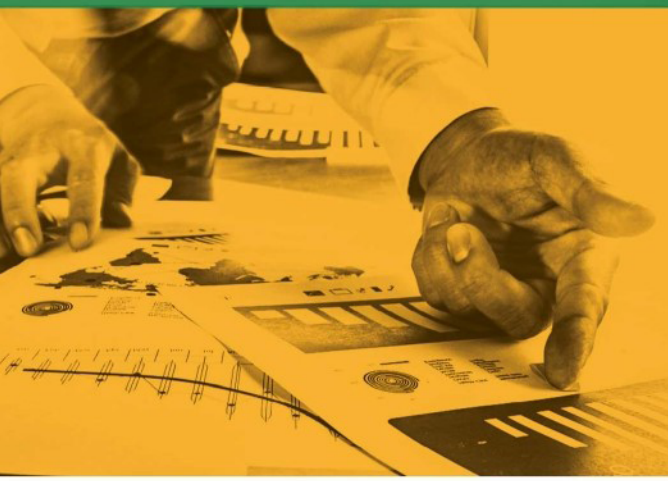
INSTITUTO DE **PREVIDÊNCIA DOS SERVIDORES** DO DISTRITO FEDERAL

VISÃO

Ser reconhecido, por beneficiários e contribuintes, pela excelência na gestão previdenciária no Distrito Federal.

VALORES

Integridade, confiabilidade, sustentabilidade e transparência.



MISSÃO

Trabalhar para a construção de um futuro previdenciário seguro a seus beneficiários, com o menor impacto possível aos contribuintes.

Conheça mais em
www.iprev.df.gov.br

GDF
É tempo de ação.