Instituto de Previdência dos
Servidores do Distrito Federal

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

2025 Brasília - DF

Expediente

Governadora do Distrito Federal
Ibaneis Rocha

Vice-Governadora do Distrito Federal
Celina Leão Hizim Ferreira

Diretora-presidente do Iprev-DF
Raquel Galvão Rodrigues da Silva

Diretora de Governança, Projetos e Compliance
Sylvia Neves Alves

Diretora de Administração e Finanças
Célia Maria Ribeiro de Sales

Diretor de Previdência
Paulo Henrique de Sousa Ferreira

Diretor Jurídico
Luiz Gustavo Barreira Muglia

Diretor de Investimentos
Thiago Mendes Rodrigues

Controladoria
Márcio Eduardo de Moura Aquino

Unidade de Atuária
Jucelina Santana da Silva

Unidade de Comunicação Social
Jucélio Duarte Ponciano

Diagramação
Unidade de Comunicação Social

SUMÁRIO

INTRODUÇÃO

A informação é um recurso vital para o funcionamento de qualquer organização, sendo um dos seus ativos mais valiosos. Para garantir sua integridade, confidencialidade e disponibilidade, é necessário estabelecer diretrizes, normas e procedimentos adequados, a fim de se evitar sua exposição a ameaças que exploram vulnerabilidades do sistema e, no caso de violação da segurança, ser possível agir para corrigir a falha, recuperar os dados e disponibilizá-los em sua total integridade aos usuários finais.

O Instituto de Previdência dos Servidores do Distrito Federal – Iprev-DF, instituído como órgão gestor único do Regime Próprio de Previdência Social do Distrito Federal, nos termos da Lei Complementar nº 769, de 30 de junho de 2008, lida com um elevado volume de dados sensíveis, como informações pessoais de servidores e pensionistas e movimentações financeiras. Nesse contexto, a adoção de uma Política de Segurança da Informação é fundamental para proteger esses dados, reduzir os riscos de perdas, fraudes e acessos não autorizados, garantindo conformidade legal, continuidade do negócio, eficiência operacional, assim como o reforço da confiança e credibilidade do Instituto de Previdência, demonstrando, assim, compromisso com a segurança e proteção das informações dos segurados.

OBJETIVO

A Política de Segurança da Informação do Iprev-DF tem por objetivo principal a proteção dos ativos de informação contra ameaças, garantindo a confidencialidade, integridade e disponibilidade das informações, a partir do estabelecimento de diretrizes e procedimentos, uso seguro das informações e conformidade com a legislação aplicável.

ABRANGÊNCIA

Estão submetidos à Política de Segurança da Informação do Iprev-DF todos os servidores, estagiários, prestadores de serviços e demais agentes públicos ou privados que tenham qualquer tipo de acesso aos dados ou informações produzidas, armazenados ou acessadas, no âmbito do Instituto de Previdência, sob pena de responsabilidade em caso de posse, armazenamento ou divulgação indevida.

Os recursos de Tecnologia da Informação e Comunicação - TIC disponibilizados pelo Iprev-DF aos usuários devem ser utilizados em atividades estritamente relacionadas às funções institucionais desempenhadas pela autarquia, sendo vedada a utilização de quaisquer desses recursos para a prática de atos ilegais contra outros recursos da rede de computadores do Iprev-DF ou redes externas.

Toda e qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada nos sistemas de informação do Iprev-DF compõe o seu rol de ativos de informação e deve ser protegida conforme normas em vigor.

PRINCÍPIOS

São princípios que regem a Política de Segurança da Informação e Comunicação do Iprev-DF:

I. A garantia da inviolabilidade da intimidade, da honra e da imagem;
II. A proteção dos dados e informações produzidas, armazenadas e acessadas no Iprev-DF;
III. O respeito à privacidade.

CLASSIFICAÇÃO DAS INFORMAÇÕES

As informações são classificadas com base em sua sensibilidade, valor e impacto, em caso de comprometimento, nas seguintes categorias:

- **Pública:** Informações que podem ser divulgadas sem restrições, pois não causam danos ao Iprev-DF, servidores ou beneficiários;
- **Interna :** Informações de uso restrito aos servidores do Iprev-DF, mas que não apresentam risco significativo se expostas;
- **Restrita:** Dados acessíveis apenas a servidores previamente definidos, sempre associados aos interesses estratégicos do Iprev-DF;
- **Confidencial:** Dados que devem ser acessados apenas por pessoas autorizadas, podendo causar impacto negativo se expostos; e
- **Sigilosa:** Informações altamente sensíveis que, se divulgadas, poderiam comprometer seriamente a operação ou a reputação do Iprev-DF.

CRITÉRIOS PARA CLASSIFICAÇÃO

» Impacto em caso de comprometimento

- **Baixo:** Vazamento ou acesso indevido teria impacto mínimo sobre a organização, como pequenos atrasos ou retrabalho;
- **Moderado:** Poderia resultar em danos operacionais, financeiros ou legais moderados;
- **Alto:** Exposição causaria grandes prejuízos, como perda de confiança, interrupção de serviços críticos ou sanções significativas; e
- **Crítico:** A divulgação poderia ter efeitos devastadores, incluindo danos à continuidade do negócio ou à segurança de terceiros.

» Necessidade de compartilhamento

- **Necessidade de saber:** Acesso restrito apenas a colaboradores ou terceiros que precisam dessas informações para executar suas funções;
- **Confiança:** Nível de confiança e autorização necessária para acessar a informação (pessoas ou entidades); e
- **Ciclo de vida:** Critério baseado em quanto tempo a informação deve permanecer acessível ou restrita. Informações podem ser reclassificadas ao longo do tempo.

» Valor da informação

- **Valor operacional:** Informações que são vitais para o funcionamento diário da organização;
- **Valor estratégico:** Informações cruciais para a tomada de decisões estratégicas; e
- **Valor legal:** Dados que devem ser preservados por motivos regulatórios ou jurídicos, como contratos, relatórios fiscais ou informações pessoais protegidas por lei (LGPD).

» Legalidade e regulamentação

Informações protegidas por regulamentações legais, como a Lei Geral de Proteção de Dados (LGPD), que exige proteção e controle rigoroso de dados pessoais; e

Cumprimento de normas setoriais (financeiro, saúde, previdência), que impõem critérios rígidos de segurança e retenção de dados.

» Confidencialidade

Nível de restrição e sigilo necessário para proteger a informação.

» Integridade

Garantia de que os dados não sejam alterados ou corrompidos.

» Disponibilidade

Necessidade de manter os dados acessíveis e utilizáveis quando necessários pelos usuários autorizados.

» Origem e propriedade dos dados

- **Dados pessoais:** Requerem níveis mais altos de proteção devido à LGPD;
- **Dados institucionais:** Informações geradas pela instituição que precisam ser classificadas de acordo com seu valor interno e estratégico; e
- **Dados de terceiros:** Informações fornecidas por parceiros ou clientes que exigem tratamento especial devido a contratos ou legislações específicas.

» Probabilidade de uso indevido ou vazamento

Avaliar o risco das informações serem utilizadas de forma indevida ou vazarem, considerando fatores como acessibilidade, relevância para terceiros e vulnerabilidades.

» Potencial de repercussão

- **Reputacional:** Impacto que o vazamento ou uso indevido poderia causar à imagem pública da organização;
- **Financeiro:** Perdas financeiras diretas ou indiretas; e
- **Operacional:** Impactos sobre a continuidade dos serviços e processos operacionais.

SEGURANÇA FÍSICA

A segurança física é uma parte crucial da política de segurança da informação, pois visa proteger os ativos de tecnologia e dados contra ameaças físicas. No contexto do Iprev-DF, a segurança física pode ser abordada em vários aspectos, incluindo proteção contra acesso não autorizado, desastres naturais e outras formas de danos físicos.

» Controle de Acesso Físico

- **Restrição de acesso:** Acesso a áreas sensíveis, como salas de servidores, centros de dados e estações de trabalho críticas, deve ser restrito apenas a pessoal autorizado. O uso de sistemas de controle de acesso, como cartões magnéticos, biometria ou senhas, é essencial para garantir que apenas pessoas autorizadas entrem nessas áreas;

- **Monitoramento e vigilância:** Instalação de câmeras de segurança (CFTV) para monitoramento contínuo das áreas sensíveis. As imagens devem ser armazenadas de forma segura e acessíveis apenas por pessoal autorizado; e

- **Registro de acesso**: Manter um registro de todas as entradas e saídas de áreas restritas, com informações detalhadas sobre o horário e a pessoa que acessou, para fins de auditoria.

» Proteção contra incêndios e desastres

- **Sistemas de prevenção e combate a incêndios:** Instalação de alarmes de incêndio, detectores de fumaça e sistemas de supressão de fogo (como sprinklers ou agentes químicos) nas áreas onde os ativos de TI estão localizados;

- **Planos de evacuação:** Implementação de planos de evacuação de emergência claramente comunicados e periodicamente testados para garantir a segurança de pessoas e equipamentos; e

- **Proteção contra desastres naturais:** Garantir que a infraestrutura crítica esteja protegida de tempestades elétricas e outros desastres naturais.

» **Segurança de equipamentos**

- **Instalação e posicionamento seguro de equipamentos:** Todos os ativos de rede devem ser instalados em locais protegidos, preferencialmente em racks ou armários trancados, para evitar acessos ou movimentações não autorizadas; e

- **Proteção contra roubo e vandalismo:** Implementação de medidas que previnam o roubo de equipamentos, como fixação física de dispositivos e uso de alarmes de segurança em áreas críticas.

» Segurança no uso de dispositivos pessoais

- **Política de uso de dispositivos:** Definição clara das regras para uso de dispositivos móveis e laptops dentro do ambiente do Iprev-DF. Isso inclui restrições de acesso a áreas sensíveis e procedimentos para conexão de dispositivos a redes corporativas; e

- **Segurança no transporte:** Equipamentos que precisam ser transportados, como laptops ou discos rígidos, devem ser armazenados em malas ou bolsas seguras.

» Ambientes Controlados

- **Ambientes com climatização:** As salas de servidores e centros de dados devem ser equipadas com sistemas de climatização controlada para evitar o superaquecimento dos equipamentos; e

- **Geradores e No-Breaks:** Garantem a continuidade dos serviços de TIC evitando a perda de dados em caso de quedas de energia.

» Gestão de visitantes

- **Autorização para Acesso:** Visitantes que necessitem acessar áreas com equipamentos críticos devem ser acompanhados por pessoal autorizado e seus acessos devidamente registrados; e

- **Procedimentos de Verificação:** Implementar procedimentos de verificação de identidade e de restrição de objetos permitidos nas áreas sensíveis.

» Backup e recuperação

- **Armazenamento de Backups Físicos:** Garantir que os backups sejam armazenados em locais físicos seguros e, de preferência, fora do local de operação principal para proteção contra desastres locais; e

- **Plano de recuperação de desastres:** Desenvolvimento de um plano de recuperação que garanta a continuidade dos serviços do Iprev-DF em caso de comprometimento físico dos ativos.

POLÍTICA DE SENHAS

A política de senhas é um componente fundamental da política de segurança da informação, pois define diretrizes para a criação, gerenciamento e proteção de senhas no ambiente de TIC. Essas diretrizes são essenciais para proteger o acesso a sistemas, dados e informações sensíveis.

A senha é uma credencial pessoal e intransferível, garantindo ao usuário identidade única para acesso à rede e aos recursos de TIC, além de protegê-lo de possíveis fraudes ou acessos indevidos. O uso de dispositivos ou senhas pertencentes a terceiros configura crime de falsa identidade, conforme previsto no art. 307 do Código Penal Brasileiro.

Com o objetivo de orientar a criação de senhas seguras, ficam estabelecidas as seguintes regras:

a) 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;

b) A senha inicial será fornecida pela unidade gestora de TIC, via e-mail institucional, no ato da posse do servidor, a partir de provocação pela unidade de Gestão de Pessoas do Iprev-DF. O servidor empossado será informado sobre suas credenciais e forma de acesso;

c) As credenciais não poderão ser fornecidas por telefone, aplicativos mensageiros ou outra forma que não assegure a identidade do servidor;

d) É obrigatório aos servidores zelarem pela confidencialidade de sua senha de acesso, podendo serem responsabilizados pelas operações realizadas com a utilização de suas credenciais;

e) 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;

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

g) A reutilização de senhas antigas deve ser proibida, devendo os usuários criarem novas senhas sempre que necessário;

h) Fica proibido o compartilhamento de credenciais para funções de administração de sistemas;

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

j) As senhas deverão seguir os seguintes pré-requisitos de complexidade:

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

POLÍTICA DE ACESSO À REDE

Todos os servidores, membros de conselhos e estagiários estão autorizados e poderão fazer uso dos recursos da rede corporativa GDFNet, 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.

Pessoas e sistemas terão acesso única e exclusivamente àqueles recursos da rede corporativa GDFnet que lhe forem indispensáveis à realização de suas atividades, com o menor privilégio de acesso possível.

Os serviços e sistemas serão disponibilizados aos usuários registrados no domínio iprev.gdfnet.df e identificados pelo seu **login e senha.**

A cada unidade administrativa do Iprev-DF será disponibilizado um diretório em rede para o armazenamento de arquivos, sendo obrigatória a utilização desses para o arquivamento de dados críticos.

O acesso a esses repositórios será concedido pelo setor de TIC, mediante solicitação do responsável hierárquico da respectiva unidade administrativa.

O uso dos recursos tecnológicos do Iprev-DF é estritamente destinado à realização das atividades institucionais, em conformidade com princípios éticos, profissionais e legais.

GESTÃO DAS ESTAÇÕES DE TRABALHO

Estações de trabalho referem-se a terminais físicos, como desktops ou laptops, fornecidos pelo Iprev-DF, conectados à rede corporativa, permitindo que os usuários acessem sistemas e recursos compartilhados como servidores e impressoras. Elas podem ser personalizadas com softwares e configurações específicas para atender às necessidades de cada colaborador ou função dentro da organização.

Para uma boa gestão das estações de trabalho, devem ser observadas algumas medidas de segurança:

I. Utilização das estações de trabalhado ser dará apenas para fins institucionais;

II. A instalação de softwares só será realizada após avaliação do setor de TIC;

III. Os softwares deverão ser devidamente licenciados;

IV. Fica proibido remover ou modificar qualquer software ou hardware sem a autorização da área de Tecnologia do Iprev-DF, a fim de se evitar o comprometimento da segurança e o desempenho da estação de trabalho;

V. A instalação de softwares e o acesso às configurações críticas dos equipamentos deverá ser restringido, sendo realizado apenas por pessoal do corpo técnico mediante credenciais de administrador do sistema;

VI. A estação de trabalho deverá ser bloqueada sempre que o servidor se ausentar do seu posto, evitando assim acessos indevidos;

VII. A movimentação de qualquer equipamento de informática deverá ser realizada pelo setor de TIC;

VIII. A utilização de dispositivos de armazenamento removíveis deve ser evitada, a fim de se reduzir o risco de infecção por softwares maliciosos, perda de dados e violação da privacidade, além de comprometer a realização de auditorias;

IX. O fornecimento de laptops será condicionado à assinatura de termo de responsabilidade, pelo qual o servidor se comprometa seguir as diretrizes de segurança estabelecidas pelo Iprev-DF em relação ao uso desse tipo de equipamento, tais como proteção física, restrição para a instalação de softwares, utilização de redes de internet seguras e garantira do sigilo dos dados; e

X. Em caso de furto/roubo ou perda do dispositivo móvel, o servidor deverá registrar ocorrência policial e encaminhar cópia, via sistema SEI, ao setor de TIC.

A utilização de software não licenciado constitui uma infração grave, que pode gerar consequências legais e financeiras tanto para o servidor quanto para a instituição. De acordo com a Lei de Direitos Autorais (Lei nº 9.610/1998) e a Lei de Propriedade Industrial (Lei nº 9.279/1996), a reprodução, distribuição ou uso de softwares sem a devida licença de seus proprietários é ilegal e passível de penalidades, incluindo multas e responsabilidade criminal. Além disso, o uso de software não licenciado compromete a segurança da informação, pois versões não autorizadas frequentemente contêm vulnerabilidades que podem expor a rede institucional a ameaças cibernéticas, como malware, ransomware e roubo de dados.

UTILIZAÇÃO DE EQUIPAMENTOS PARTICULARES E DISPOSITIVOS MÓVEIS

O uso de equipamentos particulares e dispositivos móveis no ambiente do Iprev-DF, como notebooks, tablets ou computadores pessoais, deverá seguir as seguintes diretrizes e boas praticas, a fim de se garantir a proteção de dados sensíveis:

- **Autorização Prévia:** O uso de equipamentos particulares para acessar a rede ou sistemas do Iprev-DF deverá ser previamente autorizado pela área de Tecnologia da Informação.

- **Conexão à rede:** Equipamentos pessoais não devem ser conectados diretamente à rede GDFnet, exceto em casos expressamente permitidos pela área de TI e com medidas de segurança apropriadas. Para os visitantes, o acesso à internet deve ser feito exclusivamente pela rede Wi-Fi.

- **Políticas de segurança:** Os dispositivos particulares autorizados a acessar a rede GDFnet deverão atender aos requisitos mínimos de segurança:

    a. Antivírus atualizado;
    b. Criptografia de dados;
    c. Senhas ou biometria para desbloqueio;
    d. Utilização de softwares licenciados; e
    e. Atualizações recentes do sistema operacional e softwares.

- **Acesso a dados sensíveis:** Não é permitido o armazenamento de dados sensíveis ou confidenciais do Iprev-DF em dispositivos pessoais, a menos que exista uma justificativa aprovada pela gestão e medidas de segurança adequadas.

- **Responsabilidade:** Os servidores e colaboradores que utilizarem dispositivos particulares para acessar a rede e sistemas do Iprev-DF são responsáveis por garantir a segurança física e lógica de seus equipamentos. Qualquer incidente de segurança envolvendo o uso desses dispositivos deverá ser comunicado imediatamente à área de TI.

- **Sanções:** O uso inadequado de dispositivos móveis e equipamentos particulares que comprometa a segurança da informação do Iprev-DF pode resultar em advertências, sanções disciplinares ou, em casos mais graves, responsabilidade criminal e civil.

GESTÃO DO TELETRABALHO E DO ACESSO REMOTO

Em 2023, o teletrabalho no âmbito do Governo do Distrito Federal foi revogado por meio do Decreto nº 44.265/2023, o qual determinou o retorno presencial dos servidores. Esse decreto revogou os Decretos nº 41.841/2021 e nº 42.462/2022, que tratavam do teletrabalho em caráter excepcional e provisório devido à pandemia de COVID-19.

À época, o Órgão gestor da rede de dados governamental implementou uma rede virtual privada (VPN) para que os servidores que se encontravam em teletrabalho pudessem acessar a rede GDFnet e assim utilizar sistemas governamentais que não são disponíveis na rede pública de internet.

Mesmo com a revogação do teletrabalho, ainda existe a possibilidade dos servidores acessarem remotamente os computadores do Instituto de Previdência e demais sistemas cujo acesso só é possível a partir da rede GDFNet.

Dessa forma, os acessos remotos se darão observando as seguintes normas e diretrizes:

- Os pedidos de acesso remoto serão direcionados ao setor de TIC pela chefia imediata do servidor interessado;

- O acesso aos sistemas de informações, incluindo a infraestrutura de tecnologia da informação se dará somente por necessidade do serviço, sendo observados os procedimentos, normas e disposições contidas na legislação que rege os acessos a estes ativos de tecnologia da informação;

- Não revelar fato ou informação de qualquer natureza de que se tenha conhecimento, salvo em decorrência de decisão competente na esfera judicial, bem como de autoridade superior;

- Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

- Durante as ausências da estação de trabalho, a sessão de uso do sistema deverá ser encerrada, garantindo assim a impossibilidade de acesso indevido por terceiros;

- As senhas de acesso não poderão ser reveladas a terceiros;

- O acesso remoto (VPN) não poderá ser utilizado para acessar sistemas e serviços de governo que já estão publicados na internet, tais como SEI, SIGRHWEB, portais e sites institucionais. Esse recurso será somente para acesso aos sistemas e serviços restritos e internos ao Governo do Distrito Federal;

- A estação de trabalho ou qualquer dispositivo utilizado para acesso remoto deverá possuir, no mínimo, a versão atualizada e habilitada de sistema operacional, antivírus e firewall; e

- Os computadores a serem utilizados para o acesso remoto deverão ser previamente informados ao setor de TIC, sendo vedada a utilização de redes desconhecidas, abertas (sem senhas de acesso), públicas (aeroportos, restaurantes, shoppings, lan houses, etc.), ficando o servidor sujeito ao bloqueio definitivo de seu acesso em caso de descumprimento e também às sanções e penalidades cabíveis, caso a ação desencadeie algum incidente de segurança cibernética que comprometa o ambiente corporativo.

Constitui descumprimento de normas legais, regulamentares e quebra de sigilo funcional divulgar dados obtidos dos sistemas de informação e na infraestrutura de tecnologia da informação, aos quais tenha acesso, para terceiros não envolvidos nas atividades executadas.

GESTÃO DO E-MAIL CORPORATIVO

O e-mail corporativo do Iprev-DF é uma ferramenta essencial de comunicação e deve ser utilizado exclusivamente para fins profissionais, de acordo com as políticas institucionais. As seguintes diretrizes devem ser observadas para garantir o uso correto e seguro do serviço:

- • **Finalidade profissional:** O e-mail corporativo deve ser utilizado apenas para a comunicação de assuntos relacionados às atividades e responsabilidades do Iprev-DF, o uso para fins pessoais, recreativos ou que não estejam diretamente ligados às funções desempenhadas pelo Instituto é proibido;
-
- • **Conteúdos proibidos:** Não é permitido enviar ou armazenar mensagens que contenham materiais que possam prejudicar a imagem do Iprev-DF ou que estejam em desacordo com as normas de conduta ética, incluindo:

    - » Assédio, perturbação ou intimidação de outros usuários;
    - » Conteúdos difamatórios, discriminatórios, ofensivos, caluniosos, violentos ou ameaçadores; e
    - » Material ilegal, obsceno, pornográfico ou antiético.

- • **Anexos perigosos:** É proibido o envio ou compartilhamento de arquivos com extensões que possam comprometer a segurança dos sistemas, como executáveis (.exe), scripts (.js), ou arquivos com potencial para executar código malicioso. Estes tipos de arquivos podem representar riscos à integridade da informação e à infraestrutura tecnológica da instituição;
-
- • **Sigilo e confidencialidade:** Os usuários devem manter a confidencialidade das informações enviadas e recebidas através do e-mail corporativo, garantindo que dados sensíveis e informações restritas sejam compartilhadas somente com os destinatários autorizados. É essencial evitar o uso do e-mail corporativo para o envio de informações críticas ou confidenciais sem as devidas medidas de segurança;
-
- • **Monitoramento e auditoria:** O Iprev-DF se reserva o direito de monitorar e auditar o uso do e-mail corporativo, a fim de assegurar o cumprimento das políticas de segurança da informação e das normas institucionais. O uso indevido ou comportamento que viole as diretrizes estabelecidas poderá resultar em sanções disciplinares, conforme as regulamentações internas; e
-
- • **Boas práticas de segurança:** Evitar abrir anexos ou clicar em links de remetentes desconhecidos ou suspeitos, a fim de prevenir ataques e infecções por malware. Manter senhas seguras e confidenciais, nunca compartilhando suas credenciais de acesso ao e-mail corporativo.

GESTÃO DE CONTAS DE USUÁRIOS

Todas as contas de usuários e senhas, estão armazenadas no servidor controlador de domínio iprev.gdfnet.df (Active Directory), sendo gerenciado pela unidade de tecnologia da informação.

A criação das contas de usuários para acesso à rede corporativa GDFnet se dará a partir de provocação da unidade de gestão de pessoas à unidade de tecnologia da informação, mediante publicação da nomeação do servidor ou conselheiro, no Diário Oficial do Distrito Federal.

A atribuição de permissões será realizada com base no princípio do menor privilégio necessário, ou seja, o usuário deve ter acesso apenas às informações e recursos que forem essenciais para o desempenho de suas funções.o Financeiro, em regime de repartição simples, o qual se apresenta deficitário desde sua constituição e, portanto, recebe complementação do Governo do DF para fazer face aos seus compromissos previdenciários.

As contas serão desativadas ou terão suas permissões modificadas em casos de exoneração, inatividade prolongada ou mudança de função, sendo realizadas revisões periódicas dos acessos, a fim de se identificar contas que se encaixem nesses parâmetros.

GESTÃO DE BACK-UP

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 do próprio usuário ou mau funcionamento dos sistemas, permitindo assim a restauração das informações ou dados eventualmente perdidos.

Por ser Autarquia que faz uso e possui serviços providos pelo Centro de Dados Corporativo Privado do Distrito Federal (CeTIC-DF), na forma do Decreto Distrital nº 40.015, de 14 de agosto de 2019, o Iprev-DF segue o disposto na Resolução nº 02, de 29 de abril de 2024, que aprova a Política de Backup e Recuperação de Dados do Governo do Distrito Federal.

GESTAO DE MUDANÇAS

A gestão de mudanças em relação à segurança da informação é fundamental para garantir que qualquer alteração nos sistemas, processos, ou políticas não comprometa a integridade, a confidencialidade ou a disponibilidade das informações do Iprev-DF. Implementar um processo formal para gerenciar mudanças garante que os riscos associados a elas sejam devidamente avaliados e mitigados.

Toda mudança que possa afetar a segurança da informação deve ser formalmente registrada, devendo ser aprovada pelo Comitê de Tecnologia, Governança e Segurança da Informação, considerando os riscos e impactos atrelados.

Antes da implementação de qualquer mudança, é essencial realizar uma avaliação de riscos para identificar potenciais vulnerabilidades ou falhas de segurança.

A análise deve considerar os seguintes fatores:

- Impacto sobre a confidencialidade, integridade e disponibilidade dos dados;
- Consequências para a conformidade com normas e regulamentações; e
- Possíveis pontos de exposição a ameaças ou vulnerabilidades.

O planejamento da mudança deve incluir um plano detalhado, que aborde os seguintes aspectos:

- Descrição clara da mudança;
- Cronograma para a implementação;
- Definição de responsabilidades;
- Ações para mitigar riscos à segurança;
- Plano de contingência caso a mudança cause falhas inesperadas; e
- Plano de recuperação.

As mudanças devem ser testadas, em ambiente de produção, antes de serem implementadas, visando garantir que não comprometem a segurança ou a conformidade com políticas e regulamentações.

Todas as mudanças devem ser comunicadas às partes interessadas, visando a redução de eventuais resistências e dificuldades de implementação.

Garantir que os detalhes da mudança, incluindo a avaliação de riscos, testes e resultados, estejam documentados adequadamente, com vistas a responder eventuais auditorias.

Após a implementação, a mudança deve ser monitorada para garantir que está funcionando conforme o esperado e não introduziu novos riscos.

A gestão de mudanças em relação à segurança da informação é uma prática contínua que envolve planejamento cuidadoso, avaliação de riscos, testes rigorosos e monitoramento constante para assegurar que a integridade dos sistemas e dados seja mantida.

PRIVACIDADE

Este tópico estabelece diretrizes para garantir a proteção da privacidade e a confidencialidade dos dados pessoais processados pela organização, em conformidade com as legislações aplicáveis, como a Lei Geral de Proteção de Dados (LGPD).

O Iprev-DF deve tratar os dados de forma ética e transparente, assegurando que as informações pessoais dos indivíduos sejam protegidas contra uso indevido, acessos não autorizados, perda ou violação.

Os dados pessoais serão coletados apenas com o consentimento do titular ou com base em uma das hipóteses legais permitidas, como a execução de contratos ou o cumprimento de obrigações legais.

O tratamento de dados deve sempre seguir os critérios de minimização, sendo processados apenas os dados essenciais para atingir os objetivos específicos.

Os titulares dos dados deverão ser informados sobre a finalidade da coleta, a fim de garantir que tenham claro conhecimento sobre como suas informações serão utilizadas.

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

É proibida a divulgação de informações institucionais do Iprev-DF, sem a previa ciência e anuência da alta gestão.

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

CRIPTOGRAFIA

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. Princípio do não-repúdio ou irretratabilidade, a fim de se garantir que uma ação, como o envio de uma mensagem, a realização de uma transação ou a assinatura de um documento, não possa ser negada posteriormente pela parte que a executou. Ou seja, o não repúdio impede que alguém alegue não ter realizado determinada ação, pois há provas inequívocas de que a ação foi realizada por essa pessoa ou sistema.; e

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

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; e
- Manutenção de registro e auditoria das atividades relacionadas com o gerenciamento de chaves.

GESTAO DE INCIDENTES

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.

A gestão de incidentes objetiva responder de forma eficaz a incidentes de segurança, minimizando seus impactos e evitando a recorrência. Um incidente de segurança pode ser qualquer evento que comprometa a integridade, confidencialidade ou disponibilidade das informações e sistemas.

Como incidentes de segurança, podemos citar:

- Mau funcionamento de sistemas ou serviços;
- Ataques (como os de engenharia social ou de negação de serviço);
- Acesso não autorizado;
- Envio ou recebimento de códigos maliciosos;
- Alterações em um sistema sem a aprovação do proprietário; e
- Extravio ou roubo de dados ou equipamentos que contenham informações críticas.

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.

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.

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

Para o gerenciamento de incidentes de segurança da informação, devem ser consideradas as seguintes etapas:

- Detecção e identificação: Monitoramento contínuo dos sistemas e redes para identificar rapidamente qualquer anomalia ou comportamento suspeito;
- Classificação e priorização: Após a detecção, o incidente deve ser classificado com base em sua gravidade e urgência, considerando o potencial impacto sobre os sistemas e informações da organização;

- Resposta: Plano de resposta a incidentes, que pode incluir a contenção do incidente, mitigação dos impactos e proteção dos ativos afetados (Isolamento de sistemas comprometidos, desconexão de redes afetadas, bloqueio de acessos não autorizados);
- Investigação e análise: Durante e após a resposta inicial, uma investigação detalhada deve ser conduzida para identificar as causas do incidente e a extensão do dano;

- Correção e recuperação: Implementar as ações corretivas necessárias para restaurar os sistemas e informações afetados ao seu estado operacional normal;

- Documentação e notificação: Todos os incidentes devem ser documentados em detalhes, incluindo sua causa, impacto, medidas corretivas e tempo de resposta, sendo as partes impactadas notificadas; e

- Aprendizado e melhoria contínua: Após a resolução de um incidente, realizar uma revisão pós-incidente para avaliar a eficácia da resposta, identificar áreas de melhoria e atualizar as políticas e procedimentos de segurança.

PROTEÇÃO À PROPRIEDADE INTELECTUAL

Todos os procedimentos apropriados devem ser implementados para garantir a conformidade com os requisitos legislativos, regulamentares e contratuais relacionados aos direitos de propriedade intelectual, incluído 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 especificas ou limitar a reprodução apenas para a criação de cópias de backup. É recomendado que a importância 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.

A violação de direitos autorais, após o devido processo legal, pode culminar em multa, detenção ou prisão, caso a violação ocorra com o intuito de obter lucro, além de indenização ao detentor dos direitos.

As seguintes diretrizes devem ser 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 esteja sendo violado;

III.Manter programa de conscientização das políticas para proteger os direitos de propriedade intelectual;

IV.Manter de forma adequada os registros de ativos a fim de identificar os que são passíveis de proteção dos direitos de propriedade intelectual;

V. Manter provas e evidências da propriedade de licenças, dispositivos e equipamentos;

VI.Implementar controles para assegurar que o número máximo de usuários permitidos, dentro da licença concedida, não seja 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 (vídeo ou áudio) mídias que não as permitidas pela lei de direito autoral; e

XII. Não copiar, no todo ou em partes, livros, artigos, relatórios ou outros documentos. protegidos pelo direito de propriedade intelectual.

USO DA INTELIGÊNCIA ARTIFICIAL

Sistemas de Inteligência Artificial – IA são tecnologias que simulam processos de inteligência humana, como aprendizado, raciocínio e auto-correção. Sua aplicação no ambiente de trabalho é uma realidade e vem criando novas oportunidades e habilidades, podendo ser utilizada para o processamento de dados massivos, automação de tarefas repetitivas e análise preditiva (processo que usa a análise de dados para prever resultados futuros, comportamentos e tendências).

Nesse cenário, é imprescindível definir diretrizes para o uso responsável e seguro da IA no desenvolvimento das atividades administrativas e técnicas do Instituto, visando garantir a conformidade com as normas éticas, regulatórias e de proteção de dados.

- A IA deve processar o mínimo necessário de dados pessoais para alcançar seus objetivos, a fim de reduzir o risco de exposição e facilitar a conformidade com a LGPD. Assim, deve-se limitar o seu uso, bem como anonimizar ou pseudonimizar dados sempre que possível para garantir que informações pessoais não possam ser associadas diretamente aos segurados;

- Embora a IA possa automatizar diversas tarefas, é importante que os resultados apresentados sejam analisados e só utilizados depois de devidamente validados pelo servidor responsável pela tarefa. Isso ajuda a evitar erros causados por falhas nos algoritmos ou por decisões enviesadas e garantir que casos excepcionais sejam avaliados com a devida atenção, uma vez que, mesmo podendo identificar padrões, a IA não possui a capacidade de compreender o contexto mais amplo de uma decisão, especialmente em questões humanas e sensíveis; e

- A IA aprende com os dados com os quais é treinada. Se os dados que os usuários fornecerem ao algorítimo forem incompletos ou enviesados, os resultados também serão comprometidos. Dessa forma, é essencial que os servidores entendam o funcionamento e os limites da IA. Treinamentos sobre as boas práticas de uso e monitoramento de sistemas de IA garantem a eficiência e segurança na aplicação da tecnologia.

Inteligência Artificial pode ser uma ferramenta poderosa para aumentar a eficiência e produtividade do Iprev-DF. No entanto, seu uso deve ser cauteloso e responsável, com foco na proteção dos dados sensíveis e na supervisão humana para garantir que as decisões tomadas sejam justas, transparentes e seguras.

SENSIBILIZAÇÃO E TREINAMENTO

O objetivo de um programa de sensibilização e treinamento é garantir que todos os servidores do Iprev-DF compreendam a importância da segurança da informação e estejam devidamente treinados para cumprir com as políticas, procedimentos e boas práticas relacionadas à proteção dos ativos de informação.

A segurança da informação depende, em grande parte, da conscientização e do comportamento dos usuários. Falhas humanas, como o uso inadequado de senhas, a abertura de anexos suspeitos ou a negligência no manuseio de dados confidenciais, podem resultar em incidentes de segurança. Portanto, a sensibilização contínua e o treinamento regular são essenciais para reduzir riscos e criar uma cultura de segurança dentro do Instituto de Previdência.

O Iprev-DF deverá implementar, por intermédio do Comitê de Tecnologia, Governança e Segurança da Informação, com apoio da unidade de gestão da Tecnologia da Informação, as seguintes estratégias para garantir a conscientização sobre a segurança da informação:

- **Campanhas de conscientização:** Promoção periódica de campanhas que reforcem a importância da segurança da informação, por meio de e-mails, boletins informativos, cartazes, vídeos e outras formas de comunicação;

- **Workshops e palestras:** Realização de eventos, como workshops e palestras, com especialistas internos e externos, abordando temas como cibersegurança, boas práticas, phishing, uso de redes sociais, proteção de dados, entre outros;

- **Eventos de simulação:** Condução de simulações de ataques cibernéticos e testes de phishing para avaliar a resposta dos colaboradores e fornecer feedbacks construtivos; e

- O programa de treinamento em segurança da informação será contínuo e ajustado conforme as necessidades do Iprev-DF, devendo incluir:

    - **Treinamento inicial:** Todos os novos servidores deverão receber um treinamento básico sobre as políticas de segurança da informação, abordando temas como a gestão de senhas, uso adequado dos recursos tecnológicos, proteção de dados confidenciais e práticas de cibersegurança;

    - **Treinamento periódico:** Os servidores deverão participar de treinamentos regulares, que serão atualizados para cobrir novas ameaças e boas práticas de segurança da informação, como o uso seguro de tecnologias emergentes, redes sociais e dispositivos móveis; e

» **Treinamento específico:** Servidores que atuam em áreas críticas ou que manipulam dados sensíveis devem receber treinamentos específicos relacionados às suas funções e às responsabilidades que assumem quanto à segurança da informação.

Os programas de sensibilização e treinamento serão revisados regularmente para garantir que estejam alinhados com as novas ameaças de segurança, tecnologias e regulamentos. As lições aprendidas em incidentes de segurança e auditorias de segurança também serão usadas para aprimorar o conteúdo dos treinamentos.

ATUALIZAÇÃO DA POSIC

A Política de Segurança da Informação, diretrizes, normas e demais procedimentos, deverão ser revisados 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 de Previdência;
II. Alteração ou edição de leis;
III. Expiração da validade da política de segurança;
IV. Mudanças tecnológicas; e
V. A partir dos resultados das análises de risco que estabeleçam a necessidade de mudança da norma para readequação do Instituto de Previdência à eventuais ameaças.

REFERÊNCIAS LEGAIS E NORMATIVAS

LEI COMPLEMENTAR Nº 840, DE 23 DE DEZEMBRO DE 2011. - Dispõe sobre o regime jurídico dos servidores públicos civis do Distrito Federal, das autarquias e das fundações públicas distritais.

LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. - Dispõe sobre a tipificação criminal de delitos informáticos.

LEI DISTRITAL Nº 4.990, de 12 DE DEZEMBREO DE 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.

LEI Nº 12.965, DE 23 DE ABRIL DE 2014. - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet)

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. – Lei Geral de Proteção de Dados Pessoais (LGPD).

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.

DECRETO DISTRITAL Nº 37.574 de 26.08.2016 – Aprova a Estratégia Geral de Tecnologia da Informação.

DECRETO Nº 40.015, DE 14 DE AGOSTO DE 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.

RESOLUÇÃO Nº03, DE 06 DE NOVEMBRO DE 2018. - Aprova a revisão da Política de Segurança da Informação e Comunicação (PoSIC) do Governo do Distrito Federal.

RESOLUÇÃO Nº 01, DE 29 DE ABRIL DE 2024 - Aprova a Política de Segurança da Informação e Comunicação (POSIC) do Governo do Distrito Federal.

RESOLUÇÃO Nº 02, DE 29 DE ABRIL DE 2024 - Aprova a Política de Backup e Recuperação de Dados do Governo do Distrito Federal.

PORTARIA Nº 334, DE 11 DE JULHO DE 2017. - Disciplina o uso institucional da Internet por meio da rede GDFNET, estabelecendo o bloqueio e/ou limite de acessos a determinados sítios e aplicações, além de restrições de horários para os acessos.
ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança da Informação – Sistemas de Gestão de Segurança de TIC;

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

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

IPREV DF

Instituto de Previdência dos
Servidores do Distrito Federal

Conheça mais em
www.iprev.df.gov.br