

Política de Segurança da Informação

COOPERLEGIS

Sumário

1.	INTRODUÇÃO	3
2.	ATRIBUIÇÕES.....	3
3.	IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO.....	4
4.	PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO	4
5.	REGRAS DE USO DE TECNOLOGIA.....	5
6.	REGRAS DE USO DO COMPUTADOR	6
7.	REGRAS DE USO DE INTERNET.....	8
8.	REGRAS DO USO DO CORREIO ELETRÔNICO (E-MAIL).....	11
9.	REGRAS DO USO DO TELEFONE	13
10.	DISPOSITIVOS MÓVEIS.....	13
11.	MONITORAMENTO E AUDITORIA DO AMBIENTE	15
12.	CÓPIAS DE SEGURANÇA (BACKUP).....	15
13.	REDE SEM FIO (WIFI).....	16
14.	LINHAS GERAIS DE COMPORTAMENTO	17
15.	GESTÃO DE MUDANÇAS	18
16.	REVISÕES DE ACESSOS.....	18
17.	DÚVIDAS.....	18

1. INTRODUÇÃO

Ao longo do tempo os computadores tornaram-se comuns em ambientes organizacionais, e as informações antes em papéis hoje também são representadas por bits em grandes base de dados, a utilização de redes locais e remotas fazem parte no dia a dia da maioria dos colaboradores de uma empresa, dessa forma, como o acesso a informação passou a se feito também de forma lógica, a garantia da confidencialidade, integridade, disponibilidade, autenticidade e legalidade da informação, que são as propriedades que compõe a segurança da informação, que é essencial para o bom funcionamento dos negócios. Nesse contexto, a segurança da informação assumiu o papel de destaque em ambientes corporativos.

2. ATRIBUIÇÕES

Esta política tem como objetivo atender a resolução nº 4.658 do Banco Central do Brasil e estabelecer os princípios, conceitos, valores e práticas que devem ser adotados na utilização dos recursos que tangem as informações acessadas pelos Diretores, Colaboradores e Prestadores de Serviços da COOP.DE ECO.E CRED.MUTUO DOS F.DA A. LEGS.DO EST.DA PB. LTDA em João Pessoa - COOPERLEGIS na sua atuação e com o mercado.

A COOPERLEGIS incorpora em seus valores a certeza de que o exercício de suas atividades e o crescimento de seus negócios devem se basear em princípios éticos, os quais devem ser disseminados por todos os seus colaboradores. Na busca de melhoria contínua do seu desenvolvimento e da satisfação dos cooperados, a COOPERLEGIS busca transparência e cumprimento da legislação aplicável às atividades de gestão de recursos de terceiros.

A elaboração desta Política representa o compromisso dos diretores, colaboradores e prestadores de serviços que trabalham na Cooperativa com os valores e as práticas baseadas na integridade, confiança e lealdade. Portanto, a constante busca do crescimento da COOPERLEGIS e a defesa dos interesses dos associados estarão sempre relacionadas nas diretrizes aqui expostas.

A área de Controles Internos é responsável pela implementação de um sistema de supervisão que indique que os controles de segurança da informação estão sendo devidamente executados conforme os níveis adotados pela COOPERLEGIS. Logo, a área de Controles Internos está apta a constatar eventuais desvios de conduta que possam colocar em risco: cooperados, colaboradores e a COOPERLEGIS.

3. IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação é uma importante aliada na prevenção e na recuperação de incidentes de segurança, definindo critérios, normas e procedimentos seguros para proteger os ativos da informação e garantir as propriedades básicas de segurança nos sistemas de informação.

Os pilares da segurança da informação nos dão subsídio para proteger as informações da COOPERLEGIS. Portanto, quando mencionamos “segurança da informação” entende-se que estamos falando de proteções voltadas às informações impressas, verbais e sistêmicas, bem como nos controles de acesso, vigilância, contingência de desastres naturais, contratações, cláusulas e demais questões que juntas formam uma proteção adequada para qualquer empresa. (ISO 27002 A.5.1.1)

O que é Política de Segurança da Informação?

É um conjunto de diretrizes que definem formalmente as regras, os direitos e deveres de todos os colaboradores, visando à proteção adequada dos que compartilham a informação. Ela também define as atribuições de cada um dos profissionais em relação à segurança dos recursos com os quais trabalham, além disso, deve prever o que pode ser feito e o que será considerado inaceitável. (ISO 27002 A.5.1.1)

A informação é só o que está nos sistemas?

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para a organização ou pessoa. Além do que está armazenado nos computadores, a informação também está impressa em relatórios, documentos, arquivos físicos, ou até mesmo repassada através de conversas nos ambientes interno e externo.

Por isso, todo cuidado é pouco na hora de imprimir relatórios, jogar papéis no lixo, deixar documentos em cima da mesa, conversar sobre a Cooperativa em locais públicos ou com pessoas estranhas ao nosso meio. (ISO 27002 A.5.1.1)

4. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Os princípios básicos da segurança da informação são: confidencialidade, integridade e disponibilidade das informações. Outras características são: irrefutabilidade, autenticação e o controle de acesso. Os benefícios são evidentes ao reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos. (ISO 27002 A.5.1.1)

- **Confidencialidade:** Proteção da informação compartilhada contra acessos não autorizados. Ameaça à segurança acontece quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostas voluntaria ou involuntariamente dados restritos e que deveriam ser acessíveis apenas por um determinado grupo de usuários.
- **Integridade:** Garantia da veracidade da informação, pois a mesma não deve ser alterada enquanto está sendo transferida ou armazenada. Ameaça à segurança acontece quando uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações não aprovadas e sem o controle do proprietário da informação.
- **Disponibilidade:** Prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança. As ameaças à segurança acontecem quando a informação deixa de estar acessível para quem necessita dela.
- **Acesso controlado:** O acesso dos usuários à informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. Ameaça à segurança acontece quando há descuido ou possível quebra de sigilo das senhas de acesso à rede.

5. REGRAS DE USO DE TECNOLOGIA

- Os meios que permitem o acesso à informação são autorizados e disponibilizados exclusivamente para o usuário desempenhar suas funções na COOPERLEGIS ou para outras situações formalmente permitidas. (ISO A.6.1.3)
- Quando o usuário se comunicar através recursos de tecnologia da COOPERLEGIS, a linguagem falada ou escrita deve ser profissional, de modo que não comprometa a imagem da Cooperativa. (ISO A.7.1.3)
- Os conteúdos acessados e transmitidos através dos recursos de tecnologia da COOPERLEGIS devem ser legais, de acordo com o Código de Ética, e devem contribuir para as atividades profissionais do usuário. (ISO A.15.1.5)
- O uso dos recursos de tecnologia da COOPERLEGIS pode ser examinado, auditado ou verificado pela empresa, mediante autorização expressa da Diretoria, sempre respeitando a legislação vigente. (ISSO A.10.10.1)

- Cada usuário é responsável pelo uso dos recursos que lhe foram fisicamente entregues, e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas (softwares) instalados (ISO A.6.1.3)
- Os recursos de tecnologia da COOPERLEGIS, disponibilizados para os usuários, não podem ser repassados para outra pessoa interna ou externa à organização. (ISO A.6.1.3)
- Ao identificar qualquer irregularidade no recurso de tecnologia o usuário deve comunicar imediatamente à área de Controles Internos. (ISO A.13.1.1)

6. REGRAS DE USO DO COMPUTADOR

a. Propriedade do Computador

O recurso computador disponibilizado para o usuário é de propriedade da COOPERLEGIS.

b. Disponibilização e uso

O recurso computador disponibilizado para o usuário pela COOPERLEGIS tem por objetivo o desempenho das atividades profissionais desse usuário na Cooperativa. É necessário que gestor do usuário o autorize a usar o computador. Deve ser feita uma solicitação à área de Suporte de TI, que autorizará tecnicamente e fará a liberação mediante a disponibilização de recursos.

Todos os equipamentos, softwares e permissões acessos devem ser testados, homologados e autorizados pela área Gerência para o uso na COOPERLEGIS. Além disso, a COOPERLEGIS pode a qualquer momento retirar ou substituir o computador disponibilizado para o usuário.

Cada computador tem o seu gestor, que é responsável por esse equipamento. O controle das máquinas é de responsabilidade da Gerência da Cooperativa.

A identificação do usuário ao computador é feita através de login e senha disponibilizada pela gerência ou empresa responsável pela TI, portanto ela é sua assinatura eletrônica.

Os usuários que não possuem perfil de administrador 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.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # \$ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

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.

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

A periodicidade máxima para troca das senhas é 45 (quarenta e cinco) 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.

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.

c. Programas utilizados no computador

Os programas aplicativos, programas básicos, como sistema operacional e ferramentas, e componentes físicos são implantados e configurados pela área de suporte. É desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada da Gerência. Como também é desabilitado ao usuário implantar ou alterar componentes físicos no computador.

d. Verificação do computador e acessos

A COOPERLEGIS mantém por 5 (cinco) anos todos os logs de sistemas, e verifica regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam softwares, hardwares ou acessos que não sejam autorizados pela Gerência e área de Compliance.

Os acessos a equipamentos, softwares e respectivas permissões serão testados pela área de Suporte de TI com validação da área de Controles Internos a cada 6 (seis) meses.

e. Responsabilidade do usuário

Cuidar adequadamente do equipamento, pois o usuário é o custodiante deste recurso. Garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela área de Suporte de TI.

f. Outras proteções

É implantada a proteção de tela no computador e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente). Como também é implantado o “log-off” automático por inatividade durante o período de 24 (vinte e quatro) horas.

g. Termo de Compromisso

Para ter acesso à informação da COOPERLEGIS, o usuário deverá assinar (manual ou eletronicamente) um termo de compromisso. Os casos de exceção serão definidos pela Diretoria.

O Compliance da COOPERLEGIS alerta todos os usuários que a instalação ou utilização de software não autorizados constitui em crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/1998, sujeitando os infratores à pena de detenção e multa. A COOPERLEGIS não se responsabiliza por qualquer ação individual que esteja em desacordo com a Lei mencionada acima. Todas as práticas que representem ameaça à segurança da informação serão tratadas com a aplicação de ações disciplinares.

7. REGRAS DE USO DE INTERNET

a. Responsabilidade e forma de uso

O usuário é responsável por todo acesso realizado com a sua autenticação.

Todas as regras 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 COOPERLEGIS, 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 áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A COOPERLEGIS, 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 a gerência.

O uso de qualquer recurso para atividades ilícitas poderá acarretar em 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 instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos.

Como é do interesse da COOPERLEGIS 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 negócio.

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 suas atividades e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela gerência.

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. Qualquer software não autorizado baixado será excluído.

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

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.

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 (subida) de qualquer software licenciado para COOPERLEGIS ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores não poderão utilizar os recursos da COOPERLEGIS 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 on-line, canais de broadcast e afins) serão permitidos de acordo com a necessidade e autorização da gerência.

Não é permitido acesso a sites de proxy.

O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado pela Gerência.

b. Uso de serviços de mensagem instantânea

Serviços de comunicação instantânea (WhatsApp, Telegram, Facebook Messenger e afins) serão disponibilizados apenas aos usuários indicados pela gerência e poderão ser bloqueados de acordo com a necessidade da gerência.

c. Bloqueio de endereços de Internet

Periodicamente a área de infraestrutura revisará e bloqueará o acesso para os endereços da Internet que não estejam alinhados com esta Política e com o Código de Ética da Cooperativa.

8. REGRAS DO USO DO CORREIO ELETRÔNICO (E-MAIL)

a. Endereço eletrônico do usuário

A COOPERLEGIS disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais. (ex: usuario@COOPERLEGIS.com.br)

O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence à empresa, sendo assim o endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com a COOPERLEGIS. Se houver necessidade de troca de endereço, a alteração deverá ser autorizada pela Gerência e registrada para possibilitar uma posterior verificação de autoria.

b. Criação, manutenção e exclusão do endereço de correio eletrônico

A utilização desse endereço de correio eletrônico pelo usuário necessita ser autorizada pela Gerência. A liberação do endereço de correio eletrônico será feita pela Gerência de maneira controlada e segura com o objetivo de garantir que apenas o usuário tenha possibilidade de utilizar o referido endereço.

Quando acontecer desligamento de usuário, a Gerência deverá comunicar a área de Suporte de TI e bloquear o usuários das redes.

c. Acesso à distância

O usuário pode acessar o seu endereço eletrônico cedido pela COOPERLEGIS mesmo quando estiver fora do ambiente da empresa, através do serviço de correio eletrônico via internet (web mail).

d. Propriedades do endereço

O endereço de correio eletrônico disponibilizado para o usuário e as mensagens associadas a esse endereço são de propriedade da COOPERLEGIS. Em situação autorizadas pela Diretoria, as mensagens do correio eletrônico de um usuário poderão ser acessadas pela COOPERLEGIS ou por pessoas por ela indicada. Não deve ser mantida portando, expectativa de privacidade pessoal.

e. Responsabilidades e forma de uso

O usuário que utiliza um endereço de correio eletrônico é responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail, pode enviar mensagens necessários para o seu desempenho profissional na Cooperativa. É proibido criar, copiar ou encaminhar mensagens ou imagens que:

- Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
- Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais;
- Repassem prograndas ou mensagens de alerta sobre qualquer assunto. Havendo situações em que o usuário ache benéfico divulgar o assunto para a Cooperativa, a sugestão deve ser encaminhada para a Gerência, que definirá a sua publicação ou não;
- Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física;
- Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;
- Sejam susceptíveis de causar qualquer tipo de prejuízo a terceiros;
- Defendam ou possibilitem a realização de atividades ilegais;
- Possam prejudicar a imagem da COOPERLEGIS;
- Seja incoerentes com o nosso Código de Ética.

É proibido reproduzir qualquer material recebido pelo correio eletrônico ou outro meio, que possa infringir direitos de autor, marca, licença de uso de programas ou patentes existentes, sem que haja autorização expressa do autor do trabalho e da organização.

O usuário deve estar ciente que uma mensagem de correio eletrônico da COOPERLEGIS é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional em papel timbrado da entidade. Exceto quando especificamente autorizado para tal, é proibido emitir opinião pessoal, colocando-a em nome da COOPERLEGIS. Devendo sempre observar se o endereço do destinatário corresponde realmente ao destinatário desejado.

Deve ser diligente em relação:

- Aos usuários que receberão a mensagem (Destinatário/to, copiado/Cc e Copiado Oculto/Bcc);
- Ao nível de sigilo da informação contida na mensagem;
- Aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantindo a confidencialidade dos mesmos;
- Ao uso da opção Encaminhar (Forward), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.

O usuário deverá deixar mensagem de ausência quando for passar um período maior do que 48 horas sem acessar seu correio eletrônico. Essa mensagem deve indicar o período de ausência e o endereço do substituto para quem deve ser enviada a mensagem.

9. REGRAS DO USO DO TELEFONE

a. Número do telefone do usuário

A COOPERLEGIS disponibiliza telefones para utilização do usuário no desempenho de suas funções profissionais. Se houver necessidade de troca de telefone, a alteração deverá ser autorizada pela Gerência e registrada para possibilitar uma posterior verificação de autoria.

b. Propriedades do número do telefone

O telefone disponibilizado para o usuário e as conversas associadas a esse número são de propriedade da COOPERLEGIS.

c. Responsabilidade e forma de uso

O usuário que utiliza um telefone:

- É responsável por todo conteúdo da conversa;
- Pode utilizar o telefone para o seu desempenho profissional na empresa;
- É proibido utilizar o telefone para conversar que:
 - Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
 - Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, naturalidade ou deficiência física;
 - Possuam informações pornográfica, obscena ou imprópria para um ambiente profissional;
 - Defendam ou possibilitem a realização de atividades ilegais;
 - Possam prejudicar a imagem da COOPERLEGIS;
 - Sejam incoerentes com o nosso Código de Ética.

10. DISPOSITIVOS MÓVEIS

A COOPERLEGIS 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, 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 que utilizem tais equipamentos.

A COOPERLEGIS, 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, 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, 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 carregá-los juntos.

O suporte técnico aos dispositivos móveis de propriedade da COOPERLEGIS 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.

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pela gerência da COOPERLEGIS.

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 COOPERLEGIS, notificar imediatamente a gerência.

Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

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 COOPERLEGIS e/ou a terceiros.

O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da COOPERLEGIS deverá submeter previamente tais equipamentos ao processo de autorização da gerência.

11. MONITORAMENTO E AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta PSI, bem como de sua versão educacional, o COOPERLEGIS 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 dos diretores;

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.

12. CÓPIAS DE SEGURANÇA (BACKUP)

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria:

A cópia de segurança é feita de forma centralizada no ambiente dos equipamentos servidores corporativos, sob a responsabilidade da área de Suporte de TI ou empresa fornecedora do serviço;

A área de Suporte de TI ou a empresa fornecedora, fornecerá o serviço de recuperação, a partir dos arquivos de cópia de segurança, cumprindo parâmetros de nível de serviço previamente estabelecido.

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.

A gestão dos sistemas de backup deverá 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.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios, exigem uma regra de retenção especial, seguindo as determinações fiscais e legais existentes no país.

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.

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 do backup.

Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

13. REDE SEM FIO (WIFI)

O acesso à rede Wi-Fi da COOPERLEGIS somente será permitido aos funcionários e cooperados devidamente cadastrados.

O cooperado que desejar usufruir desta tecnologia, deverá solicitar as informações necessárias de acesso aos funcionários da COOPERATIVA, o usuário estará ciente e de acordo com as normas abaixo:

Não fazer passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos computacionais.

Responsabilizar-se pela sua identidade eletrônica, senha, credenciais de autenticação, autorização ou outro dispositivo de segurança.

Responder pelo mau uso dos recursos computacionais em quaisquer circunstâncias.

Responder por atos que violem as regras de uso dos recursos computacionais, estando por tanto, sujeito às penalidades legais.

O cooperado deve manter seus computadores pessoais com softwares de drivers e antivírus atualizados.

Por tratar de uma rede sem fio particular fornecida apenas para os cooperados, o acesso à internet é monitorado e terá restrições de acesso.

Se necessário, o cooperado deve procurar a COOPERATIVA para maiores esclarecimentos.

14. LINHAS GERAIS DE COMPORTAMENTO

No ambiente externo, é melhor ficar atento

Falar sobre informações restritas ou segredos profissionais em um lugar público ou por telefone merecem cuidado especial. Frequentemente, as pessoas são o elo mais fraco na segurança da informação de uma empresa.

Quando seu equipamento viajar com você, evie deixá-lo por muito tempo sozinho em uma sala ou mesa da Cooperativa. Qualquer pendrive ou conexão de rede pode conter dados valiosos.

Cuidado com o lixo que você produz

O lixo pode ser uma fonte de informações para pessoas mal intencionadas. Destrua os documentos que contenham informações sensíveis, pessoais ou da COOPERLEGIS antes de descartá-los. Se o papel que vai ser jogado no lixo contém informações que não devem ser lidas por estranhos, rasgue-o antes de jogá-lo fora.

Cuidado com senhas e acessos no sistema

Cada tarefa desenvolvida na COOPERLEGIS precisa ter um responsável. A única forma de saber o responsável por cada atividade é através da identificação do usuário. Tudo que é feito com a sua identificação (assinatura ou senha) é de sua responsabilidade. Portanto, cuidado com seus dados, seja na rede ou nos sistemas, pois sua identificação serve para garantir que você é realmente quem está usando esse acesso. Se uma outra pessoa tem acesso a sua senha, ela poderá utilizá-la para se passar por você, porém, a responsabilidade por tudo que ela fizer será sua. Alguns exemplos de ações que podem ser atribuídas a você, são:

- Liberação de ações indevidas;
- E-mails com informações inadequadas;
- Acesso a páginas da internet proibidas.

Compartilhar sua senha é como assinar um cheque em branco. É permitido apenas a utilização senhas fortes, isto é, com mais de 8 (oito) caracteres, combinando numéricos e alfanuméricos, maiúsculas e minúsculas e não utilize datas comemorativas, sobrenomes, nome do cônjuge, nome dos filhos, placas de carro, etc. Não escreva a senha em local público ou de fácil acesso.

Adote um comportamento seguro

- Não compartilhe nem divulgue sua senha a terceiros;
- Não transporte informações confidenciais da COOPERLEGIS em qualquer meio (CD, DVD, pendrive, papel, etc) sem as devidas autorizações e proteções;
- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontro sociais, etc);
- Não abra mensagens de origem desconhecida;
- Armazene e proteja adequadamente documentos impressos e arquivos eletrônicos que contém informações confidenciais;
- Siga corretamente a Política para uso de internet e correio eletrônico estabelecida pela COOPERLEGIS.

15. GESTÃO DE MUDANÇAS

A área de Suporte de TI é responsável por participar, documentar, homologar e implementar toda e qualquer alteração seja de acesso, hardware e software ou que tenha impacto direto no desenvolvimento do negócio ou operacional da COOPERLEGIS. As solicitações devem ser encaminhadas da Gerência para a área de Suporte de TI, e tais demandas devem ser registradas em sistemas para acompanhamento histórico.

16. REVISÕES DE ACESSOS

A área de Controles Internos e Suporte de TI são responsáveis por liderar anualmente os processos de revisões de acessos físicos ou lógicos de todos os colaboradores da COOPERLEGIS e propor a alteração e sua respectiva implementação.

17. DÚVIDAS

Quaisquer dúvidas relacionadas com a presente política devem ser esclarecidas com a Diretoria da COOPERLEGIS ou com a área de Controles Internos

Esta Política foi aprovada na reunião da diretoria em _____ de _____ de 2020.