POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. Introdução

O IPPA - Instituto de Previdência Social dos Servidores Públicos do Município de Palhoça - é o órgão gestor da previdência municipal. Sua missão é servir os servidores públicos municipais de Palhoça da melhor maneira possível, pois a seriedade com que é tratado condiz com o tamanho da sua magnitude, à medida que representa não só uma autarquia, mas a segurança e a tranqüilidade dos servidores que dedicaram boa parte de sua vida ao trabalho digno e respeitoso com os cidadãos de Palhoça, sempre cumprindo com sua função.

O IPPA entende que a informação institucional é um bem essencial para suas atividades e para resguardar a qualidade e garantia dos serviços ofertados aos servidores municipais.

O IPPA compreende que a manipulação de sua informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações institucionais.

Dessa forma, o IPPA estabelece sua Política de Segurança da Informação, como parte integrante do seu sistema de gestão institucional, alinhada às boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações do Instituto ou sob sua responsabilidade.

2. Propósito

Esta política tem por propósito:

I- estabelecer diretrizes e normas de Segurança da Informação que permitam aos servidores e fornecedores do IPPA adotarem padrões de comportamentos seguros, adequados às metas e necessidades do IPPA;

II- Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação;

III- Resguardar as informações do IPPA, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade;

IV- Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus servidores e fornecedores;

V- Minimizar os riscos de perdas financeiras, da confiança de seus beneficiários ou de qualquer outro impacto negativo nos serviços do IPPA como resultado de falhas de segurança.

3. Escopo

Esta política se aplica a todos os usuários da informação do IPPA, incluindo qualquer indivíduo ou organização que possui ou possuiu vínculo com o IPPA, tais como servidores, ex-servidores, prestadores de serviço, ex-prestadores de serviço, que possuíram, possuem ou virão a possuir acesso às informações do IPPA e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura do IPPA.

4. Diretrizes

O objetivo da gestão de Segurança da Informação do IPPA é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte às operações críticas dos serviços e minimizando riscos identificados e seus eventuais impactos na instituição.

A Presidência e o Conselho Administrativo estão comprometidos com uma gestão efetiva de Segurança da Informação. Desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da instituição. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às necessidades do IPPA.

É política do IPPA:

I- Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação sejam atingidos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas;

II- Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: servidores, terceiros contratados e, onde pertinente, beneficiários.

III- Garantir a educação e conscientização sobre as práticas adotadas pelo IPPA de segurança da informação para servidores, terceiros contratados e, onde pertinente, beneficiários.

IV- Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;

V- Tratar integralmente incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas;

VI- Garantir a continuidade dos serviços através da adoção, implantação, teste e melhoria contínua de e melhorias de segurança, técnica e administrativas;

VII- Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da instituição.

5. Princípios

São princípios para o Sistema de Segurança da Informação a Confidencialidade, a Integridade e a Disponibilidade, conforme a ISO 27.001:2013. Esses princípios devem nortear todas as atividades dentro do IPPA, a fim de que as informações sejam protegidas no âmbito desta instituição.

São definições de Confidencialidade, Disponibilidade e Integridade:

I- Confidencialidade: propriedade em que a informação não é disponibilizada ou divulgada para pessoas, entidades ou processos não autorizados;

II- Disponibilidade: propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada;

III- Integridade: propriedade de proteger a exatidão e a integridade dos ativos.

Além dos princípios basilares, devem ser observados os princípios correlatos da Segurança da Informação, tais como o princípio da autenticidade, o princípio do não repúdio e o princípio da utilidade.

6. Papéis e Responsabilidades

São responsabilidades quanto à Segurança da Informação do IPPA:

a) Conselho Administrativo

I – Aprovar a Política de Segurança da Informação, bem como acompanhar e monitorar a sua execução.

b) Presidência

I – Dirigir, supervisionar e coordenar as atividades relativas à Segurança da Informação;

II - Garantir a implantação e manutenção do processo de Segurança da Informação;

III – Coordenar a atualização da Política de Segurança da Informação (PSI), propondo revisão e políticas complementares, bem como os procedimentos que assegurem as ações da Política de Segurança da Informação.

c) Grupo de Trabalho sobre LGPD

I – Articular projetos e ações voltados à adequação à Lei Federal n° 13.709/2018 (LGPD) no âmbito do IPPA.

d) Gestores das áreas

I- Gerenciar as informações geradas ou sob a responsabilidade da sua área de atuação durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pelo IPPA;

II- Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de atuação conforme normas, critérios e procedimentos adotados pelo IPPA;

III- Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de atuação, ajustando a classificação e rotulagem das mesmas conforme necessário;

IV- Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

V- Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pelo IPPA.

e) Procuradoria Jurídica

I – Dar todo apoio necessário, do ponto de vista jurídico, para implantação e funcionamento da Política de Segurança no IPPA.

f) Recursos Humanos

I – Informar o desligamento de colaboradores do IPPA ao responsável pela àrea de Tecnologia da Informação;

II – Manter ações de treinamento e educação dos usuários em Segurança da Informação;

g) Servidores e fornecedores IPPA Usuários da Informação

I – Zelar e Proteger a segurança da Informação do IPPA;

II - Comunicar ao responsável pela àrea de Tecnologia da Informação qualquer evento que viole esta política;

III - Assinar os termos de uso e afins que se fizerem necessários, assumindo responsabilidades;

IV - Responder pela inobservância da Política de Segurança da Informação.

V - Ler, compreender e cumprir integralmente os termos da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;

VI- Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Segurança da Informação, suas normas e procedimentos ao responsável pela àrea de TI ou, quando pertinente, à Presidência;

7. BACKUP

Os backups são essenciais para deixar as informações seguras e não perder nenhum dado em caso de ataques.

Todos os backups são feitos de forma automática utilizando softwares de mercado com essa finalidade. Essas rotinas são executadas preferencialmente fora do horário comercial, nos períodos em que não há nenhum ou pouco acesso de usuários ou processos aos sistemas de informática.

Esses backups são executados diariamente e ficam armazenados da seguinte forma:

Backup Local - Realizado backup local em modo bare metal de todo o conteúdo do servidor local, diariamente às 21 horas em mídias locais USB que possuem alternância de gravação (feito rodízio de mídias)

Backup Nuvem - Realizada uma cópia completa em nuvem do Google dos diretórios de rede que o servidor possui.

O backup local possui monitoramento de erros, com geração de alertas e atuação corretiva.

O Backup local é revisado mensalmente com restauração de dados para testes de integridade.

O Backup nuvem é revisado mensalmente com restauração de dados para testes de integridade.

O IPPA possui procedimentos de contingência mapeados e definidos em um manual, que pode ser solicitado à Diretoria do IPPA. Estes procedimentos definem a existência de cópias de segurança dos sistemas informatizados e dos bancos de dados.

8. Acesso à Internet e Comportamento em Mídias Sociais

O IPPA fornece acesso à Internet aos seus usuários autorizados, conforme as necessidades inerentes ao desempenho de suas atividades profissionais.

Toda informação que é acessada, transmitida, recebida ou produzida através do acesso à internet fornecida pelo IPPA está sujeita a monitoramento, não havendo por parte do usuário qualquer expectativa de privacidade.

Durante o monitoramento do acesso a internet, o IPPA se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, ler, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais, toda informação trafegada, seja originada de sua rede interna e destinada a redes externas ou o contrário.

Durante o acesso à Internet fornecido pelo IPPA não será permitido o download, o upload, a inclusão, a disponibilização, a visualização, a edição, a instalação, o armazenamento

e/ou a cópia de qualquer conteúdo relacionado expressa ou subjetivamente, direta ou indiretamente, com:

a) Qualquer espécie de exploração sexual;

b) Qualquer forma de conteúdo adulto, erotismo, pornografia;

c) Qualquer tipo de Pornografia infantil;

d) Qualquer forma de ameaça, chantagem e assédio moral ou sexual;

e) Qualquer ato calunioso, difamatório, infamante, vexatório, aviltante ou atentatório à moral e aos bons costumes da sociedade;

f) Preconceito baseado em cor, sexo, opção sexual, raça, origem, condição social, crença, religião, deficiências e necessidades especiais;

g) Incentivo ao consumo excessivo ou recorrente de bebidas alcoólicas, fumo e substâncias entorpecentes, sejam estas lícitas ou não;

h) A prática e/ou a incitação de crimes ou contravenções penais;

i) A prática de propaganda política nacional ou internacional;

j) A prática de quaisquer atividades comerciais desleais;

k) O desrespeito a imagem ou aos direitos do IPPA;

l) A disseminação de códigos maliciosos e ameaças virtuais;

m) Tentativa de expor a infraestrutura computacional do IPPA a ameaças virtuais;

n) Divulgação não autorizada de qualquer informação do IPPA classificada como confidencial ou de uso interno;

o) Uso de sites ou serviços que busquem contornar controles de acesso à internet.

9. Comportamento em mídias e redes sociais

A publicação de conteúdo referente ao IPPA em mídias e redes sociais é feita por departamentos e usuários que possuem essa responsabilidade específica, sendo os demais usuários proibidos de publicar qualquer tipo de informação em nome da instituição.

Quando no uso de suas mídias e redes sociais particulares, servidores, prestadores de serviço e terceiros contratados devem observar as seguintes restrições:

I- Não é permitido o uso de símbolos, bem como de qualquer parte da identidade visual do IPPA sem autorização prévia e expressa;

II- Não é permitida a criação, participação ou interação de/com quaisquer perfis, comunidades, grupos, tópicos de discussão e afins que empreguem o nome, símbolo ou outros sinais distintivos do IPPA, excetuando-se os canais oficiais da instituição;

III- Não é permitida a publicação de qualquer tipo de imagem, foto, vídeo, áudio relacionado ao ambiente institucional do IPPA sem a expressa autorização da instituição, excetuando-se material divulgado em canais oficiais.

10. Serviço de E-Mail

O IPPA fornece o serviço de e-mail para seus usuários autorizados exclusivamente para o desempenho de suas atividades profissionais;

Não é permitido o uso de qualquer serviço de e-mail, que não seja o oficialmente fornecido pelo IPPA.

Quando o usuário fizer uso do serviço de e-mail do IPPA, não é permitido:

I- Utilizar do serviço de e-mail em caráter pessoal ou para fins que não sejam de interesse do IPPA;

II- Utilizar de termos ou palavras de baixo calão na redação de mensagens;

III- Enviar informação classificada como de uso interno ou confidencial para endereços eletrônicos que não fazem parte do domínio institucional do IPPA, excetuando-se quando expressamente autorizados;

IV- Inscrever o endereço de e-mail do IPPA em listas de distribuição e grupos de discussão que não estejam relacionadas com atividades laborais ou do interesse da instituição;

V- Fazer uso de qualquer técnica de falsificação ou simulação de falsa identidade e manipulação de cabeçalhos de e-mail. Qualquer tentativa, mesmo não consumada, será tratada como um incidente de segurança da informação e estará sujeita a sanções e/ou demais penalidades aplicadas conforme decisão da Presidência;

VI- Tentar a interceptação ou alteração do conteúdo da mensagem de outros usuários ou terceiros, a menos que devidamente autorizado;

VII- Utilizar o serviço de e-mail para o envio de mensagens indesejadas (spam) ou qualquer tipo de técnica que possa levar a sobrecarga do serviço de e-mail;

VIII- Usar o serviço de e-mail para disseminar ou transmitir mensagens de caráter injurioso, calunioso ou que possam ferir a legislação em vigor;

IX- Usar o serviço de e-mail para o envio de mensagens cujo conteúdo incite uso de drogas, terrorismo, práticas subversivas, violência, aborto, práticas racistas, assim como qualquer outro que possa infringir a legislação vigente;

O IPPA adota um padrão para criação dos endereços de E-mail sendo composto pelo nome do departamento @ippa.sc.gov.br ou primeironome@ippa.sc.gov.br.

Casos de endereços de e-mail coincidentes ou que possam ocasionar cacofonias e situações vexatórias poderão ser alterados para seguir um modelo fora do padrão adotado pelo IPPA, devendo primeiramente ser revisados pelo responsável pela área de Tecnologia da Informação.

Não é permitido o uso de sobrenomes de filiação na composição do endereço de e-mail como, por exemplo, tais como Júnior, Filho, Neto, Segundo e Terceiro.

Os usuários do serviço de e-mail do IPPA devem adotar a assinatura padrão, formatada de acordo com o seguinte modelo:

a) Nome Completo;
b) Cargo;
c) Telefone.

Ao final do e-mail, após a assinatura, deverá ser exibido o seguinte aviso de confidencialidade:

“Esta mensagem, juntamente com qualquer outra informação anexada, é protegida por lei, e somente os seus destinatários são autorizados a usá-la. Caso a tenha recebido por engano, por favor, informe o remetente e em seguida apague a mensagem, observando que não há autorização para armazenar, encaminhar, imprimir, usar, copiar o seu conteúdo.”

11. Requisitos do Controle de Acesso

11.1. Gerenciamento de acesso do usuário

Os procedimentos formais de controle de acesso do usuário devem ser documentados, implementados e mantidos atualizados para cada aplicativo e sistema de informações, isto para garantir o acesso de usuário autorizado e impedir o acesso não autorizado. Eles devem abranger todos os estágios do ciclo de vida do usuário, desde o registro inicial até o cancelamento final.

Os direitos de acesso do usuário devem ser revisados em intervalos regulares. As contas de administração do sistema só devem ser fornecidas aos usuários que realmente irão executar tarefas de administração do sistema.

11.2. Registro de usuário

Uma solicitação de acesso à rede e aos sistemas de computadores da instituição deve primeiro ser enviada ao Suporte de TI para aprovação. Todas as solicitações serão tratadas de acordo com um procedimento formal que garanta que as verificações de segurança sejam realizadas e que a autorização seja obtida antes da criação da conta de usuário.

Uma senha inicial forte deve ser criada na configuração da conta e comunicada ao usuário por meios seguros. O usuário deve ser obrigado a alterar a senha no primeiro uso da conta.

Quando o servidor for exonerado, em circunstâncias comuns, seu acesso aos sistemas e dados deve ser suspenso no último dia de trabalho. É responsabilidade do supervisor solicitar a suspensão dos direitos de acesso por meio do Suporte de TI.

Em circunstâncias excepcionais, em que haja um risco do servidor tomar providências que possam prejudicar a instituição antes ou após a exoneração, uma solicitação para remover o acesso pode ser aprovada e acionada antes da notificação da exoneração. Esta precaução será aplicável nos casos em que o servidor tem acessos privilegiados.

As contas de usuário devem ser inicialmente suspensas ou desativadas apenas, e não excluídas. Os nomes das contas de usuários não devem ser reutilizados, pois isso pode causar confusão no caso de uma investigação posterior.

11.3. Fornecimento do acesso

Cada usuário deve ter direito de acesso e permissões a sistemas de computador e dados que sejam compatíveis com as tarefas que deve executar.Isso será baseado na função, ou seja, uma conta de usuário será adicionada a um grupo com as permissões de acesso exigidas para essa função.

As funções de grupo devem ser mantidas de acordo com os requisitos dos serviços e quaisquer alterações devem ser formalmente autorizadas e controladas por meio do processo de gerenciamento de mudanças.

As permissões adicionais não devem ser concedidas a contas de usuário fora da função do grupo. Se tais permissões forem necessárias, isso deve ser tratado como uma modificação e formalmente solicitado.

11.4. Remoção ou adequação dos direitos de acesso

Quando é necessário um ajuste de direitos ou permissões de acesso, isso deve ser feito como parte da mudança de função. É preciso garantir que os direitos de acesso, que não são mais necessários na nova função, sejam removidos da conta do usuário. No caso de um usuário assumir uma nova função além da existente, deve ser solicitado mudanças.

Sob nenhuma circunstância os administradores poderão alterar suas próprias contas de usuário ou permissões.

11.5. Gestão dos direitos de acesso privilegiado

Os direitos de acesso privilegiados, como aqueles associados a contas de nível de administrador, devem ser identificados para cada sistema ou rede e rigorosamente controlados. Em geral, os usuários técnicos, não farão o uso diário de contas de usuário com acesso privilegiado. Em vez disso, uma conta de usuário “admin” separada deve ser criada e usada somente quando necessário. Estas contas devem ser específicas para um indivíduo, por ex. “João da Silva Admin”. Contas de administração genéricas não devem ser usadas, pois fornecem identificação insuficiente do usuário.

O acesso a permissões no nível de administrador só deve ser destinado a indivíduos com essas funções e que receberam treinamento suficiente para entender as implicações de seu uso.

O uso de contas de usuário com acesso privilegiado em rotinas automatizadas, deve ser evitado sempre que possível. Quando isso for inevitável, a senha usada deve ser protegida e alterada regularmente.

11.6. Revisão dos direitos de acesso ao usuário

Anualmente, os responsáveis de ativos e sistemas serão obrigados a analisar quem tem acesso às suas áreas de responsabilidade e o nível de acesso. Isto para identificar:

I- Pessoas que não devem ter acesso;
II- Contas de usuário com mais acesso do que o exigido pela função;
III- Contas de usuário com alocações de função incorretas;
IV- Contas de usuário que não fornecem identificação adequada, por exemplo contas genéricas ou compartilhadas;
V- Quaisquer outros problemas que não estejam em conformidade com esta política.

Esta revisão será realizada por um procedimento formal e quaisquer ações corretivas identificadas e realizadas.

Uma revisão das contas de usuários com acesso privilegiado será realizada trimestralmente pelo responsável da área de TI para assegurar que esta política esteja sendo cumprida.

11.7. Autenticação e senha do usuário

Uma senha forte é uma barreira essencial contra o acesso não autorizado.

A política do IPPA é utilizar métodos de autenticação adicionais com base em uma avaliação de riscos que leve em consideração:

I- O valor dos ativos protegidos;
II- O grau de ameaça que se acredita existir;
III- O custo do(s) método(s) adicional(is) de autenticação;
IV- A facilidade de uso e praticidade do(s) método(s) proposto(s);
V- Quaisquer outros controles relevantes.

O uso de métodos de autenticação de múltiplos fatores deve ser justificado com base nos fatores acima, e implementados e mantidos de maneira segura.

Se a autenticação de um ou vários fatores é usada, a qualidade das senhas de usuários deve ser aplicada, conforme os seguintes parâmetros:

Parâmetro	Valor
Comprimento mínimo	8
Comprimento máximo	100
Caracteres necessários	Pelo menos uma letra maiúscula Pelo menos um símbolo Pelo menos um número
Semelhança de senha	A nova senha não pode compartilhar mais de três caracteres na mesma posição que a senha antiga
Mudar a frequência	Pelo menos a cada 90 dias
Bloqueio de conta	Em 5 tentativas incorretas de logon
Ação de bloqueio de conta	A conta deve ser reativada pelo [Serviço de TI]
Outros controles	A senha não pode conter o nome do usuário

Quaisquer exceções a estas regras devem ser autorizadas pelo responsável pela àrea de TI.

11.8. Responsabilidades do usuário

Todos os usuários devem desempenhar sua parte na proteção do acesso que receberam e garantir que sua conta não seja usada para prejudicar a instituição.

Para maximizar a segurança das informações, todo usuário deve:

I- Ter uma senha forte, ou seja, que esteja de acordo com as regras definidas nesta política;
II- Nunca informar sua senha ou permitir que alguém use sua conta;
III- Não anotar sua senha por escrito ou eletronicamente, por exemplo. em um arquivo ou e-mail;
IV- Evitar usar a mesma senha para outras contas de usuário, pessoais ou relacionadas ao serviço;
V- Assegurar de que qualquer PC ou dispositivo conectado à rede esteja bloqueado ou desconectado, quando não estiver por perto;
VI- Informar ao responsável pela área de TI sobre quaisquer alterações em suas funções e requisitos de acesso.

O não cumprimento desses requisitos pode resultar na aplicação de ações disciplinares contra o(s) indivíduo(s) envolvido(s).

12. Controle de Monitoramento do ambiente físico

O IPPA faz o monitoramento do seu ambiente físico interno e externo com o uso de circuito interno de televisão e câmeras de filmagem instaladas em suas dependências integrado com sistema de alarme.

As câmeras de filmagem estão dispostas de forma a resguardar a dignidade humana, sendo vedada a sua instalação em banheiros, lavabos e na área reservada ao atendimento médico.

A filmagem descrita nesta Política tem por objetivo assegurar a segurança física do ambiente do IPPA, bem como a sua segurança patrimonial, não constituindo qualquer violação à intimidade, vida privada, honra ou imagem da pessoa filmada, o que o usuário tem ciência expressamente neste ato.

As imagens captadas dentro das dependências do IPPA serão arquivadas enquanto for razoavelmente esperado que elas possam ser úteis. Isso pode variar em diferentes circunstâncias e, portanto, os períodos de retenção serão definidos de acordo com a situação ou contexto em que uma determinada câmera do CCTV é operada. Quando o período de retenção tiver expirado, as imagens devem ser excluídas com segurança, se apropriado, por meio de um processo automático.

As imagens deverão ser mantidas em caráter estritamente confidencial, somente podendo ser divulgadas em caso de infração às regras constantes em suas políticas e normas e/ou infração de legislação vigente.

Para fins da LGPD, o IPPA atuará como o controlador de dados para o uso do CCTV.

Quando é usado um terceiro como parte do tratamento de imagens do CCTV, será considerado um operador no contexto da LGPD e um contrato em conformidade com o produto deve estar vigente.

O IPPA não permite o uso de qualquer dispositivo de gravação audiovisual dentro do seu perímetro físico, excetuando-se quando o usuário estiver formalmente autorizado.

13. Dispositivos Móveis

13.1. Dispositivos fornecidos pelo IPPA

A menos que especificamente autorizado, somente dispositivos móveis fornecidos pelo IPPA devem ser usados para manter ou processar informações internas em nome da instituição.

Se o servidor precisar usar equipamentos móveis, receberá um dispositivo adequado, que será configurado para cumprir as políticas da instituição. O suporte será fornecido pelo responsável pela área de TI, que pode, às vezes, precisar de acesso ao seu dispositivo para resolução de problemas e manutenção.

O servidor deve garantir que o dispositivo seja transportado em um invólucro protetor quando possível e não seja exposto a situações nas quais possa ser danificado. Não é permitido deixar o dispositivo à vista do público, como na parte de trás de um carro ou em uma sala de reunião.

Não é permitido remover nenhuma marca de identificação no dispositivo, como uma etiqueta de patrimônio ou um número de série.

Não é permitido adicionar hardware periférico ao dispositivo sem a aprovação do TI.

Não é permitido manter informações internas no dispositivo, a menos que isso tenha sido autorizado e que os controles apropriados sejam implementados. Não é permitido deixar tokens de acesso, números de identificação pessoal ou outros itens de segurança com o dispositivo.

É necessário certificar de que a tela do dispositivo “trave” após um curto período de inatividade e que exija um código de acesso ou senha para desbloqueá-lo. As senhas

usadas devem ser fortes e difíceis de adivinhar. Nenhum login não seguro, ou seja, aqueles que não exigem uma senha podem ser configurados no dispositivo.

O dispositivo fornecido pela instituição é apenas para uso das funções do servidor do IPPA. O equipamento não deve ser compartilhado com familiares ou amigos ou usado para atividades pessoais. O servidor poderá ser solicitado a devolver o dispositivo ao TI a qualquer momento para inspeção e auditoria. O usuário não deve instalar nenhum software não autorizado ou alterar a configuração do dispositivo sem antes consultar o TI.

13.2. Uso de Dispositivos Móveis Pessoais

Os indivíduos não devem usar seus próprios dispositivos para manter e processar informações da instituição, a menos que tenham enviado uma solicitação para fazê-lo, e essa solicitação tenha sido formalmente aprovada. É política do IPPA avaliar cada solicitação TSPD para estabelecer:

I- A identidade da pessoa que faz a solicitação;
II- O motivo da solicitação;
III- Os dados que serão mantidos ou tratados no dispositivo;
IV- O dispositivo específico que será usado.

As solicitações devem ser enviadas para o Suporte de TI.

O princípio geral desta política é que o grau de controle exercido pela instituição sobre o dispositivo TSPD seja apropriado para a sensibilidade dos dados contidos nela.

Para garantir que os dados sejam protegidos adequadamente, é importante que o IPPA possa monitorar e auditar o nível de conformidade com essa política. O nível de monitoramento e auditoria será apropriado para cada informação armazenada no dispositivo.

Os métodos e o tempo de monitoramento e auditoria deverão respeitar a privacidade do proprietário do dispositivo, em conformidade com a legislação aplicável. Em geral, o monitoramento do uso fora do horário comercial será evitado.

No caso de perda ou roubo do dispositivo, o proprietário deve informar o Suporte de TI o mais rápido possível, fornecendo detalhes sobre as circunstâncias da perda e a sensibilidade das informações de propriedade do IPPA armazenadas nele. O IPPA reserva o direito de apagar remotamente o dispositivo, sempre que possível, como medida de segurança. Isso pode envolver a exclusão de dados pertencentes ao proprietário do dispositivo.

Ao ser exonerado ou pedir exoneração, o proprietário do dispositivo deve permitir que o dispositivo seja auditado e todos os dados e aplicativos relacionados aos serviços do IPPA sejam removidos.

14. Instalação de software

Os servidores não podem instalar software nos dispositivos de computação operados na rede do IPPA, sem prévia autorização;

As solicitações de software devem primeiro ser aprovadas pelo gerente do solicitante e, em seguida, enviadas ao responsável pela àrea de Tecnologia da Informação por escrito ou por e-mail;

O software deve ser selecionado de uma lista de softwares aprovada, mantida pelo responsável pela área de Tecnologia da Informação, a menos que nenhuma seleção na lista atenda à necessidade do solicitante.

O responsável pela área de Tecnologia da Informação obterá e rastreará as licenças, testará novos softwares quanto a conflitos e compatibilidade e realizará a instalação.

Os usuários não devem ter acesso administrativo ao computador para permitir que instalem software nele. Somente software aprovado será permitido e isso deve ser instalado pelo departamento de TI mediante solicitação autorizada.

A varredura regular de computadores de usuários para detectar software não autorizado deve ser realizada.

15. Ameaça Malware

15.1 Definição

Malware é qualquer código ou software que possa ser prejudicial ou destrutivo para as capacidades de processamento de informações da organização.

O termo é derivado da expressão “Software Malicioso” e também pode ser chamado de código malicioso ou comumente “um vírus”.

15.2 Tipos de Malware

Os tipos mais comuns de malware encontrados hoje são:

- ***Vírus*** – um programa que executa uma função indesejada no computador infectado. Isso pode envolver ações destrutivas ou a coleta de informações que podem ser usadas pelo invasor;
- ***Trojan*** – um programa que finge ser um código legítimo, mas que esconde outras funções indesejadas. Muitas vezes disfarçado como um jogo ou programa utilitário;
- ***Worm*** – um programa capaz de se copiar em outros computadores ou dispositivos sem interação do usuário;
- ***Logic bomb*** – código malicioso que foi configurado para ser executado em uma data e hora específica ou quando certas condições são atendidas;
- ***Rootkit*** – um programa usado para disfarçar atividades maliciosas em um computador, ocultando os processos e arquivos do usuário;
- ***Keylogger*** – código que registra as teclas digitadas pelo usuário;
- ***Backdoor*** – um programa que permite acesso não autorizado ao invasor.

Geralmente, esses tipos de malware são usados em combinação uns com os outros.

15.3 Como o Malware se propaga

Para que um software mal-intencionado execute sua finalidade, ele precisa ser instalado no dispositivo ou no computador de destino. As técnicas de infecção mais comuns são as seguintes:

15.3.1 Phishing

Esse método envolve enganar o usuário para realizar alguma ação que faça com que um programa malicioso seja executado e infecte o computador que está sendo usado. Geralmente é conseguido através do envio geral de e-mails não solicitados (Spam) com anexos de arquivos ou links da web. Quando o usuário abre o arquivo ou clica no link, a ação mal-intencionada é acionada.

15.3.2 Websites e Código Móvel

O uso disseminado de códigos móveis, como o JavaScript, forneceu outra rota para infectar computadores com malware. Muitas vezes sites são criados para hospedar o malware que é ativado ou clicando em um link ou, em alguns casos, simplesmente visitando o site.

Cada vez mais, sites legítimos são comprometidos e feitos para hospedar malware sem o conhecimento do proprietário, o que facilita muito esse tipo de ataque para o usuário.

15.3.3 Mídia Removível

Cartões de memória USB, CDs, DVDs e outros dispositivos de mídia removível fornecem uma maneira eficaz de espalhar malwares em computadores. Quando a mídia é inserida

na máquina, o malware é executado e infecta o alvo ou se copia na mídia removível para se preparar para infectar a próxima máquina em que for conectado.

15.3.4 Hacking

Ou “Cracking”, é um método mais direcionado e, portanto, menos comum de introduzir malware em um computador ou rede, obtendo acesso não autorizado à rede de fora (e às vezes dentro) da organização. Este método requer mais conhecimento por parte do agressor e, muitas vezes, explora as vulnerabilidades existentes no software ou nos dispositivos de rede utilizados. Depois que o acesso for obtido, o malware será instalado remotamente na máquina comprometida.

15.4 Anti-Malware

Para evitar a infecção de computadores e redes do IPPA e evitar as consequências potencialmente terríveis de tal infecção, há uma série de controles importantes que serão adotados como política.

O conceito chave adotado nesta política é “defesa em profundidade” e nenhum controle individual deve ser usado para fornecer proteção adequada. Portanto, esta não é uma escolha entre os controles, mas uma lista de controles necessários, os quais devem ser implementados sempre que possível para proteger contra as ameaças anteriormente descritas.

15.4.1 Firewall

Um firewall será instalado em todos os pontos em que a rede interna estiver conectada à Internet.

As permissões de acesso devem ser definidas de forma que o usuário não possa desabilitar o firewall.

15.4.2 Antivírus

Uma plataforma antivírus comercial com suporte será instalada na organização em locais chave:

- Firewall;
- Servidores de e-mail;
- Servidores proxy;
- Todos os outros servidores;
- Todos os computadores do usuário;
- Dispositivos móveis, incluindo laptops.

Por padrão, a varredura de acesso deve estar ativada para fornecer proteção em tempo real. Varreduras completas regulares também devem ser realizadas pelo menos uma vez por mês.

Os usuários não devem poder desativar a proteção configurada centralmente.

15.4.3 Filtragem de Spam

Um sistema será instalado para filtrar e-mails não solicitados e potencialmente prejudiciais (spam). Os tipos de anexos que costumam conter malware devem ser bloqueados ou removidos antes da entrega ao usuário.

15.4.4 Gestão de Vulnerabilidade

Informações sobre vulnerabilidades de software serão coletadas de fornecedores e fontes de terceiros e atualizações aplicadas quando disponíveis.

A varredura de vulnerabilidades deve ser realizada regularmente, particularmente em redes e servidores críticos para os negócios.

15.4.5 Treinamento de conscientização do usuário

Os usuários devem estar cientes quando começarem a trabalhar na organização da política de segurança da informação e receberem treinamento para evitar serem vítimas de ataques.

Esse treinamento de conscientização deve ser repetido regularmente para todos os servidores que fazem uso de equipamentos de TI.

15.4.6 Monitoramento de ameaças e alertas

Informações sobre ameaças emergentes serão obtidas de fontes adequadas e usuários alertados sobre possíveis ataques, fornecendo o máximo de detalhes para maximizar a chance de reconhecimento.

15.4.7 Revisões Técnicas

Avaliações regulares serão realizadas em redes e servidores essenciais aos negócios para identificar qualquer malware que tenha sido instalado desde a última revisão.

15.4.8 Gestão de Incidentes de Malware

No caso de um malware ser detectado em um servidor, rede ou outro componente de TI, um incidente de segurança das informações será gerado. Isso será gerenciado de

acordo com os procedimentos estabelecidos no *Procedimento de Resposta a Incidentes de Segurança da Informação*.

16. Sanções e Punições

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa;

A aplicação de sanções e punições será realizada conforme a análise da Presidência, devendo-se considerar a gravidade da infração, efeito alcançado e as recorrências podendo a Presidência, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.

No caso de terceiros contratados ou prestadores de serviço, a Presidência deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato.

Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano o IPPA, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nos itens anteriores desta política.

16.1. Casos Omissos

Os casos omissos serão avaliados pela Presidência.

As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação do IPPA adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações do IPPA.

17. Glossário

Ameaça: Causa potencial de um incidente, que pode vir a prejudicar a instituição;

Ativo: Tudo aquilo que possui valor para a instituição;

Ativo de informação: Patrimônio intangível da instituição, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro,

mercadológico, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas a instituição por parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional da instituição ou por infraestrutura externa contratada pela instituição, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.

Confidencialidade: Propriedade dos ativos da informação da instituição, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.

Controle: Medida de segurança adotada pela instituição para o tratamento de um risco específico.

Disponibilidade: Propriedade dos ativos da informação da instituição, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas.

Gestor da Informação: Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação.

Incidente de segurança da informação: Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da instituição.

Integridade: Propriedade dos ativos da informação da instituição, de serem exatos e completos.

Risco de segurança da informação: Efeito da incerteza sobre os objetivos de segurança da informação da instituição.

Segurança da informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da instituição.

Usuário da informação: Colaboradores com vínculo empregatício de qualquer área da instituição ou terceiros alocados na prestação de serviços a instituição, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizados a utilizar manipular qualquer ativo de informação da instituição para o desempenho de suas atividades profissionais.

Vulnerabilidade: Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da instituição.

18. Revisões

Esta política é revisada com periodicidade anual ou conforme o entendimento da Presidência.

19. Gestão da Política

Esta política foi aprovada pela Presidência e, posteriormente, pelo Conselho Administrativo.

Esta Política será revisada de acordo com a demanda que se fizer necessária.