2024

Versão 1.2

Política de SEGURANÇA DA INFORMAÇÃO

Funpar

01.
Introdução

O Manual de Normas da Política de Segurança da Informação da Fundação da Universidade Federal do Paraná para o Desenvolvimento da Ciência, da Tecnologia e da Cultura, doravante intitulada FUNPAR, tem como objetivo estabelecer orientações, normas e ações que estabelecem as diretrizes corporativas para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

A presente Política de Segurança da Informação (PSI) está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2013 (substituta da ABNT NBR ISO/IEC 27002:2005), reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como, está de acordo com as leis vigentes em nosso País.

A segurança da informação é, obtida pela implantação de uma gama de controles que incluem procedimentos de rotina (como as verificações de antivírus), infraestrutura de hardware e software (como a gestão de soluções para assinatura eletrônica de documentos), além da criação de uma política devidamente documentada.

Chegamos, assim, à Política de Segurança da Informação (PSI), definida como as regras que ditam o acesso, o controle e a transmissão da informação da Instituição.

- Lembrando que uma política de segurança não é um documento imutável e inquestionável.
- Muito pelo contrário, requer atualização constante e participação não só da diretoria da empresa, mas também dos funcionários e da equipe de Unidade de Tecnologia da Informação (UNITIN).

1. Objetivos da PSI

Estabelecer diretrizes que permitam aos colaboradores da FUNPAR seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades do negócio e da proteção legal da empresa e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como, a implementação de controles e processos para seu atendimento.

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela FUNPAR pertence à referida instituição:

- As exceções devem ser explicitadas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais:

- O uso pessoal dos recursos é permitido, desde que não prejudique o desempenho dos sistemas e serviços.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

A FUNPAR, por meio da Unidade de Tecnologia da Informação (UNITIN), poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

É também obrigação de cada colaborador manter-se atualizado em relação a este Manual de Normas da Política de Segurança da Informação e aos procedimentos e normas relacionadas, buscando orientação do seu gestor, da Unidade de Tecnologia de Informática (UNITIN) ou da Unidade de Gestão de Pessoas (UNIGEP) sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

As diretrizes aqui estabelecidas deverão ser adotadas por todos os colaboradores, bem como, os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

2. Princípios da PSI

Como se trata de uma metodologia de proteção às informações da empresa, a Política de Segurança da Informação (PSI) é implementada nas organizações por intermédio de alguns princípios básicos, os quais garantem que cada variável importante receba a devida atenção e corrobora com o objetivo central da ação que é aumentar a integridade dos sistemas de informações.

A Política de Segurança da Informação (PSI) é regida por três princípios básicos conhecidos como “trinca sagrada” da segurança da informação, são eles:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

3. Requisitos da PSI

Quando empresas lidam com dados, um dos seus grandes deveres é mantê-los intocáveis, de forma a preservar a sua originalidade e confiabilidade. Caso contrário, erros podem ocorrer na interpretação dessas informações, gerando também rupturas no Compliance do negócio e, no pior dos casos, sanções penais pesadas.

Nesse contexto, garantir a integridade é, pois, adotar todas as precauções necessárias para que a informação não seja modificada ou eliminada sem autorização, isto é, que mantenha a sua legitimidade e consistência, condizente exatamente com a realidade.

Para isso, deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a FUNPAR julgar necessário para reduzir os riscos dos seus ativos de informação, como por exemplo, em:

- Estações de trabalho;
- Notebooks;
- Acessos à internet;
- Correio eletrônico; e
- Sistemas comerciais e financeiros desenvolvidos pela FUNPAR ou por terceiros.

Para a uniformidade da informação, a Política de Segurança da Informação (PSI) deverá ser comunicada a todos os colaboradores da FUNPAR a fim de que a política seja cumprida dentro e fora da Instituição;

Deverá haver um comitê multidisciplinar responsável pela gestão da segurança da informação, doravante designado como Comitê de Segurança da Informação (CSI);

Deverá fazer parte de todos os contratos (CLT e prestadores de serviços) da FUNPAR o anexo Termo de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição;

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores.

- Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Unidade de Tecnologia de Informática (UNITIN) e ela, se julgar necessário, deverá encaminhar posteriormente ao Comitê de Segurança da Informação (CSI) para análise.

Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação;

Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e:

- Justificados
- Concordados;
- Documentados;
- Implementados; e
- Testados durante a fase de execução.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação;

Este Manual de Normas da Política de Segurança da Informação é de uso obrigatório para todos os colaboradores, independentemente do nível hierárquico ou função, bem como, de vínculo empregatício ou prestação de serviço;

02.
Responsabilidades Específicas

Além da diretoria, a Unidade de Gestão de Pessoas (UNIGEP) também deve ler o documento e aprovar suas premissas, de acordo com as leis trabalhistas e com a Política de Recursos Humanos da instituição.

Trata-se de efetivamente implantar a política. Nesse momento, é preciso comunicar todos os funcionários, que devem receber uma cópia do documento, além de um treinamento prático que apresente seus pontos principais.

A política deve estar sempre acessível aos colaboradores e a assinatura de cada um deles, com uma declaração de comprometimento, deve ser recolhida após o treinamento.

Colaboradores, prestadores de serviços, estagiários e afins da FUNPAR, em qualquer nível hierárquico, na sua esfera de competência, serão responsáveis por cumprir e zelar pela materialização e realização eficaz das normas e princípios da segurança da informação, em atenção especial ao compromisso com os critérios legais e éticos que envolvam a instituição.

1. Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Será de inteira responsabilidade de cada colaborador todo prejuízo ou dano que vier a sofrer ou causar à FUNPAR e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

2. Dos Colaboradores em Regime de Trabalho Temporários

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança da Informação (CSI).

A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

3. Dos Gestores de Pessoas e/ou Processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento deste Manual de Normas da Política de Segurança da Informação da FUNPAR.

Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como, comprometendo-se a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da FUNPAR.

Antes de conceder acesso às informações da instituição, exigir a assinatura do Termo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Adaptar às normas, processos, procedimentos e sistemas sob sua responsabilidade para atender a este Manual de Normas da Política de Segurança da Informação.

4. Do Custodiante da Informação

4.1 DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO (TI)

Ajustar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por este Manual de Normas da Política de Segurança da Informação.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários.

- No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade, como, por exemplo:
  - Manutenção de computadores;
  - Realização de cópias de segurança;
  - Auditorias; ou
  - Testes no ambiente.

Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Garantir segurança especial para sistemas com acesso público, incluindo o ambiente educacional, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes.

- Para as trilhas geradas e mantidas em meio eletrônico, implantar controles de integridade para torná- las juridicamente válidas como evidências.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a FUNPAR.

Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela Tecnologia da Informação (TI), nos ambientes totalmente controlados por ela.

O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

Garantir que todos os ativos críticos de Tecnologia da Informação (TI) sejam instalados em ambientes especializados conhecidos como Data Centers:

- Esses devem conter todas as proteções e contingências necessárias para a sua respectiva proteção. Implantar e manter funcionais os controles e padrões de segurança definidos para os ativos de tecnologia.

Manter atualizada a infraestrutura tecnológica, de acordo com a recomendação de fabricantes de hardware e software.

Tratar os riscos e vulnerabilidades identificados em ativos, sistemas ou processos sob sua responsabilidade ou custódia.

Quando ocorre movimentação interna dos ativos de Tecnologia da Informação (TI), garantir que as informações de um usuário não sejam removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- Os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário;

- Os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

Proteger continuamente todos os ativos de informação da empresa contra código malicioso e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.

Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

Monitorar o ambiente de Tecnologia da Informação (TI), gerando indicadores e históricos de:

- Uso da capacidade instalada da rede e dos equipamentos (espaço disponíveis para uso);
- Tempo de resposta no acesso à internet e aos sistemas críticos da FUNPAR;
- Períodos de indisponibilidade no acesso à internet e aos sistemas críticos da FUNPAR;
- Incidentes de segurança:
    - Vírus;
    - Trojans;
    - Furtos;
    - Acessos indevidos;
    - Entre outros.

Atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet, por exemplo:

- Sites visitados;
- E-mails recebidos/enviados;
- Upload/download de arquivos;
- Entre outros.

4.2 DA ÁREA DE RECURSOS HUMANOS

Verificar o histórico de candidatos a emprego, de acordo com a ética e leis vigentes.

Garantir que o Manual de Normas da Política de Segurança da Informação e seus procedimentos sejam seguidos e divulgados no processo de admissão/ integração de novos colaboradores.

4.3 DA ÁREA JURÍDICA

Apoiar na aplicação de medidas disciplinares referente às violações da política de segurança da informação e de Privacidade.

Identificar requisitos legais pertinentes à segurança da informação e à privacidade.

Garantir a adoção de cláusulas pertinentes à segurança das informações e à proteção de dados nos contratos estabelecidos com a FUNPAR.

4.4 DE FORNECEDORES E PARCEIROS DE NEGÓCIOS

Cumprir as determinações das Políticas e Procedimentos publicados pela da FUNPAR.

Orientar os colaboradores da empresa sobre o cumprimento das determinações das diretrizes e procedimentos publicados pela FUNPAR.

Cumprir com o acordo de confidencialidade.

4.5 DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO (CSI)

O Comitê de Segurança da Informação (CSI) é um grupo composto por representantes-chave para a segurança da informação e tem como principal responsabilidade a gestão e o direcionamento das atividades relacionadas à segurança da informação. Seu propósito fundamental é garantir a proteção, confidencialidade, integridade e disponibilidade dos dados e informações da instituição.

Deve ser formalmente constituído, por colaboradores com nível hierárquico mínimo de gestão, nomeados para participar do grupo pelo período de dois anos.

A composição do Comitê deverá ter o Gerente de Administração e Finanças no comando, além de um colaborador de cada uma das seguintes áreas:

- Unidade de Gestão de Pessoas (UNIGEP);
- Unidade de Controle e Informações Gerenciais (UNICOG);
- Unidade de Gestão da Tecnologia da Informação (UNITIN).

O Comitê de Segurança da Informação (CSI) deverá submeter toda e qualquer deliberação à Assessoria Jurídica (ASSJUR) da FUNPAR antes de sua divulgação.

Deverá o Comitê de Segurança da Informação (CSI) reunir-se formalmente pelo menos uma vez a cada seis meses:

- Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a FUNPAR.

O Comitê de Segurança da Informação (CSI) poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

4.5.1 CABE AO COMITÊ DE SEGURANÇA DA INFORMAÇÃO (CSI)

- Propor investimentos relacionados à Segurança da Informação com o objetivo de reduzir riscos;
- Propor alterações nas versões da Política de Segurança da Informação (PSI) e a inclusão, a eliminação ou a mudança de normas complementares;
- Realizar avaliações periódicas dos riscos à segurança da informação da instituição, de modo a identificar áreas de vulnerabilidade e tomar medidas proativas para mitigá-las;
- Avaliar os incidentes de segurança e propor ações corretivas;
- Definir as medidas cabíveis nos casos de descumprimento da Política de Segurança da Informação (PSI);
- Orientar e coordenar as ações de Segurança da Informação, promovendo a execução de acordo com o que foi estabelecido;
- Estabelecer políticas, normas e diretrizes relacionadas à segurança da informação, definindo os padrões que devem ser seguidos por todos os membros da organização;
- Desenvolver e estabelecer programas de conscientização e divulgação da Política de Segurança da Informação (PSI);
- Realizar monitoramento contínuo dos sistemas e infraestrutura de TI para identificar possíveis ameaças e garantir que os controles de segurança estejam sendo efetivamente aplicados. Além disso, realizar auditorias periódicas para verificar a conformidade com as políticas e normas estabelecidas;
- Conduzir a gestão de incidentes de segurança da informação, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;
- Conduzir os processos de monitoramento e Segurança da Informação;
- Definir controles para tratamento de riscos, vulnerabilidades, ameaças e não conformidades identificadas pelos processos de Segurança da Informação;
- Propor projetos e iniciativas para melhoria do nível de Segurança da Informação;
- Reportar suas atividades ao Departamento Administrativo e Financeiro da FUNPAR.

03.
Do Monitoramento e da Auditoria do Ambiente

Para garantir as regras mencionadas neste Manual de Normas da Política de Segurança da Informação, a FUNPAR poderá:

- Implantar sistemas de monitoramento nas estações de trabalho:
  - Servidores;
  - Correio eletrônico;
  - Conexões com a internet;
  - Dispositivos móveis ou wireless; e
  - Outros componentes da rede.

- A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como, material manipulado;
- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação (CSI);
- Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

1. Correio Eletrônico

O uso do correio eletrônico da FUNPAR é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição.
- Caso necessite enviar e-mail para múltiplos destinatários, deverá solicitar ao “moderador”; do e-mail para efetuar tal atividade.
- Enviar mensagem por correio eletrônico pelo endereço de seu departamento, ou usando o nome de usuário de outra pessoa, ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a FUNPAR ou suas unidades vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins em autorização expressa e formal concedida pelo proprietário desse ativo de informação;

- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades da FUNPAR estiver sujeita a algum tipo de investigação;
- Produzir, transmitir ou divulgar mensagem que:
  - Contenha qualquer ato ou forneça orientação que conflite ou contradiga os interesses da FUNPAR;
  - Contenham ameaças eletrônicas, como:
    - Spam;
    - E-mail bombing;
    - Vírus de computador.
  - Contenha arquivos que representem um risco à segurança, a exemplo, sem se limitar a arquivos com código executável:
    - .exe,
    - .cm,
    - .bat,
    - .pif,
    - .js,
    - .vbs,
    - .hta,
    - .cpl,
    - .reg,
    - .dll,
    - .inf.
- Obter acesso não autorizado a outro computador, servidor ou rede;
- Interrompa um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Possa burlar qualquer sistema de segurança;
- Espia secretamente ou assedie outro usuário;
- Acesse informações confidenciais sem explícita autorização do proprietário;
- Acesse indevidamente informações que possam causar prejuízos a qualquer pessoa;
- Inclua imagens criptografadas ou de qualquer forma mascaradas;
- Contenha anexo(s) superior(es) a 5MB para enviar (interno e internet) de 5MB para recebimento (internet):
  - As exceções deverão ser comunicadas e aprovadas pelo Comitê de Segurança.
- Contenha conteúdo considerado impróprio, obsceno ou ilegal:
  - Que seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico, entre outros:

- Que contenha perseguição preconceituosa baseada em:
  - Sexo;
  - Raça;
  - Incapacidade física ou mental;
  - Ou outras situações protegidas;
- Que contenha fins políticos local ou nacional (propaganda política);
- Que esteja em desacordo com a Lei nº 13.709/2018 (LGPD).

- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

2. Padrão de assinaturas

2.1 PADRÃO PARA USO GERAL DOS COLABORADORES

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador;
- SIGLA DO DEPARTAMENTO;
- Nome do departamento;
- Correio eletrônico;
- Telefone(s);
- Endereço.

Após a assinatura, acrescentar a mensagem da Lei nº 13.709/2018 – Lei de Geral de Proteção de Dados Pessoais (LGPD), no tamanho pequeno e fonte em itálico:

- *Esta mensagem, incluindo seu(s) anexo(s), pode conter informações privilegiadas e/ou de caráter confidencial em decorrência de relação contratual e/ou da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD), não podendo ser retransmitida sem autorização expressa do remetente. Se você recebeu esta mensagem por engano, por favor, informe-nos e apague-a; não copie ou divulgue seu conteúdo.*

Em caso de ausência prolongada por motivos diversos (férias, treinamento, licença, etc.), o colaborador deverá colocar mensagem de ausência no seu e-mail para que processos e atividades sejam conduzidos sem maiores transtornos.

O Colaborador deverá alinhar com o gestor a quem deverá ser direcionada as mensagens na sua ausência.

2.2 PADRÃO COM CELULAR CORPORATIVO

Assinatura caso o colaborador precise colocar um número de telefone corporativo além de seu ramal.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador;
- SIGLA DO DEPARTAMENTO:
  - Nome do departamento.
- Correio eletrônico;
- Telefone(s);
- Endereço.

Após a assinatura, acrescentar a mensagem da Lei nº 13.709/2018 – Lei de Geral de Proteção de Dados Pessoais (LGPD), no tamanho pequeno e fonte em itálico:

- *Esta mensagem, incluindo seu(s) anexo(s), pode conter informações privilegiadas e/ou de caráter confidencial em decorrência de relação contratual e/ou da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD), não podendo ser retransmitida sem autorização expressa do remetente. Se você recebeu esta mensagem por engano, por favor, informe-nos e apague-a; não copie ou divulgue seu conteúdo.*

Em caso de ausência prolongada por motivos diversos (férias, treinamento, licença, etc.), o colaborador deverá colocar mensagem de ausência no seu e-mail para que processos e atividades sejam conduzidos sem maiores transtornos.

O Colaborador deverá alinhar com o gestor a quem deverá ser direcionada as mensagens na sua ausência.

2.3 PADRÃO CARGO COM MATRÍCULA

Assinatura caso o cargo exija matrícula junto a algum órgão (ex: CRC/PR, OAB, etc.). Caso seja necessário, coloque o cargo em CAIXA ALTA (ex: CONTADOR, ASSESSOR JURÍDICO, ENGENHEIRO, etc.), sigla do órgão e o número da matrícula onde está "000.000/0-0"

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador;
- SIGLA DO DEPARTAMENTO:
  - Nome do departamento:
- NOME DO CARGO:
  - SIGLA DO ÓRGÃO:
    - 000.000/0-0
- Correio eletrônico;
- Telefone(s);
- Endereço.

Após a assinatura, acrescentar a mensagem da Lei nº 13.709/2018 – Lei de Geral de Proteção de Dados Pessoais (LGPD), no tamanho pequeno e fonte em itálico:

- *Esta mensagem, incluindo seu(s) anexo(s), pode conter informações privilegiadas e/ou de caráter confidencial em decorrência de relação contratual e/ou da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD), não podendo ser retransmitida sem autorização expressa do remetente. Se você recebeu esta mensagem por engano, por favor, informe-nos e apague-a; não copie ou divulgue seu conteúdo.*

Em caso de ausência prolongada por motivos diversos (férias, treinamento, licença, etc.), o colaborador deverá colocar mensagem de ausência no seu e-mail para que processos e atividades sejam conduzidos sem maiores transtornos.

O Colaborador deverá alinhar com o gestor a quem deverá ser direcionada as mensagens na sua ausência.

2.4 PADRÃO DIRETOR COM MATRÍCULA

Assinatura para uso de diretores, caso o cargo exija matrícula junto a algum órgão (ex: CRC/PR, OAB, etc.).

Não é necessário colocar o departamento, apenas o cargo em CAIXA ALTA após "DIRETOR...". Na terceira linha, coloque a sigla do órgão e o número da matrícula onde está "000.000/0-0". Caso precise colocar duas matrículas, coloque-as lado a lado, sem o cargo como no modelo abaixo.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador;
- DIRETOR...
  - SIGLA:
    - Matrícula.
- Correio eletrônico;
- Telefone(s);
- Endereço.

Após a assinatura, acrescentar a mensagem da Lei nº 13.709/2018 – Lei de Geral de Proteção de Dados Pessoais (LGPD), no tamanho pequeno e fonte em itálico:

- *Esta mensagem, incluindo seu(s) anexo(s), pode conter informações privilegiadas e/ou de caráter confidencial em decorrência de relação contratual e/ou da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD), não podendo ser retransmitida sem autorização expressa do remetente. Se você recebeu esta mensagem por engano, por favor, informe-nos e apague-a; não copie ou divulgue seu conteúdo.*

Em caso de ausência prolongada por motivos diversos (férias, treinamento, licença, etc.), o colaborador deverá colocar mensagem de ausência no seu e-mail para que processos e atividades sejam conduzidos sem maiores transtornos.

O Colaborador deverá alinhar com o gestor a quem deverá ser direcionada as mensagens na sua ausência.

2.5 PADRÃO DIRETOR SEM MATRÍCULA

Assinatura para uso de Diretores.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador;
- DIRETOR...
- Correio eletrônico;
- Telefone(s);
- Endereço.

Após a assinatura, acrescentar a mensagem da Lei nº 13.709/2018 – Lei de Geral de Proteção de Dados Pessoais (LGPD), no tamanho pequeno e fonte em itálico:

- *Esta mensagem, incluindo seu(s) anexo(s), pode conter informações privilegiadas e/ou de caráter confidencial em decorrência de relação contratual e/ou da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD), não podendo ser retransmitida sem autorização expressa do remetente. Se você recebeu esta mensagem por engano, por favor, informe-nos e apague-a; não copie ou divulgue seu conteúdo.*

Em caso de ausência prolongada por motivos diversos (férias, treinamento, licença, etc.), o colaborador deverá colocar mensagem de ausência no seu e-mail para que processos e atividades sejam conduzidos sem maiores transtornos.

O Colaborador deverá alinhar com o gestor a quem deverá ser direcionada as mensagens na sua ausência.

2.6 PADRÃO DIRETOR COM MATRÍCULA

Assinatura para uso de gestores, caso o cargo exija matrícula junto a algum órgão (ex: CRC/PR, OAB, etc.). Adequar GESTOR OU GESTORA em CAIXA ALTA. Caso seja necessário, coloque o cargo em CAIXA ALTA (ex: CONTADOR, ASSESSOR JURÍDICO, ENGENHEIRO, etc.), sigla do órgão e o número da matrícula onde está "000.000/0-0"

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador;
- GESTOR;
- SIGLA DO DEPARTAMENTO;
- Nome do departamento;
- NOME DO CARGO:
  - SIGLA DO ÓRGÃO:
  - Número da matrícula.
- Correio eletrônico;
- Nome do departamento;
- Endereço.

Após a assinatura, acrescentar a mensagem da Lei nº 13.709/2018 – Lei de Geral de Proteção de Dados Pessoais (LGPD), no tamanho pequeno e fonte em itálico:

- *Esta mensagem, incluindo seu(s) anexo(s), pode conter informações privilegiadas e/ou de caráter confidencial em decorrência de relação contratual e/ou da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD), não podendo ser retransmitida sem autorização expressa do remetente. Se você recebeu esta mensagem por engano, por favor, informe-nos e apague-a; não copie ou divulgue seu conteúdo.*

Em caso de ausência prolongada por motivos diversos (férias, treinamento, licença, etc.), o colaborador deverá colocar mensagem de ausência no seu e-mail para que processos e atividades sejam conduzidos sem maiores transtornos.

O Colaborador deverá alinhar com o gestor a quem deverá ser direcionada as mensagens na sua ausência.

2.7 PADRÃO GESTOR SEM MATRÍCULA

Assinatura para uso de gestores, adequar GESTOR OU GESTORA em CAIXA ALTA.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador;
- GESTOR;
- SIGLA DO DEPARTAMENTO;
- Nome do departamento;
- Correio eletrônico;
- Telefone(s);
- Endereço.

Após a assinatura, acrescentar a mensagem da Lei nº 13.709/2018 – Lei de Geral de Proteção de Dados Pessoais (LGPD), no tamanho pequeno e fonte em itálico:

- *Esta mensagem, incluindo seu(s) anexo(s), pode conter informações privilegiadas e/ou de caráter confidencial em decorrência de relação contratual e/ou da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD), não podendo ser retransmitida sem autorização expressa do remetente. Se você recebeu esta mensagem por engano, por favor, informe-nos e apague-a; não copie ou divulgue seu conteúdo.*

Em caso de ausência prolongada por motivos diversos (férias, treinamento, licença, etc.), o colaborador deverá colocar mensagem de ausência no seu e-mail para que processos e atividades sejam conduzidos sem maiores transtornos.

O Colaborador deverá alinhar com o gestor a quem deverá ser direcionada as mensagens na sua ausência.

2.8 PADRÃO CONSULTORES

Assinatura para uso de consultores, adequar para CONSULTOR ou CONSULTORA em CAIXA ALTA.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador;
- CONSULTOR;
- SIGLA DO DEPARTAMENTO;
- Nome do departamento;
- Correio eletrônico;
- Telefone(s);
- Endereço.

Após a assinatura, acrescentar a mensagem da Lei nº 13.709/2018 – Lei de Geral de Proteção de Dados Pessoais (LGPD), no tamanho pequeno e fonte em itálico:

- *Esta mensagem, incluindo seu(s) anexo(s), pode conter informações privilegiadas e/ou de caráter confidencial em decorrência de relação contratual e/ou da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD), não podendo ser retransmitida sem autorização expressa do remetente. Se você recebeu esta mensagem por engano, por favor, informe-nos e apague-a; não copie ou divulgue seu conteúdo.*

Em caso de ausência prolongada por motivos diversos (férias, treinamento, licença, etc.), o colaborador deverá colocar mensagem de ausência no seu e-mail para que processos e atividades sejam conduzidos sem maiores transtornos.

O Colaborador deverá alinhar com o gestor a quem deverá ser direcionada as mensagens na sua ausência.

2.9 ESTAGIÁRIO

Assinatura para o uso de estagiários, alterar para ESTAGIÁRIO ou ESTAGIÁRIA em CAIXA ALTA.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador;
- SIGLA DO DEPARTAMENTO;
- Nome do departamento;
- ESTAGIÁRIO
- Correio eletrônico;
- Telefone(s);
- Endereço.

Após a assinatura, acrescentar a mensagem da Lei nº 13.709/2018 – Lei de Geral de Proteção de Dados Pessoais (LGPD), no tamanho pequeno e fonte em itálico:

- *Esta mensagem, incluindo seu(s) anexo(s), pode conter informações privilegiadas e/ou de caráter confidencial em decorrência de relação contratual e/ou da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD), não podendo ser retransmitida sem autorização expressa do remetente. Se você recebeu esta mensagem por engano, por favor, informe-nos e apague-a; não copie ou divulgue seu conteúdo.*

Em caso de ausência prolongada por motivos diversos (férias, treinamento, licença, etc.), o colaborador deverá colocar mensagem de ausência no seu e-mail para que processos e atividades sejam conduzidos sem maiores transtornos.

O Colaborador deverá alinhar com o gestor a quem deverá ser direcionada as mensagens na sua ausência.

2.10 PADRÃO MENOR APRENDIZ

Assinatura para o uso de menores aprendizes.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador;
- SIGLA DO DEPARTAMENTO;
- Nome do departamento;
- MENOR APRENDIZ
- Correio eletrônico;
- Telefone(s);
- Endereço.

Após a assinatura, acrescentar a mensagem da Lei nº 13.709/2018 – Lei de Geral de Proteção de Dados Pessoais (LGPD), no tamanho pequeno e fonte em itálico:

- *Esta mensagem, incluindo seu(s) anexo(s), pode conter informações privilegiadas e/ou de caráter confidencial em decorrência de relação contratual e/ou da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD), não podendo ser retransmitida sem autorização expressa do remetente. Se você recebeu esta mensagem por engano, por favor, informe-nos e apague-a; não copie ou divulgue seu conteúdo.*

Em caso de ausência prolongada por motivos diversos (férias, treinamento, licença, etc.), o colaborador deverá colocar mensagem de ausência no seu e-mail para que processos e atividades sejam conduzidos sem maiores transtornos.

O Colaborador deverá alinhar com o gestor a quem deverá ser direcionada as mensagens na sua ausência.

3. Internet

Todas as regras atuais da FUNPAR visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a FUNPAR, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em arquivos privados da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação (PSI).

A FUNPAR, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor, resultando ao colaborador penalidades previstas na Consolidação das Leis Trabalhistas (CLT).

O uso de qualquer recurso para atividades ilícitas poderá acarretar em ações administrativas e penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades.

Como é do interesse da FUNPAR que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que:

- Não comprometa a banda da rede em horários estritamente comerciais;
- Não perturbe o bom andamento dos trabalhos; e
- Não implique conflitos de interesse com os seus objetivos de negócio.

Somente os colaboradores que estão devidamente autorizados a falar em nome da FUNPAR para os meios de comunicação poderão manifestar-se, seja:

- Por e-mail;
- Entrevista on-line;
- Podcast;
- Documento físico;
- Entre outros.

Apenas os colaboradores autorizados pela instituição poderão copiar, imprimir ou enviar imagens da tela para terceiros, devendo atender:

- À norma interna de uso de imagens;
- À Lei de Direitos Autorais;
- À Lei Geral de Proteção de Dados Pessoais;
- À proteção da imagem garantida pela Constituição Federal; e
- Demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em:

- Listas de discussão;
- Sites ou comunidades de relacionamento;
- Salas de bate-papo ou chat;
- Comunicadores instantâneos; ou
- Qualquer outra tecnologia correlata que venha surgir na internet.

Os colaboradores com acesso à internet não poderão fazer o download sem o apoio/supervisão da Unidade de Tecnologia da Informação (UNITIN), mesmo de programas ligados diretamente às suas atividades na FUNPAR e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas.

O uso, instalação, cópia ou distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos:

- Qualquer software não autorizado baixado será excluído pela Unidade de Tecnologia da Informação (UNITIN).

Os colaboradores não poderão em hipótese alguma utilizar os recursos da FUNPAR para fazer o download ou distribuição de software ou dados pirateados:

- Atividade considerada delituosa de acordo com a legislação nacional, ensejando penalidades previstas na Consolidação das Leis Trabalhistas (CLT).

O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias:

- Para tal, grupos de segurança, cujos integrantes deverão ser definidos pelos respectivos gestores, precisam ser criados a fim de viabilizar esse acesso especial;
- Mediante solicitação e aprovação da área técnica responsável, o uso de jogos será passível de concessão, em regime de exceção:
    - Quando eles tiverem natureza intrínseca às atividades de cursos relacionados ao desenvolvimento de jogos.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Colaboradores com acesso à internet não poderão efetuar upload de qualquer software licenciado à FUNPAR ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software, ou pelos dados, e pela Unidade de Tecnologia da Informação (UNITIN).

Os colaboradores não poderão utilizar os recursos da FUNPAR para deliberadamente propagar qualquer tipo de vírus:

- Worm;
- Cavalo de troia;
- Spam;
- Assédio;
- Perturbação; ou
- Programas de controle de outros computadores.

O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de streaming (rádios online, canais de broadcast e afins) serão permitidos a grupos específicos. Porém, os serviços de comunicação instantânea (MSN, ICQ e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisite formalmente à Unidade de Tecnologia da Informação (UNITIN).

Não é permitido acesso a sites de proxy ou de navegação anônima.

4. Identificação

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a FUNPAR e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro, art. 307:

- *Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:*
    - *Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.*

Tal norma em conjunto com o Código de Conduta e Ética da FUNPAR, visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Todos os dispositivos de identificação utilizados na FUNPAR, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (civil e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a FUNPAR e a legislação (civil e criminal) será dos usuários que dele se utilizarem.

- Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas.

A Unidade de Gestão de Pessoas (UNIGEP) da FUNPAR é a responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

A Unidade de Tecnologia da Informação (UNITIN) responde pela criação da identidade lógica dos colaboradores na instituição, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas.

- Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Os usuários deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

O funcionário receberá da Unidade de Tecnologia da Informação (UNITIN) uma senha padrão para acesso ao sistema e será de sua responsabilidade a alteração dessa senha, por uma senha pessoal de acordo com as políticas de senha.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografadas).

- Não devem ser baseadas em informações pessoais, como:
  - Próprio nome;
  - Nome de familiares;
  - Data de nascimento;
  - Endereço;

- Placa do veículo;
- Nome da empresa;
- Nome do departamento; e
- Não devem ser constituídas de combinações óbvias de teclado, como:
  - “abcdefgh”;
  - “87654321”;
  - “12345678”;
  - Entre outras.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitam que terceiros tiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é de 90 (noventa) dias, não podendo ser repetidas as 3 (três) últimas senhas.

- Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 30 dias;
- Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários, devendo ser preservadas as pastas de trabalho, franqueado acesso ao gestor responsável mediante solicitação à Unidade de Tecnologia da Informação (UNITIN).

Portanto, assim que algum usuário for demitido ou solicitar demissão, a Unidade de Gestão de Pessoas (UNIGEP) deverá imediatamente comunicar tal fato à Unidade de Tecnologia da Informação (UNITIN), a fim de que essa providência seja tomada.

- A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como, aos usuários de testes e outras situações similares.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à Unidade de Tecnologia da Informação (UNITIN) para cadastrar uma nova senha.

5. Computadores e Recursos Tecnológicos

Os equipamentos disponíveis aos colaboradores são de propriedade da FUNPAR, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como, cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da Unidade de Tecnologia de Informática (UNITIN).

- As gerências que necessitarem fazer testes deverão solicitá-los previamente à Unidade de Tecnologia da Informação (UNITIN), ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativas e atualizadas permanentemente.

- O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante envio de e-mail para Unidade de Tecnologia da Informação (UNITIN).

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio da FUNPAR (fotos, músicas, vídeos, etc.) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores.

- Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente sem prévia comunicação.

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede.

- Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de Backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os colaboradores da FUNPAR e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Unidade de Tecnologia da Informação (UNITIN).

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

- Todos os computadores de uso individual deverão ter senha de Bios para restringir o acesso de colaboradores não autorizados:
  - Tais senhas serão definidas pela Unidade de Tecnologia da Informação (UNITIN), que terá acesso a elas para manutenção dos equipamentos;
- Os colaboradores devem informar à Unidade de Tecnologia da Informação (UNITIN) qualquer identificação de dispositivo estranho conectado ao seu computador;
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da Unidade de Tecnologia da Informação (UNITIN) ou por terceiros devidamente contratados para o serviço;
- Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus:
- Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de informática;
- O colaborador deverá manter a configuração do equipamento disponibilizado pela Unidade de Tecnologia da Informação (UNITIN), seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação (PSI) e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações;
- Deverão ser protegidos por senha (bloqueados), todos os terminais de computador e impressoras quando não estiverem sendo utilizados;
- Todos os recursos tecnológicos adquiridos pela FUNPAR devem ter imediatamente suas senhas padrões (default) alteradas;
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da FUNPAR:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Acessar informações confidenciais sem explícita autorização do proprietário;
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de:
  - Atos de violação;
  - Assédio sexual;
  - Perturbação;
  - Manipulação ou supressão de direitos autorais ou propriedades intelectuais;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional;
- Criação de túneis na rede visando burlar os sistemas de segurança.

6. Dispositivos móveis

Para as atividades que exigirem maior mobilidade e necessidade de fluxo de informação entre colaboradores e/ou clientes externos, a FUNPAR permitirá o uso de dispositivo móvel, sempre com autorização do gestor.

- Quando se descreve "dispositivo móvel" entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição ou aprovado e permitido pela Diretoria e pela Unidade de Tecnologia da Informação (UNITIN), como:
  - Notebooks;
  - Smartphones; e
  - Pendrives.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores previamente autorizados que utilizem tais equipamentos.

A FUNPAR, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O colaborador autorizado, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na FUNPAR, mesmo depois de terminado o vínculo contratual mantido com a instituição.

Todo colaborador deverá realizar periodicamente cópia de segurança (Backup) dos dados de seu dispositivo móvel.

- Deverá, também, manter estes Backups separados de seu dispositivo móvel, ou seja, não os carregar juntos.

O suporte técnico aos dispositivos móveis de propriedade da FUNPAR e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico da Unidade de Tecnologia da Informação (UNITIN).

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da Unidade de Tecnologia da Informação (UNITIN).

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador, como:

- Sua casa;
- Hotéis;
- Fornecedores; e
- Clientes.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela FUNPAR, notificar imediatamente seu gestor direto e a Unidade de Tecnologia da Informação (UNITIN).

Também deverá procurar a ajuda das autoridades policiais, para registrar um boletim de ocorrência (BO).

O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracteriza a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar a FUNPAR e/ou a terceiros.

Não serão validados para uso e conexão em sua rede corporativa, quando não fornecidos ao colaborador pela instituição, dispositivo móvel, como:

- Smartphones;
- Palmtops;
- Pen drives; e
- Players de qualquer espécie.

7. Data Center

Data Center corresponde a um local físico que armazena máquinas de computação e seus equipamentos de hardware relacionados. Ele contém a infraestrutura de computação que os sistemas de Tecnologia da Informação (TI) exigem, como servidores, unidades de armazenamento de dados e equipamentos de rede, além de equipamentos de gerenciamento de energia, como fonte de alimentação ininterrupta.

O objetivo principal do Data Center é garantir a disponibilidade de equipamentos que suportem sistemas fundamentais para o funcionamento da instituição, garantindo assim a continuidade dos serviços prestados pela mesma.

Quando houver acesso às dependências dos Data Centers, este deverá ser realizado através de um forte esquema de segurança:

- O acesso ao Data Center da FUNPAR somente deverá ser feito por funcionários autorizados e deverá, sempre que possível, estar trancada com chave;
- Deverão existir duas cópias de chaves da porta do Data Center:
  - Uma das cópias ficará de posse do gestor responsável pelo Data Center;
  - A outra, de posse do gestor de Unidade de Logística e Materiais (UNILOG);
- O acesso ao Data Center, por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do Data Center for comprometida, como por:
  - Incêndio,
  - Inundação,
  - Abalo da estrutura predial,
  - Pane no sistema de refrigeração; ou
  - Quando o sistema de autenticação não estiver funcionando.

A sala de Data Center deve possuir iluminação de emergência e interruptores elétricos de emergência que permitam o desligamento em caso de necessidade.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado.

Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer colaborador responsável pela administração de liberação de acesso.

O Data Center deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração da Unidade de Logística e Materiais (UNILOG).

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno (que produz fumaça) ou inflamável no ambiente.

A entrada ou retirada de quaisquer equipamentos do Data Center somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal deste instrumento pelo responsável do Data Center.

No caso de desligamento de empregados ou colaboradores que possuam acesso ao Data Center, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de colaboradores autorizados.

8. Acesso remoto externo

Por conta da epidemia do Corona vírus, início de 2020, as empresas adotaram o sistema trabalho remoto, uma nova realidade. Portanto, após o término da pandemia, esse modelo ficou em evidência e inúmeras organizações decidiram adotá-lo, de forma definitiva ou temporária.

Para atender essa demanda, caso aconteça, a FUNPAR estabeleceu critérios para a disponibilização do serviço de acesso remoto externo à rede corporativa, bem como as regras para a sua utilização, visando à prevenção do acesso não autorizado às informações:

- Os empregados ou prestadores de serviços da FUNPAR, para o desempenho de suas atribuições, poderão ter permissão de acesso remoto aos recursos computacionais da rede corporativa da FUNPAR, quando necessário, mediante autorização prévia;
- A Unidade de Tecnologia da Informação (UNITIN) será responsável pelo processo, de orientações técnicas e a disponibilização de equipamentos de informática necessários;
- É essencial adotar algumas boas práticas para que o trabalho remoto se torne algo positivo, para isso, é necessário que o colaborador tenha disciplina de:
    - Lidar com as possíveis distrações;
    - Manter a qualidade e eficiência do serviço;
    - Cumprir as metas determinadas;
    - Controlar a jornada de trabalho;
    - Manter e cumprir as normas e políticas da Instituição;
    - Ter maturidade para administrar a sua agenda.

Cada colaborador deve manter suas credenciais de acesso (login e senha) em sigilo absoluto e não fornecê-lo a outra pessoa, garantindo assim, a impossibilidade de acesso indevido por pessoas não autorizadas.

É vedada a utilização do acesso remoto para fins não relacionados às atividades do colaborador na FUNPAR.

Não existe na legislação uma norma atribuindo ao empregador a responsabilidade de fornecer os equipamentos de trabalho e arcar com os custos de infraestrutura para o desempenho das atividades remotas.

No caso de utilização de computador pessoal para trabalho remoto, a FUNPAR não se responsabiliza pela manutenção deste, bem como não se responsabiliza pela instalação de outros softwares, como:

- Sistemas operacionais;
- Antivírus;
- Ferramentas de textos;
- Planilhas;

A FUNPAR não se responsabilizará por qualquer tipo de dano ocorrido ao computador pessoal, ainda que este esteja sendo usado no âmbito de trabalho remoto.

A FUNPAR poderá determinar horários para acesso remoto, conforme determinação das gerências e/ou diretorias, restringindo o tempo de acesso ou determinando horários comerciais para acessos remotos.

A Unidade de Tecnologia da Informação (UNITIN) somente irá liberar acesso remoto mediante autorização do Gestor da Unidade, mediante termo de autorização através de memorando interno.

A entrega do equipamento, caso tenha sido autorizada, será feita mediante assinatura de documento, termo de entrega de equipamento.

O Equipamento ao ser devolvido à FUNPAR passará por verificação pela Unidade de Tecnologia da Informação (UNITIN).

9. Backup

Todos os Backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de Backup" – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os colaboradores responsáveis pela gestão dos sistemas de Backup deverão realizar pesquisas frequentes para:

- Identificar atualizações de correção;
- Novas versões do produto;
- Ciclo de vida:
  - Quando o software não terá mais garantia do fabricante;
- Sugestões de melhorias;
- Entre outros.

Os backups (cópias de segurança) imprescindíveis, críticos, para o bom funcionamento dos negócios da FUNPAR, exigem uma regra de retenção especial conforme previsto nos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

- A classificação da informação faz parte das exigências da ISO 27001 e ISO 27002. As normas são consideradas as principais diretrizes de segurança da informação e recomenda que as informações sejam classificadas de acordo com seu valor, requisitos legais, criticidade e sensibilidade.

Na situação de erro de Backup e/ou Restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse Backup, eles deverão ser autorizados apenas mediante justificativa de necessidade nos termos do Procedimento de Controle de Backup e Restore.

Quaisquer atrasos na execução de Backup ou Restore deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Mídias de Backup:

- O procedimento de backup (cópia de segurança) pode ser descrito de forma simplificada como copiar dados em uma mídia diferente com o objetivo de posteriormente recuperar as informações, caso haja algum problema.
    - Obs.: Backup: é uma cópia de informações importantes que está guardada em um local seguro.

Testes de restauração (Restore) de Backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade.

10. Mesa e tela limpas

Uma política de mesa limpa e tela limpa envolve a remoção de todas as informações comerciais confidenciais de sua mesa todos os dias.

A política de mesas e tela limpa são práticas de segurança da informação recomendadas para o local de trabalho:

- Documentos deixados ou guardados de forma inadequada no ambiente de trabalho podem causar riscos de:
    - Violação da segurança,
    - Fraudes; ou
    - Roubo de informações.

A política de mesa limpa e tela limpa se refere a práticas relacionadas a assegurar que informações, tanto em formato digital quanto físico, e ativos não sejam deixados desprotegidos em espaços de trabalho pessoais ou públicos quando não estão em uso.

Para adotar uma Política de Mesa Limpa e Tela Limpa com sucesso, devem ser considerados os seguintes itens:

- Os documentos em papéis e mídias eletrônicas não devem permanecer sobre a mesa desnecessariamente, devem ser armazenados em armários ou gavetas trancadas quando não estiverem em uso, especialmente fora do horário do expediente;
- Informações sensíveis ou críticas para o negócio da organização devem ser trancadas em local separado e seguro (armário ou cofre à prova de fogo);
- Não devem ser deixados à mostra:
    - Sobre a mesa;
    - Colados em paredes:
    - Divisórias; ou
    - Monitor do computador:
    - Anotações;
    - Recados; ou
    - Lembretes;
- Não anotar informações sensíveis em quadros brancos e flip chart;
- Não guardar pastas com documentos sensíveis em prateleiras de fácil acesso;
- Destruir os documentos impressos antes de jogá-los fora:
    - Sempre que possível utilizar máquinas desfragmentadores;
- Documentos e impressões deverão ser descartados exclusivamente na lixeira (branca), disponibilizadas em todos os andares, para lixo confidencial;
- Leia os documentos na tela do computador, sempre que possível;
- Informações sensíveis ou confidenciais, quando impressas em local coletivo, devem ser retiradas da impressora imediatamente;
- Devolver, o quanto antes possível, todos os documentos obtidos por empréstimos de outros departamentos, quando eles não são mais necessários;
- Computadores pessoais e terminais de computador e impressoras não devem ser deixados “logados”, caso o usuário responsável não esteja presente;
- Nos computadores, utilizar um protetor de tela que solicite uma senha de acesso;
- Guardar agendas e cadernos de anotações numa gaveta ou em local seguro;

- Manter os pertences pessoais em gavetas ou armários trancados;
- Nunca deixar crachá de identificação ou chaves em qualquer lugar, mantenha-as junto a você;
- Notificar o pessoal da segurança imediatamente se seu crachá ou chaves sumirem;
- Mesas e móveis deverão ser posicionados de forma que dados sensíveis não sejam visíveis de janelas e corredores;
- Ao final do expediente ou no caso de ausência prolongada do local de trabalho, limpar a mesa de trabalho, guardar documentos, trancar as gavetas e armários e, desligar o computador;
- Não deixar as chaves na fechadura das gavetas e armários;
- A Unidade Financeira, SESMT e a ASSJUR deverão manter o ambiente de trabalho sempre fechado. A sala deverá estar trancada sempre que não houver funcionário da unidade no local.

11. Limpeza de Pastas Departamentais

A FUNPAR tem a disponibilidade de 3.14TB (Terabyte) de espaço para armazenamento de informações, arquivos:

- PDF;
- Excel;
- Word;
- Imagem;
- Banco de Dados; e
- Sistemas.

A Unidade de Tecnologia da Informação (UNITIN), em conjunto com a Unidade de Controle e Informações Gerenciais (UNICOG) monitoram periodicamente o uso da rede para que não chegue próximo do limite de desligamento total do sistema.

Fica os gestores das Unidades responsáveis pela administração desses ambientes e também pela orientação aos seus comandados pelo uso consciente das pastas departamentais.

O uso sem controle do espaço em disco acarretará em paralisação total dos sistemas Protheus e portais.

Os arquivos de uso esporádico deverão ser transportados para um local de armazenamento indicado pela Unidade de Tecnologia da Informação (UNITIN), OneDrive.

A limpeza da rede será acompanhada pela Unidade de Tecnologia da Informação (UNITIN) em conjunto com a UNICOG que fará auditorias sempre que houver necessidade e comunicará os resultados para a Gerência Geral.

- Locais de rede a serem monitorados:
  - SOFTWARE (F:);
  - PASTA DEPARTAMENTAL (G):
    - DERFI (G:);
    - UNITIN (G:) e
    - Etc.
  - SCANNER (S:);
  - PROTOCOLO (P;).

É de responsabilidade de todos o bom uso e manutenção das pastas departamentais.

04.
Da Segurança de Arquivos de Trabalho

Todos os arquivos que contiverem dados ou informações de interesse exclusivo da FUNPAR e seus clientes, deverão conter senha de proteção ou senha de gravação.

Arquivos a serem enviados por e-mail deverão ser gravados preferencialmente em Acrobat Reader e em determinadas situações devem conter senha de proteção.

Arquivos de trabalho não devem ser encaminhados para e-mails externos, inclusive e-mail pessoal, que não sejam autorizados pela FUNPAR.

05.
Adesão à LGPD

A Lei Geral de Proteção de Dados (LGPD), nº 13.709/2018, estabelece sanções para aqueles que não cumprem suas regras, que envolvem desde uma simples advertência a multas de alto valor.

Os negócios lidam com uma quantidade enorme de informações e precisam definir ações para prevenir ameaças à confidencialidade, à integridade e à disponibilidade dos dados.

- Qualquer deslize pode ocasionar sanções legais. Ou seja, é fundamental conhecer esses riscos e ter uma política para evitar ataques aos sistemas empresariais, resguardando as informações dos stakeholders, especialmente aquelas confidenciais.

Com uma política de privacidade e segurança da informação bem definida, o gestor consegue reduzir consideravelmente esses riscos. Dessa forma, a organização terá bons mecanismos de proteção contra falhas de segurança e ameaças internas.

06.
Considerações

1. Gerais

A Política de Segurança da Informação (PSI) é um documento com regras e práticas que evitam vazamentos de informações privilegiadas, invasões de sistemas e outros tipos de ataques. Uma Política de Segurança da Informação (PSI) é tão eficaz quanto o grau em que é praticada dentro da organização.

Portanto, uma boa política é aquela de fácil entendimento e acessível, atingindo e informando eficientemente todos os colaboradores.

Também é flexível e aberta a mudanças de requisitos e à evolução do negócio, além de constantemente atualizada para permanecer relevante. Afinal, as informações da sua organização devem ser preservadas e resguardadas de todas as formas possíveis.

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da FUNPAR. Ou seja, qualquer incidente de segurança subentende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

2. Finais

O presente Manual de Normas da Política de Segurança da Informação, será revisado anualmente para realização de possíveis ajustes caso necessário ou a qualquer tempo e critério, sempre que fatos supervenientes o exigirem ou recomendarem.

Toda e qualquer solicitação de alteração, mudança, ajuste, inclusão ou exclusão, deverá, inicialmente ser contatado a Unidade de Normatização de Processos - UNINOP para a elaboração do processo. Durante o andamento do processo de revisão e alteração, não é permitida a utilização da proposta solicitada.

Os responsáveis pela revisão do documento serão a Unidade de Normatização de Processos – UNINOP, Assessoria Jurídica - ASSJUR, Departamento de Administração e Finanças – DEPAFI, Departamento de Administração e Finanças – DIRAFI, Departamentos e Unidades diretamente afetadas e fornecedores das informações a serem incorporadas ou retiradas do Manual.

A autoridade concedida para aprovação deve ser exercida com responsabilidade dentro dos limites definidos e em conformidade com as Políticas Corporativas, Compliance e dos procedimentos a favor dos interesses da FUNPAR.

Quem descumprir este Manual de Normas da Política de Segurança da Informação estará sujeito às medidas legais ou disciplinares cabíveis, que serão determinadas pelos administradores competentes.

Após a conclusão da fase de aprovações e das assinaturas competentes, este Manual de Normas da Política de Segurança da Informação, deverá ser encaminhado à Unidade de Comunicação - UNICOM para a fase de diagramação, publicação e da divulgação nos canais competentes da FUNPAR.

Este Manual de Normas da Política de Segurança da Informação entra em vigor a partir da data de sua publicação e pode ser alterada a qualquer tempo, por decisão da Diretoria ou mediante o surgimento de fatos relevantes. Após publicado não será permitido o uso de normas que não estejam contemplados neste manual de políticas.

A publicação desta versão exclui automaticamente a versão anterior.

07.
Registro de Alterações

Tabela de Alterações			
Data	**Responsável**	**Função**	**Atividade**
28/02/2018	Comitê de Segurança da Informação		Elaboração - versão 1.0
16/02/2023	Marlon Meteth Ferreira da Silva	UNITIN	1ª Revisão - versão 1.1
03/06/2024	Antonio Hélio Nielsen	UNINOP	2ª Revisão - versão 1.2
04/06/2024	Marcos Cesar Miranda da Silva	DIRAFI	Aprovação da versão 1.2
04/06/2024	Marlon Meteth Ferreira da Silva	UNITIN	Análise - versão 1.2
04/06/2024	Aline Simão	UNIGEP	Avaliação da versão 1.2
05/06/2024	Rosemeiri Garanhani Bonatto Guimarães	ASSJUR	Análise - versão 1.2
05/06/2024	Fábio Miranda Borges	DEPAFI	Avaliação da versão 1.2
05/06/2024	Nilton Cesar da Rocha	UNITIN	Análise - versão 1.2


funpar