Política

Segurança da Informação

Elaborador: George L. Vignoto Silva | **Revisor:** Roberto Stricher

Aprovador: Política aprovada pelo CONSUNI – Conselho Superior Universitário em xxxxxx | Versão: 01

UNIPAR
UNIVERSIDADE PARANAENSE

Sumário

1. OBJETIVO

Normatizar os procedimentos visando a preservação da segurança da informação, primando pela confidencialidade, integridade, disponibilidade, autenticidade, bem como a legalidade dos processos que amparam a operacionalização e gestão das atividades da Instituição.

2. DEFINIÇÕES

INFORMAÇÃO: compreende-se a toda a base de conhecimento, conteúdo, dado, conceito, envio ou recebimento de mensagens, processo ou fato existente, em meio físico ou eletrônico, que compõe documentos e informações de propriedade, interesse ou posse da UNIPAR e inclui, mas não se limita a, qualquer dado, material, procedimento, processo, especificações, inovações e aperfeiçoamento técnicos e comerciais que agreguem valor para o negócio da empresa, assim como todas as informações confidenciais dos nossos acadêmicos sob nossa custódia.

SEGURANÇA DA INFORMAÇÃO: é a proteção da Informação contra vários tipos de ameaças, para garantir a continuidade do negócio, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades de negócios.

CONFIDENCIALIDADE: proibição de disponibilização ou exposição da Informação a indivíduos, entidades ou processos não autorizados expressamente, seja por contratos ou outros instrumentos formais.

INTEGRIDADE: garantia da exatidão e completeza das informações, tal como foram criadas ou recebidas, utilizando tecnologias, controles e processos que garantam esse requerimento pelo próprio design dos produtos e sistemas.

DISPONIBILIDADE: garantia de que a informação estará disponível sempre que for preciso. Sistemas e informações pertencentes ao ecossistema tecnológico deverão estar disponíveis para acadêmicos, colaboradores e terceiros, atendendo também a confidencialidade das informações e integridade de seu conteúdo, formando, assim, uma tríade de Segurança de qualidade superior.

AUTENTICIDADE: garantia de que a informação foi criada, editada ou emitida por quem se disse ter sido, sendo capaz de gerar evidências não repudiáveis em relação ao criador, editor ou emissor.

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS: toda e qualquer informação relacionada a pessoa natural identificada ou identificável. Os dados pessoais contidos nas informações devem ser protegidos com a adoção de medidas técnicas e organizacionais de Segurança da Informação, nos termos impostos pela Lei nº 13.709/2018 (LGPD) que estará disciplinada em conjunto com o Procedimento de Tratamento de Dados Pessoais, Código de Conduta, Ética e Integridade e Política de Privacidade.

CFTV: sistema fechado de televisão interno, que distribui sinais provenientes de câmeras localizadas em locais específicos da UNIPAR, para um ou mais pontos de visualização e controle.

DOWNLOAD: ação de transferir dados de um computador remoto para um computador local. A cópia de arquivos pode ser feita tanto a partir de servidores dedicados (como FTP, por exemplo), quanto pelo simples acesso a uma página da Internet no navegador.

TENTATIVA DE BURLA: atos que busquem violar as diretrizes estabelecidas nos documentos normativos da UNIPAR e sejam frustrados por erro durante o planejamento ou durante sua execução.

COLABORADOR: empregado, estagiário, menor aprendiz, empregado com contrato de trabalho temporário ou qualquer outro indivíduo ocupante de cargo ou emprego na UNIPAR.

TERCEIRO: prestador de serviço, terceirizado, fornecedor, credenciado, consultor, instrutor e parceiro.

USB: tecnologia que permite a conexão de periféricos sem a necessidade de desligar o computador, além de transmitir e armazenar dados.

MÍDIAS REMOVÍVEIS: dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Disquete, Pen Drive, cartão de memória entre outros.

SOFTWARE: Conjunto de instruções, programas e dados a eles associados, empregados durante a utilização do computador, também conhecido como aplicativo.

FIREWALL: dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

NUVEM: disponibilidade de recursos do sistema de computador, especialmente armazenamento de dados e capacidade de computação, sem o gerenciamento ativo direto do utilizador.

STORAGE: equipamento voltado para armazenar dados de servidores, da rede local da empresa ou mesmo de um celular.

DoS ou DDoS: (*Distributed Denial of Service*) ataque de negação de serviço, é uma tentativa de fazer com que aconteça uma sobrecarga em um servidor ou computador comum para que recursos do sistema fiquem indisponíveis para seus utilizadores.

ITIL: (Information Technology Infrastructure Library) em tradução livre para o português, significa Biblioteca de Infraestrutura de Tecnologia da Informação. O ITIL serve para organizar processos de TI e orientar profissionais a exercerem suas funções com eficiência.

3. PRINCÍPIOS

Preservar e proteger as informações sob a responsabilidade da Universidade Paranaense - UNIPAR, inclusive as contidas nos recursos de Tecnologia da Informação e Comunicação, dos diversos tipos de ameaça e desvios de finalidade em todo o seu ciclo de vida, estejam elas em qualquer suporte ou formato.

Prevenir e mitigar impactos gerados por incidentes envolvendo a segurança da informação e comunicação.

Assegurar a confidencialidade, a integridade, a disponibilidade e a autenticidade, assim como a legalidade no desenvolvimento das atividades do negócio.

Cumprir a legislação vigente no Brasil e demais instrumentos regulamentares relacionados às atividades da Instituição no que diz respeito à segurança da informação, aos objetivos institucionais e aos princípios de privacidade, morais e éticos.

4. CATEGORIAS DAS INFORMAÇÕES

PÚBLICAS: são todas as informações disponibilizadas ou destinadas ao público, através da Internet, ou veiculadas em documentos publicados em jornais, revistas, folders, redes sociais, panfletos, avisos ou palestras autorizadas.

Somente os Departamento de Comunicação Social Universitário e Reitoria poderão publicar informações sobre a empresa ou “em nome da UNIPAR”, bem como, definir e orientar porta-vozes do negócio.

INTERNAS: são todas as informações disponíveis aos colaboradores por meio das ferramentas aprovadas, com armazenamento interno, em servidores da UNIPAR ou terceiros autorizados.

As informações classificadas como “INTERNA” não poderão ser encaminhadas, divulgadas ou publicadas em quaisquer meios para terceiros não autorizados, devendo a sua disponibilização ser restrita ao ambiente de trabalho da UNIPAR e seu uso limitado aos colaboradores ou Terceiros (mediante assinatura de “Termo de Sigilo e Confidencialidade” (*Non-Nisclosure Agreement - NDA*), que realmente necessitem ter acesso a tais informações.

RESTRITAS: são todas as informações de determinada área, assim classificadas, restritas a ela, que não possam ser acessadas por outros setores da UNIPAR. Seu acesso e manuseio incorrem somente ao próprio setor que a criou.

O acesso das informações restritas a outros setores poderá ser realizado através de autorização do Gestor da área solicitada.

CONFIDENCIAIS: são todas as informações que por sua origem, natureza ou importância não devam ser compartilhadas ou colocadas à disposição de pessoas não autorizadas, bem como, indistintamente, dados recebidos ou compilados de/sobre acadêmicos, senhas, informações financeiras ou de salários, código fonte, informações sensíveis de usuários entre outras.

As informações classificadas como confidenciais deverão ser mantidas em arquivos físicos ou eletrônicos com níveis de segurança compatíveis com a relevância da Informação, tais como cofres, armários com chaves, diretórios criptografados ou envio dos arquivos somente após a inclusão de mecanismos de segurança (senha ou criptografia).

A transmissão de informações confidenciais deverá ser realizada utilizando meios de transmissão confiáveis e seguros para as partes, previamente autorizadas, com contrato de sigilo claro e dentro da validade, sejam as partes: funcionários, colaboradores, associados, fornecedores ou qualquer tipo de parceiro de negócios que precisam: criar, armazenar ou processar qualquer tipo de Informação confidencial.

Para transmissão de informações confidenciais por e-mail em servidores e domínios diferentes, é necessário adicionar criptografia adicional em nível de arquivo (senha no arquivo utilizando criptografia forte de no mínimo AES 1024 bits ou equivalente).

A proteção por senha deve ser aplicada INCLUSIVE para proteção de certificados privados de uso geral (por exemplo, ao se gerar pares de chaves SSH, é necessário aplicar senha FORTE nas chaves privadas).

Atendendo aos requisitos contratuais de sigilo, os meios de armazenamento previamente aprovados são: discos criptografados, transmissão por rede ou internet utilizando SSL (com certificado de origem e destino da transmissão pertencentes às partes acordadas em contrato), SSH ou SFTP (FTP via SSH) usando criptografia SHA256 ou RSA.

SIGILOSAS: são todas as informações que possuam o mais alto nível de sensibilidade e criticidade para o negócio. Informações estratégicas com alto nível de confidencialidade também podem ser classificadas como SIGILOSAS a critério do proprietário da informação. Informações em que seu possível vazamento implica em impacto financeiro direto ao negócio ou ponha em risco a continuidade dos negócios é um indício para que ela receba esta classificação.

Devem ser armazenadas em volumes criptográficos acrescidos de criptografia de arquivo: criptografia multinível com chaves e algoritmos distintos.

Não podem ser copiadas, fotografadas, filmadas (incluindo sistemas de CFTV) ou testemunhadas, pessoalmente ou por meio de telepresença de qualquer forma.

Sempre que possível, a depender da necessidade, as informações SIGILOSAS não deverão ser armazenadas, processadas ou transmitidas no ambiente computacional (*brain storage only*).

O armazenamento das informações SIGILOSAS, em regime de exceção, poderá ocorrer em sistemas offline ou sistemas online previamente aprovados pelo setor de TI.

A classificação dos documentos deverá ocorrer em campo visível, preferencialmente na primeira página e próximo ao cabeçalho do Documento.

Os documentos que contenham mais de um tipo de Informação com classificação original distintas, por exemplo, dois documentos unidos em um único arquivo, a classificação mais restritiva passa a valer para todo o documento.

Qualquer informação que não tenha sua classificação especificada de forma clara no documento será automaticamente considerada como Informação "RESTRITA".

É vedada a revelação de qualquer informação de propriedade ou sob a responsabilidade da UNIPAR, por seus dirigentes, colaboradores e terceiros, sem a prévia e formal autorização para tanto, inclusive no âmbito acadêmico, excetuando-se a hipótese de que a informação esteja previamente classificada como "pública".

PUBLICAÇÃO DE INFORMAÇÕES ABERTAS: Somente os gestores da UNIPAR, com assessoria devida do Departamento de Comunicação Social Universitário, poderão classificar informações para divulgar externamente ou as definir como Informação Pública.

DESCARTE DE INFORMAÇÃO CLASSIFICADA: As informações classificadas como RESTRITA, CONFIDENCIAL ou SIGILOSA devem sofrer tratamento especial no seu descarte.

O descarte de informações, armazenadas em meio físico ou eletrônico, deverá ser realizado segundo o procedimento de descarte aplicável ao caso, para garantir que a informação descartada não possa ser recuperada de qualquer forma.

Além dos demais procedimentos aplicáveis, (i) todas as informações impressas deverão ser trituradas/destruídas antes de seu descarte; aparelhos eletrônicos devem ser "resetados" antes de seu descarte; e (ii) informações eletrônicas deverão ser deletadas mediante o uso de ferramentas apropriadas ao descarte de dados, a ser disponibilizada pelo Departamento de Tecnologia da Informação.

EXTRAVIO DE INFORMAÇÃO: Qualquer evento de perda, extravio ou roubo de informações, devem ser reportados IMEDIATAMENTE ao Departamento de Tecnologia da Informação, bem como, ao Encarregado (DPO), através do e-mail: **lgpd@unipar.br**

5. DIRETRIZES

A UNIPAR respeita a privacidade dos titulares de dados e garante a disponibilidade, integridade e confidencialidade dos dados pessoais em todo o seu ciclo de vida, desde a coleta, armazenamento, compartilhamento, até o descarte, em qualquer tipo de formato de armazenamento e suporte de acordo com a sensibilidade do dado pessoal, a finalidade e a gravidade dos riscos, observado no que couber a Política de Proteção de Dados e Privacidade desta Instituição.

5.1. USO DOS ATIVOS DE TI (FERRAMENTAS CORPORATIVAS)

A UNIPAR oferece ao colaborador: conta de correio eletrônico, acesso à internet e outras ferramentas de comunicação e produtividade para a dinamização do trabalho ou utensílios como aparelho e linha celular, gavetas, armários e quaisquer dispositivo, físico ou lógico, para a execução do trabalho.

O uso destas ferramentas está sujeito a esta Política e restrições de acesso, de acordo com o nível de acesso outorgado ao usuário e deliberações do Departamento de Tecnologia da Informação, aprovados pela Reitoria.

Como política de nível de acesso à Informação, utilizamos a premissa de "menor privilégio possível". O Colaborador somente terá acesso aos aplicativos e informações que forem estritamente necessários para a realização do seu trabalho.

É expressamente proibido o uso de qualquer recurso corporativo, computadores, redes, acessos, bem como, quaisquer meios de comunicação corporativas para o uso pessoal e/ou prática de qualquer ato ilícito, sob pena de responsabilização civil ou até criminal.

O colaborador é responsável pelos ativos de tecnologia da informação fornecidos pela UNIPAR, bem como, pelas informações que inserir em tais ativos.

5.2. USO E ACESSO DA INTERNET

São permitidos, observado esta política de Segurança da Informação, podendo haver bloqueios de sites classificados como inseguros ou não confiáveis.

É proibido a transferência de arquivos por meio de quaisquer protocolos, aplicativos ou ferramentas não oficiais, ou que não forem previamente aprovados e divulgados pelo Departamento de Tecnologia da Informação.

A aprovação supramencionada, refere-se a uma análise de segurança da ferramenta e do fornecedor do produto, a fim de garantir que somente ferramentas e fabricantes de alta maturidade em Segurança da Informação, Proteção de Dados e Políticas Claras de Privacidade, sejam incorporados à lista de ferramentas e fornecedores oficiais da UNIPAR.

É proibido o *download* de materiais protegidos por direitos autorais ou a instalação de *softwares* não homologados pelo Departamento de Tecnologia da Informação. O

colaborador deve consultar o Departamento de Tecnologia da Informação antes de realizar o download de qualquer software de terceiros.

5.3. USO DO EMAIL CORPORATIVO (CORREIO ELETRÔNICO)

O correio eletrônico da UNIPAR, assim como todas as plataformas de comunicação utilizadas na empresa, são ferramentas de trabalho, não devendo ser utilizado para outros fins.

As informações contidas nas mensagens eletrônicas são de propriedade da UNIPAR podendo ser monitoradas a qualquer tempo sem aviso ou notificação prévia para fins de auditoria de conformidade às normas internas, regulamentações ou boas práticas aplicadas ao negócio da UNIPAR. (Vide o item 5.20).

É proibido o *download* de materiais protegidos por direitos autorais ou a instalação de softwares não homologados pelo Departamento de Tecnologia da Informação. O colaborador deve consultar o Departamento de Tecnologia da Informação antes de realizar o download de qualquer software de terceiros.

É proibido o envio de informações classificadas como "INTERNAS" e "CONFIDENCIAIS" para endereços de e-mail de outros domínios além do @unipar.br, exceto para terceiros (acadêmicos ou fornecedores) diretamente envolvidos no respectivo assunto da mensagem.

As informações classificadas como "SIGILOSAS" não devem ser armazenadas ou transmitidas por e-mail simples. Para isso, é obrigatório o uso de criptografia forte adicional para proteção do conteúdo da mensagem e seus anexos, através de solicitação ao Departamento de Tecnologia da Informação e autorização do gestor imediato.

Quando houver o "desligamento" de colaborador do quadro operacional da UNIPAR (rescisão do contrato de trabalho), deverão ser observados os seguintes procedimentos em relação ao seu e-mail corporativo:

A. O colaborador, independente de seu cargo poderá, desde que acompanhado por um outro colaborador da UNIPAR designado para essa tarefa, retirar eventual e-mail pessoal e/ou informações pessoais constantes em sua caixa de e-mails corporativa e/ou arquivos digitais e físicos;

B. O e-mail corporativo do colaborador desligado emitirá mensagem de resposta automática ao receber novos e-mails, informando que aquele e-mail está suspenso e que o remetente poderá entrar em contato diretamente com a UNIPAR através dos outros canais de comunicação (por exemplo, e-mail de eventual gestor do colaborador desligado);

C. Após a notificação do desligamento, o e-mail corporativo ficará ativo pelo prazo máximo de até 24 (vinte e quatro) horas, findo esse período o acesso será

bloqueado, permanecendo "*offline*" e armazenado sob responsabilidade do Departamento de Tecnologia da Informação, pelo prazo máximo de 3 (três) meses, e/ou a critério da Diretoria Executiva de Gestão das Relações Trabalhistas, transcorrendo este prazo, o e-mail será excluído definitivamente, junto com todas as informações e dados pessoais.

5.4. CRIAÇÃO DE PERFIS DE ACESSO (*LOGINS*)

A criação de perfis de acesso aos sistemas UNIPAR será realizada pelo Departamento de Tecnologia da Informação, mediante solicitação por gestor competente, devidamente instruída com o nome do colaborador, matrícula, nome do gestor imediato, departamento lotado, local e ramal bem como perfil de acesso para servidor de arquivos e internet.

Os usuários criados deverão refletir a identidade do colaborador, inviabilizando qualquer interpretação contrária ou de caráter genérico.

5.5. INFRAESTRUTURA DE TECNOLOGIA DA INFORMAÇÃO (ITIL)

A Gestão de Mudanças no ITIL é o processo de gerenciamento responsável por efetuar mudanças nos ambientes e consequentemente aos serviços de tecnologia da informação constantes na UNIPAR, através de padrões de avaliação, aprovação, implementação e revisão de todas estas mudanças.

Os ambientes de produção serão segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

É proibido a modificação de aplicativos e sistemas realizadas diretamente nos ambientes de produção. Eventuais alterações deverão ser avaliadas e aprovadas pelo Departamento de Tecnologia da Informação.

5.6. SENHAS DE ACESSO

A senha de acesso aos recursos computacionais da UNIPAR é de inteira responsabilidade do colaborador, que não deverá, em hipótese alguma, compartilhar ou emprestar a outros colaboradores e terceiros (uso pessoal e intransferível)

Os usuários deverão utilizar senhas "fortes", misturando letras e números, em todos os sistemas corporativos.

O tamanho mínimo de senha recomendável é de 9 caracteres, com o uso obrigatório de 4 (quatro) opções (maiúsculo, minúsculo, caractere especial e numeral).

Serão aplicadas restrições ao uso de palavras/informações comuns, tais como: data de nascimento, nome e sobrenome entre outros.

Toda ação feita, dentro ou fora do ambiente computacional da UNIPAR, será de responsabilidade do colaborador que a deu causa, ou, daquele em que as credenciais estão vinculadas.

5.7. CONTAS INATIVAS

Toda e qualquer credencial de acesso com ausência de atividade em até 50 (cinquenta) dias serão bloqueadas em TODOS os sistemas corporativos.

5.8. AUTENTICAÇÃO MULTI-FATOR

É recomendável o uso de autenticação multi-fator (2FA ou MFA; *Two factor Authentication* ou *Multi-Factor Authentication*) para todos os serviços onde a opção estiver disponível.

5.9. ACESSO REMOTO

Os colaboradores previamente cadastrados, mediante aprovação explícita dos seus gestores diretos, poderão obter acesso remoto ao ambiente computacional da UNIPAR para trabalho fora de seu ambiente normal (*Home Office*). Será necessário a abertura de chamado ao departamento de TI com a devida aprovação da gestão.

Para os serviços realizados em *Home Office,* é obrigatório que a conexão estabelecida seja realizada através de VPN privada corporativa ou Remote Desktop, previamente configurada pelo Departamento de Tecnologia da Informação.

5.10. MESA LIMPA E TELA LIMPA

Os colaboradores deverão zelar pela limpeza e organização do ambiente de trabalho a fim de não expor desnecessariamente informações classificadas, e/ou dados pessoais.

Os documentos e anotações impressos, poderão permanecer nas mesas em caráter temporário, após uso, deverão ser recolhidos em compartimentos fechados (Ex. gavetas, armários, cofres entre outros).

Os documentos notoriamente importantes (que possuem assinaturas por exemplo), destinados ao descarte, deverão ser depositados em um local/armário especial para que possam ser revisados antes de sua destruição.

Toda Informação que permanecer nas mesas poderá e deverá ser destruída pelo colaborador responsável.

Os colaboradores deverão observar as boas-práticas destinadas a segurança da informação tais como;

A. Apagar informações escritas em quadros ou lousas;

B. Evitar impressões desnecessárias de informações e documentos;

C. Retirar imediatamente as impressões realizadas na impressora;

D. Evitar a retenção desnecessária de documentos emprestados;

E. Desligar ou suspender os computadores e demais equipamentos durante ausência;

F. Proteger do acesso não autorizado, chaves, senhas, crachás entre outros;

G. Desconectar do computador, após o uso, todas as mídias removíveis;

H. Posicionar estrategicamente os móveis e equipamentos eletrônicos inviabilizando a visualização de terceiro através de portas e janelas;

I. Gerenciar e permitir o acesso de terceiros apenas aos locais a eles destinados;

J. Manter gavetas, armários, cofres, entre outros, fechados e seguros;

K. Alimentar-se apenas em locais apropriados;

L. Zelar pela organização e limpeza do local de trabalho;

M. Assegurar-se ao sair do local de trabalho, de que portas, janelas, armários, entre outros, estejam devidamente trancados.

A segurança dos documentos é de responsabilidade do colaborador que o detém, o qual deverá zelar e evitar qualquer tipo de "vazamento" e/ou incidente de segurança.

5.11. BLOQUEIO DE DISPOSITIVO POR INATIVIDADE

Todos os dispositivos de acesso aos sistemas corporativos deverão sofrer bloqueio automático após 10 minutos de inatividade (computadores, smartphones, tablets ou qualquer outro dispositivo, móvel ou não) desde que disponível no equipamento tal funcionalidade e que seja de propriedade da UNIPAR.

5.12. CAPTURA DE TRÁFEGO NA REDE

É expressamente proibido a captura de tráfego de rede dentro da rede corporativa da UNIPAR salvo eventos devidamente autorizados pelo Departamento de Tecnologia da Informação ou pela Reitoria, para fins exclusivos de diagnóstico, auditoria e monitoração previamente autorizados.

5.13. USO DE DISPOSITIVOS PESSOAIS

O uso de dispositivos pessoais fica restrito a rede de "convidados" e rede "acadêmica" da UNIPAR.

Não é permitida a conexão de dispositivos não corporativos à rede corporativa, cabeadas ou sem fio, sem a devida autorização e cadastro pelo Departamento de Tecnologia da Informação.

Os colaboradores que realizam o uso de dispositivos móveis para o desempenho de funções e tarefas específicas, o farão utilizando equipamentos verificados pela UNIPAR, com os devidos controles e proteções técnicas aplicadas.

5.14. REDES SOCIAIS

É proibido ao colaborador emitir qualquer comunicado, opinião ou comentário EM NOME da UNIPAR sem a expressa aprovação e alinhamento com as áreas de marketing e comunicação.

As interações de resposta, réplica aos comentários feitos por terceiros sobre a UNIPAR e afins, serão realizadas pelo Departamento de Comunicação Social Universitário, mesmo sendo postadas em redes pessoais.

A publicação de fotos em áreas internas deverá ser evitada, para que informações restritas contidas nas áreas internas da UNIPAR, não sejam "vazadas" e/ou publicadas indevidamente.

5.15. SOFTWARES

É proibido a instalação de softwares não aprovados pelo Departamento de Tecnologia da Informação, em quaisquer dispositivos que acessam os sistemas de Informação da UNIPAR, quais sejam: computadores, notebooks, dispositivos portáteis como tablets e celulares, inclusive software, aplicativos, plug-ins pagos ou gratuitos.

O Departamento de Tecnologia da Informação deverá possuir um portfólio de ferramentas e aplicativos atualizados para atender as demandas do negócio incluindo ferramentas de produtividade e afins. A maioria dessas ferramentas serão previamente instaladas em todos os dispositivos corporativos.

Os computadores e notebooks da UNIPAR terão o acesso bloqueado para instalação e atualização de qualquer tipo de software, onde o usuário deverá solicitar ao setor de Tecnologia da informação a instalação/atualização, momento em que será realizada a análise dos riscos dessa instalação/atualização.

5.16. ANTIVÍRUS E FIREWALL

Para acesso a rede da UNIPAR, os computadores deverão possuir softwares de proteção contra códigos maliciosos (antivírus, anti spyware, anti adware, dentre outros) previamente instalados e atualizados.

O Departamento de Tecnologia da Informação poderá acessar remotamente qualquer máquina sob domínio da UNIPAR e realizar o bloqueio imediato daquelas em que forem constatadas potenciais ameaças/riscos que impactem na disponibilidade dos serviços e de rede interna.

É proibido desabilitar as ferramentas de antivírus e firewall.

O antivírus dos servidores e estações de trabalho serão atualizados automaticamente e a varredura por vírus será realizada diariamente nas estações e nos servidores.

5.17. CÓPIAS DE SEGURANÇA (BACKUPS)

Para aumentar os níveis de segurança, bem como, garantir a continuidade de negócio, será realizado backups dos servidores.

Os usuários da rede corporativa deverão salvar os arquivos importantes para cumprimento da função diretamente no servidor de rede.

O backup completo de todas as aplicações deverá ser executado diariamente conforme a política de backup ao que se refere à periodicidade diária, semanal e mensal bem como sua retenção conforme o tipo de aplicação.

O backup individual das máquinas de trabalho será realizado conforme a necessidade e solicitação do usuário, quando houver a substituição e/ou manutenção destes equipamentos.

5.18. SEGURANÇA DO AMBIENTE FÍSICO

Os servidores (máquinas) que armazenam os sistemas utilizados pela UNIPAR, estão alocados em ambientes protegidos. O acesso a esses ambientes é monitorado e controlado, restrito a pessoas previamente identificadas e autorizadas pelo Departamento de Tecnologia da Informação.

O acesso dessas áreas por pessoas não autorizadas previamente, porém, que necessitem realizar o acesso físico ao local, deverá ser realizado obrigatoriamente com o acompanhamento de pessoas autorizadas.

O acesso às dependências da UNIPAR com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, não pertencente ou não autorizado previamente por esta, deverá ser feito com autorização expressa do Departamento de Comunicação Social Universitário e Reitoria, mediante a supervisão de um colaborador indicado.

5.19. USO DE MÍDIAS REMOVÍVEIS E DA PORTA USB

O uso de mídias removíveis não é recomendado pela UNIPAR, devendo ser tratado como exceção à regra. A porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações.

A liberação das portas USB dos computadores será avaliada mediante solicitação ao Departamento de Tecnologia da Informação, devendo o usuário solicitante apresentar autorização do Gestor do Departamento, bem como, justificar a necessidade do uso.

Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação, e

continuidade de negócio, vez que, este tipo de mídia pode conter softwares maliciosos, o que pode danificar e comprometer dados e equipamentos.

É vedado aos usuários utilizarem mídias removíveis como meio preferencial de armazenamento de informações corporativas, devendo valer-se das ferramentas de "nuvem" disponibilizadas pela UNIPAR.

5.20. POSTURA GERAL DE PRIVACIDADE

Os acessos aos sistemas internos devem ter como justificativa um propósito real de profissionalismo.

É expressamente proibido o acesso a quaisquer informações de acadêmicos, colaboradores, terceiros a qualquer registro nos sistemas de informação da UNIPAR sem um propósito claro ligado diretamente ao exercício das funções atribuídas na relação de trabalho entre o colaborador e a empresa.

É expressamente proibido o acesso a dados de acadêmicos, funcionários e terceiros por mera curiosidade, tais como: acessar contas de celebridades, pessoas públicas, parentes, amigos ou qualquer outro, sem que haja um propósito de negócio e principalmente, uma solicitação relacionada ao caso.

5.21. ÁUDIO, VÍDEOS E FOTOS

É vedada qualquer atividade relacionada à captura de dados e seu compartilhamento público, inclusive no âmbito acadêmico, na internet e/ou nas mídias sociais, envolvendo gravação de áudio, vídeo ou foto de informações confidenciais, restritas a uso interno, sigilosas ou enquadradas como dados pessoais, que sejam utilizadas na realização das atividades profissionais dentro das dependências da UNIPAR por seus gestores, colaboradores e terceiros, sem autorização para tanto, exceto se ocorrer em razão justificável como necessário para cumprimento das atividades profissionais prestadas pelo colaborador.

5.22. MONITORAÇÃO

A UNIPAR reserva-se ao direito de monitorar todas as atividades realizadas por seus colaboradores nos sistemas de informação, para garantir o cumprimento desta e outras políticas da empresa.

Os ambientes internos e externos da UNIPAR também podem sofrer gravação audiovisual com o propósito principal de gerenciar a segurança dos perímetros da empresa, contra incidentes de segurança de qualquer natureza.

O uso e acesso ao sistema de vigilância (CFTV) é restrito e gerenciado pelo Departamento de Facilities.

6. PENALIDADES

A violação desta Política poderá acarretar sanções administrativas e/ou legais, sem prejuízo da rescisão do contrato de trabalho e/ou qualquer outro contrato de relacionamento de prestação de serviço entre terceiros, assim como qualquer entidade com relação contratual direta ou indireta com a UNIPAR.

A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, deve ser tratada como uma violação.

7. PAPÉIS E RESPONSABILIDADES

7.1. DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

a) Revisão e atualização das ações educacionais sobre Segurança da Informação, objetivando uma "reciclagem" contínua de todos os colaboradores e terceiros.

b) Revisão desta Política de Segurança da Informação sempre que necessário, servindo como guia para ações de educação e difusão da cultura de Segurança da Informação e proteção de dados pessoais.

c) Fomento à cultura de Segurança da Informação dentro da UNIPAR e em toda cadeia de relacionamento incluindo, acadêmicos, colaboradores e terceiros.

d) Designar uma equipe de Respostas a Incidentes de Segurança da Informação, preparada para receber, analisar e responder as notificações.

e) Tratar com prioridade os comunicados de incidentes de segurança da informação e comunicação, realizando o encaminhamento adequado aos profissionais envolvidos na demanda.

7.2. COLABORADORES E TERCEIROS

a) Cumprir rigorosamente os termos desta Política de Segurança da Informação.

b) Reportar ao Departamento de Tecnologia da Informação, ou ao canal disponibilizado por este, a suspeita ou confirmação de descumprimentos de toda a documentação de Segurança da Informação e seus Objetivos de Controle, bem como de tentativas de burla de recursos e ferramentas e/ou quaisquer incidentes de Segurança da Informação.

OBSERVAÇÃO: Considera-se como Incidentes de Segurança da Informação:

- Acesso não autorizado aos recursos de TI, sistemas e bancos de dados da UNIPAR ou de Terceiros;
- Ataques de negação de serviços (DoS ou DDoS);
- Acesso não autorizado ou vazamento de dados, pessoais ou não;
- Uso impróprio de informações;

- Pirataria;
- Falhas de equipamentos da UNIPAR;
- Vírus;
- Violação aos termos desta Política.

Os casos omissos e eventual procedimento diverso do previsto nesta Política de Segurança da Informação serão submetidos à análise do GRC.

8. REGULAMENTAÇÃO INTERNA / EXTERNA

- Lei Geral de Proteção de Dados Pessoais – 13.709/2028;
- Política de Conduta, Ética e Integridade;
- ISO 27001.

9. VIGÊNCIA E HISTÓRICO DE APROVAÇÃO

A presente Política de Gestão de Contratos, contendo os direcionamentos e regramentos, passa a vigorar a partir de sua aprovação.

DATA	DESCRIÇÃO	APROVADOR
DD/MM/AAAA	Criação da atual política	Conselho Superior Universitário na Ata #
DD/MM/AAAA	2ª Versão – Revisão e atualização do documento.	Conselho Superior Universitário na Ata #