copplasa.

seu par em seguros e benefícios

diretrizes e normas administrativas

sumário

1. Objetivos 3
2. Aplicações das Diretrizes e Normas Administrativas 3
3. Das Responsabilidades Específicas 4
    3.1 – Dos Colaboradores em Geral 4
    3.2 – Dos Colaboradores em Regime de Exceção (Temporários e Prestadores de Serviços) 4
    3.3 – Dos Gestores de Pessoas e/ou Processos 4
4. Dos Custodiantes da Informação 4
    4.1 – Da Área de Tecnologia da Informação 4
5. Do Monitoramento 5
6. Correio Eletrônico 5
7. Internet 6
8. Identificação 8
9. Computadores e Recursos Tecnológicos 9
10. Dispositivos Móveis 11
11. Dispositivo Móvel Pessoal 11
12. Compartilhamentos de Arquivos Externo 12
13. Compartilhamentos de Arquivos Interno 12
14. Processo de Admissão e Desligamento 12
15. Disposições Finais 12
16. Assinatura Eletrônica 12

O Documento de Diretrizes e Normas Administrativas, é o documento que orienta e estabelece as diretrizes corporativas da Copplasa 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 Empresa.

1. Objetivos

Estabelecer diretrizes que permitam aos colaboradores da Copplasa seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de 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. Preservar as informações da Copplasa quanto à:

• **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.

2. Aplicações das Diretrizes e Normas Administrativas

As diretrizes aqui estabelecidas deverão ser seguidas por seus sócios, administradores, diretores, funcionários e colaboradores, bem como aos prestadores de serviço, obrigando-se fielmente a conduzirem as suas atividades de acordo com os mais estritos e rigorosos princípios de integridade, incluindo e não se limitando a evitar, por si e/ou por meio de terceiros, qualquer tipo de envio de dados e informações sem a prévia autorização/alinhamento da Copplasa.

Todo incidente que afete a segurança da informação deverá ser comunicado imediatamente à Gerência de TI para análise.

A Copplasa analisará qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

O não cumprimento dos requisitos previstos nesta Diretrizes e Normas Administrativas acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

3. Das Responsabilidades Específicas

3.1 – 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 Copplasa e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

3.2 – Dos Colaboradores em Regime de Exceção (Temporários e Prestadores de Serviços)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto na Diretrizes e Normas Administrativas. A concessão poderá ser revogada a qualquer tempo se for verificado que o colaborador que o recebeu não está cumprindo as condições definidas no aceite.

3.3 – 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 da política da Copplasa.

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

Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente.

4. Dos Custodiantes da Informação

4.1 – Da Área de Tecnologia da Informação

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais. Acordar com os gestores o nível de serviço que será prestado e os limites de acesso de cada colaborador.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Diretrizes e Normas Administrativas, e pelas complementares.

Os administradores e operadores dos sistemas computacionais podem, pela característica das atividades de suas funções, 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, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

Quando ocorrer movimentação interna de equipamentos, garantir que as informações do usuário serão removidas de forma irrecuperável antes de disponibilizar o equipamento para outro usuário.

Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo, garantir segurança especial para sistemas com acesso público fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

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

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

Garantir, da forma mais rápida possível, mediante solicitação formal ou ação emergencial, 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.

5. Do Monitoramento

Para garantir as regras mencionadas neste Diretrizes e Normas Administrativas, a Copplasa poderá:

• Implantar sistemas de monitoramento nas estações de trabalho, 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 Gestão de TI;

• Realizar, a qualquer tempo, inspeção física nas máquinas;

• Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

6. Correio Eletrônico

O uso do correio eletrônico da Copplasa é para fins corporativos e relacionados às atividades do colaborador (usuário) dentro da Empresa. A utilização desse serviço para fins pessoais não é permitida.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da Copplasa para:
• Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;

• Enviar mensagens 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 Copplasa ou suas unidades vulneráveis a ações civis ou criminais;

• Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem 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;

• Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades da Copplasa estiver sujeita a algum tipo de investigação;

• Produzir, transmitir ou divulgar mensagem que:
  ✓ Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Copplasa;
  ✓ Contenha ameaças eletrônicas, como: spam, vírus de computador;
  ✓ Vise obter acesso não autorizado a outro computador, servidor ou rede;
  ✓ Vise de forma premeditada interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
  ✓ Vise burlar qualquer sistema de segurança;
  ✓ Vise vigiar secretamente ou assediar outro usuário;
  ✓ Vise acessar informações confidenciais sem explícita autorização do proprietário;
  ✓ Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
  ✓ Inclua imagens criptografadas ou de qualquer forma mascaradas;
  ✓ Contenha anexo(s) superior(es) a 35 MB para envio (interno e internet) e 35 MB para recebimento (internet);
  ✓ Tenha conteúdo considerado impróprio, obsceno ou ilegal;
  ✓ Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
  ✓ Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
  ✓ Tenha fins políticos locais ou do país (propaganda política);
  ✓ Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura oficial corporativa, com o exato modelo disponibilizado pela área de Comunicação e Marketing. A utilização da assinatura corporativa é obrigatória e o colaborador deve comunicar imediatamente ao seu gestor e à área de TI, caso tenha qualquer dificuldade para adicioná-la em suas mensagens eletrônicas.

7. Internet

Todas as regras aqui estabelecidas visam um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta com a internet ofereça um grande potencial de benefícios, ela abre portas para riscos significativos para os ativos de informações.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a controle interno da área de TI. Portanto, a Copplasa, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos.

Os equipamentos, tecnologias e serviços fornecidos para o acesso à internet são ou estão sob propriedade da Copplasa, que poderá analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação que estejam armazenados em disco local, na estação de trabalho, em ambientes corporativos em nuvem ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A Copplasa, 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.

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

A internet disponibilizada pela Copplasa aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins que não prejudiquem o andamento dos trabalhos.

Como é do interesse da Copplasa 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 nem implique conflitos de interesse com os seus objetivos de negócios.

Somente os colaboradores que estão devidamente autorizados a falar em nome da Copplasa poderão nos meios de comunicações manifestar-se, seja por e-mail, entrevista on-line, podcast, documento físico, entre outros.

Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, 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 poderão fazer o download (baixa) somente de programas ligados diretamente às atividades da Copplasa, desde que autorizados pelo Gestor e/ou a área de TI.

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

Os colaboradores não poderão em hipótese alguma utilizar os recursos da Copplasa para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do Gestor e a área TI.

Os colaboradores não poderão utilizar os recursos da Copplasa deliberadamente e propagar qualquer tipo de vírus, spam, assédio, perturbação ou programas de controle de outros computadores.

8. Identificação

Os recursos de identificação e senha protegem a identidade do colaborador, evitando e prevenindo que uma pessoa se faça passar por outra perante a Copplasa e/ou terceiros. O uso de dispositivos ou senhas de identificação de outra pessoa constitui crime no Código Penal Brasileiro (art. 307 e 308– falsa identidade).

Tal norma 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 Copplasa, como o número de registro do colaborador, crachá, identificações de acesso aos sistemas, certificados e assinaturas digitais e os dados biométricos, estão associados a uma pessoa física (Colaborador) e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo uso correto perante a Copplasa e a legislação (cível e criminal), de forma que qualquer dispositivo de identificação pessoal 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 Copplasa e a legislação (cível 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. Essa regra se aplica somente aos usuários únicos onde não existe compartilhamento de logins.

A Gerência de TI responde pela criação da identidade lógica dos colaboradores, nos termos dos procedimentos 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 que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 12 (doze) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo).

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.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a Gerência TI. Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

Os usuários podem alterar a própria senha, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

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

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao Departamento de Tecnologia da Informação, 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 à área de TI.

9. Computadores e Recursos Tecnológicos

Os equipamentos disponibilizados aos colaboradores são de propriedade da Copplasa, de modo que caberá a cada colaborador utilizá-los e manuseá-los corretamente para as atividades de interesse da Copplasa, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido procedimentos de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação dos equipamentos, sem o conhecimento prévio da área de TI da Copplasa.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o TI mediante registro de chamado no suporte.copplasa.com.br

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 estiver de acordo com a classificação de tal necessidade, seja interna ou externamente.

Arquivos pessoais e/ou não pertinentes aos negócios da Copplasa tais como: (fotos, músicas, vídeos etc.) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o

armazenamento da máquina. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente e o usuário será comunicação.

Todos os documentos imprescindíveis para as atividades dos colaboradores da Copplasa deverão ser salvos no Drives corporativo na nuvem do SharePoint. 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.

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

• Os colaboradores devem informar ao departamento técnico 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 de TI da Copplasa, ou por terceiros devidamente contratados pela Copplasa para o serviço.

• É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.

• O colaborador deverá manter a configuração do equipamento disponibilizado pela Copplasa, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da empresa, assumindo a responsabilidade como custodiante de informações.

• Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.

• Todos os recursos tecnológicos adquiridos pelo Copplasa devem ter imediatamente suas senhas padrões (*default*) alteradas.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da Copplasa:
• 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);

• Interromper um serviço 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 sem a devida autorização legal do titular;

• 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.

10. Dispositivos Móveis

A Copplasa deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis. Quando se descreve "dispositivo móvel" entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua Gerência de Sistemas, como: notebooks, smartphones.

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

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

O colaborador, 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 Copplasa, mesmo depois de terminado do vínculo contratual mantido com a empresa.

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel. Por padrão o WhatsApp Business deverá ficar programado para realizar o backup diariamente na respectiva conta google.

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 de TI.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela Copplasa constituirá uso indevido do equipamento e infração.

Celular disponibilizado para colaboradores: todos os recursos corporativos como, e-mail, WhatsApp e sistemas devem ser utilizados apenas no aparelho disponibilizado pela Copplasa.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela Copplasa, notificar imediatamente seu gestor direto e a TI. Também deverá registrar o em até 24 horas o boletim de ocorrência (BO) na delegacia presencialmente.

O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará 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 Copplasa e/ou a terceiros.

11. Dispositivo Móvel Pessoal

Caso haja utilização de equipamentos/dispositivos pessoais, sob prévia autorização da gestão e da área de TI, poderão ser adotados procedimentos e aplicações corporativas de segurança que visem ampliar a proteção das informações transitadas e/ou armazenadas em tais recursos, de igual modo todos os cuidados quanto a segurança das informações deverá ser adotada pelo colaborador.

12. Compartilhamentos de Arquivos Externo

O compartilhamento externo de documentos que contenham dados/informações de pessoas só poderá ser realizado mediante a inserção de senha de criptografia. As senhas implementadas ficam sob responsabilidade do gestor de cada área.

13. Compartilhamentos de Arquivos Interno

O compartilhamento interno de documentos contendo dados de pessoas só poderá ser realizado por meio de link da nuvem corporativa (Sharepoint) e anexados como link.

14. Processo de Admissão e Desligamento

O gestor é responsável por preencher o formulário via GLPI, o sistema de chamados da Copplasa, para os processos de admissão e desligamento. É responsabilidade do gestor definir o perfil de acesso necessário para o novo colaborador, observando as diretrizes da política de segurança da informação da empresa.

Todos os acessos devem estar alinhados às funções e responsabilidades do colaborador. O departamento de TI poderá revisar e ajustar os acessos solicitados, garantindo que estejam em conformidade com os princípios de mínimo privilégio e necessidade de saber. Além disso, todos os acessos concedidos serão monitorados regularmente para garantir a segurança e a conformidade contínua.

No desligamento, o gestor deverá coletar todos os equipamentos da empresa e os cartões de acesso, entregando-os à área de TI.

15. Disposições Finais

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da Copplasa. Ou seja, qualquer incidente de segurança causado de forma intencional subtende-se como alguém agindo contra a ética e os bons costumes regidos pela empresa.

16. Assinatura Eletrônica

Documento segue na forma de assinatura eletrônica, pelo que se declara como expressão da verdade, através de seus contatos (e-mail ou telefone) informados, para dar autenticidade e reconhecer este documento com número de registro de LOG, tudo sob as penas da Lei.