

Políticas e Normas Internas de Conscientização da LGPD



Uso do Computador: A Quem se Aplica

- Esta política se aplica a todos os usuários (colaboradores e/ou terceiros) que utilizam computadores da Cergapa.

Objetivos

- Definir os requisitos e as regras de segurança para o uso de computadores no âmbito da Cergapa;
- Conscientizar os usuários de suas responsabilidades com as informações da Cergapa;
- Sugerir maneiras adequadas para o bom uso dos computadores.

Regras de Segurança de Senhas

- A senha deve conter as seguintes características mínimas listadas abaixo:
6 caracteres, contendo no mínimo letras e números.

Política de Segurança do Computador

- O computador é um **instrumento** de comunicação interna e externa para a realização do negócio da Cergapa;
- O uso do computador é **pessoal** e o usuário é responsável pelo bom uso seguindo as recomendações desta Cartilha;
- O computador é para uso **estritamente** profissional, não sendo permitida a sua utilização para outros fins, que não sejam suas atividades profissionais.

Política de Segurança do Computador

- O servidor é para uso particular com relação a sua **função na empresa**. Fica proibido o uso para armazenamento de músicas, vídeos ou arquivos particulares;
- A senha de login do computador é de uso pessoal, **intransferível** e de conhecimento exclusivo. É da inteira responsabilidade do usuário todo e qualquer prejuízo causado pelo fornecimento de sua senha pessoal a terceiros, independente do motivo;
- Cabe ao usuário **zelar** pelos equipamentos que utiliza, não sendo permitida qualquer **remoção**, desconexão de partes, substituição ou qualquer **alteração** nas características físicas ou técnicas dos equipamentos integrantes;
- A instalação de **softwares** não é permitida via regra do servidor de domínio. Quando necessário, solicitar à TI para verificar a possibilidade;
- Softwares que se instalam no perfil móvel e fogem à regra do servidor devem ser **solicitados** da mesma forma à TI;

Política de Segurança do Computador

- É atribuição da Área de TI **fiscalizar** o cumprimento desta Política sempre que for solicitado, ou quando achar necessário, e das normas vinculadas a ela, no âmbito da Cergapa, a fim de se manter a integridade das informações e de identificar situações de falha;
- Para tanto, a Cergapa se reserva no direito de **auditar** e controlar o uso dessas informações, mantendo o sigilo e evitando violações de privacidade de acordo com a LGPD - LEI N° 13.709, De 14 De Agosto De 2018.

Sobre os Dados e Backup do Usuário

- É realizado backup **diariamente** do perfil móvel, “servidor:” e diretório do setor (público);
- O perfil móvel não deve ser utilizado para armazenamento de arquivos **importantes**. O “servidor” existe para esse propósito;

Sobre os Dados e Backup do Usuário

- O perfil móvel pode ser **auditado** pela TI sem aviso prévio para preservar o ambiente de backup. Ou seja, arquivos ali dispostos podem ser **excluídos**.

Responsabilidades e Recomendações

- Ao se afastar de sua estação de trabalho, o usuário deverá tomar medidas para evitar o acesso não autorizado de terceiros ao conteúdo de seu microcomputador e aos sistemas de informação corporativos, efetuando **bloqueio** do sistema operacional;
- Ao término do horário de trabalho é dever do usuário efetuar o **desligamento** do equipamento. Para que, inclusive, sejam feitas atualizações periódicas do sistema operacional (determinadas pelo fornecedor);
- É de responsabilidade do usuário a troca de senha do login de forma **periódica**. É aconselhado a troca a cada ano (teclar CTRL + ALT + DEL, e optar pela opção “Alterar uma senha”).

Políticas em Relação a LGPD

- Por tratarmos dados pessoais de associados e funcionários acabamos enquadrados na Lei Geral de Proteção de Dados Pessoais (LGPD);
- Por este motivo temos que assegurar que estes dados sejam tratados dentro das definições ditas pela Lei;
- Desta forma algumas regras devem ser seguidas para estarmos adequados a Lei em relação ao uso da área de trabalho;
- Estar atendo no tratamento dos dados pessoais seguindo os preceitos da Lei conforme cartilha LGPD;
- Não compartilhar dados pessoais de associados ou funcionários;
- Somente usar os sistemas da Useall, ou qualquer outro, para acessar dados pessoais quando necessário o tratamento conforme definido no processo da sua função;
- Documentos PDFs contendo dados pessoais devem ser armazenados nos respectivos diretórios do setor, para evitar acesso indevido;
- Não salve no diretório público PDFs com dados pessoais para evitar que pessoas não autorizadas vejam o documento;

Políticas em Relação a LGPD

- Jamais anote dados pessoais de associados ou funcionários em Post-it e deixe-o exposto sobre a mesa;
- Armazene documentos com dados pessoais de maneira adequada para que não fique exposto à pessoas não autorizadas;
- Não utilizar documentos com dados pessoais como rascunho;
- Quando impresso documento em impressora compartilhada que contenha dados pessoais de associados ou funcionários, não esqueça o documento no local;
- Quando for impresso um documento com dados pessoais de forma equivocada, este mesmo documento deve ser picotado antes de ir para o lixo;
- Somente fornecer documentos com dados pessoais ao titular ou pessoa com vínculo com o titular (Ex.: 2º Via da Fatura).

Uso do E-Mail - A Quem se Aplica

- Esta política se aplica a todos os usuários (colaboradores e/ou terceiros) que utilizam o serviço de e-mail da Cergapa.

Objetivos

- Definir os requisitos e as regras de segurança para o uso do correio eletrônico (e-mail) no âmbito da Cergapa.
- Conscientizar os usuários de suas responsabilidades com as informações da Cergapa.
- Sugerir maneiras adequadas para o bom uso do e-mail.

Contas de E-mail: Nova, Exclusão e Bloqueio

Nova Conta de E-mail:

- Caberá ao responsável do Processo solicitar ao responsável da TI a elaboração do novo e-mail e indicar informações básicas sobre o novo usuário, tais como: nome completo, setor no qual está desempenhando suas atividades, função exercida, e justificativa da necessidade da conta;
- A TI da Cergapa efetuará o cadastro e informará ao interessado: o seu usuário, senha provisória e Política de Segurança, respondendo o chamado do responsável do setor;
- A senha deve ser confidencial, não pode ser compartilhada e obedece as regras estabelecidas no item Regras de Segurança de Senhas.

Contas de E-mail: Nova, Exclusão e Bloqueio

Exclusão de conta de e-mail:

- A exclusão de e-mail se dá no desligamento de funcionário ou em virtude da não utilização do endereço específico;

- Para que o processo seja realizado algumas etapas devem ser cumpridas:

O responsável do Processo deverá solicitar ao responsável da TI a desativação do e-mail e indicar informações básicas sobre o usuário a ser excluído, tais como: nome completo, setor no qual está desempenhando suas atividades, função exercida, e justificativa desta necessidade;

A TI da Cergapa efetuará a exclusão e informará ao interessado quando o serviço for efetivado, respondendo o chamado do responsável do setor;

Havendo necessidade técnica para a exclusão, nenhum dos passos são necessários.

Contas de E-mail: Nova, Exclusão e Bloqueio

Bloqueio da conta de e-mail:

- Por necessidade técnica ou em virtude de mal-uso por parte do usuário a conta de e-mail pode ser bloqueada por tempo indeterminado;
- Necessidade técnica entende-se por acesso não autorizada à conta, entre outras situações que venham a prejudicar a Cergapa.

Regras para Login Incorreto

- Foi ativado, por questões de segurança, o bloqueio devido a login incorreto, ou seja, o número permitido de erros consecutivos de login antes de ocorrer o bloqueio são 3 tentativas.
- A conta ficará bloqueada por uma hora.

Tempo Limite de Sessão do Login

- Com relação ao tempo de sessão para o login, também ficou estabelecido algumas regras, para evitar que a sessão do usuário permaneça com login ativo por tempo indeterminado;
- As regras abaixo são executadas pelo servidor:
 - Tempo limite da sessão ociosa: 12 horas;

Regras de Segurança de Senhas

- A senha deve conter as seguintes características mínimas listadas abaixo:
 - 8 caracteres, contendo no mínimo: 1 maiúsculo, 1 minúsculo, 1 numérico, 1 não-alfanumérico (ex.: @, \$, #, &, %.)

Política de Segurança do E-Mail

- O correio eletrônico é um instrumento de comunicação interna e externa para a realização do negócio da Cergapa;
- O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço;
- E-Mail para uso estritamente profissional, não sendo permitida a sua utilização para outros fins, que não sejam suas atividades profissionais;
- As mensagens do correio eletrônico devem ser escritas em linguagem profissional e que não comprometa a imagem da Cergapa, não vá de encontro a legislação vigente e nem aos princípios éticos da Cergapa;
- Sempre identificar a empresa, nome e setor na assinatura. Se o usuário identificar que seu e-mail está sem assinatura, deve providenciar no cadastro da assinatura ao seu respectivo endereço;
- Todos os e-mails serão passíveis de monitoramento e rastreamento para futuras auditorias;

Política de Segurança do E-Mail

- Vedado o envio de e-mails em grandes quantidades caracterizando SPAM ou LISTAS sendo os mesmos passíveis a auditoria e ações da Presidência;
- Vedado o reenvio ou, de qualquer forma, propagar mensagens em cadeia ou "pirâmides", "correntes", independentemente da vontade do destinatário de receber tais mensagens assim como, e-mails com conteúdo pornográfico e racista;
- Proibido a abertura de anexos de e-mail com as seguintes extensões: exe, com, bat, src, pif, dat, ini, sys, key e scr, por se tratarem, na maioria dos casos, de vírus ou programas maliciosos;
- O conteúdo do correio eletrônico de cada usuário pode ser acessado pela Cergapa quando em situações que ponham em risco a sua imagem, o seu negócio e/ou a segurança. Este acesso será feito a critério da Cergapa , mediante comunicação ao superior imediato do usuário, à área de TI. Procedimentos desse tipo são para evitar ataques de *phishing*, *spam's*, DDOS, ataques em massa e similares.

Direito, Deveres, Responsabilidades e Recomendações

- Verificar regularmente a sua caixa de entrada do ambiente de correio eletrônico;
- Não compartilhar a senha;
- Quando passar por um período sem acessar, deixe uma mensagem de ausência e indique quem pode ser procurado;
- Não enviar mensagens não autorizadas divulgando informações sigilosas e/ou de propriedade da Cergapa;
- Não utilizar o e-mail da empresa para assuntos pessoais;
- Adotar o hábito de leitura dos e-mails diariamente e excluir com frequência os e-mails não necessários;
- O usuário é o responsável pelas mensagens enviadas por intermédio do seu endereço de correio eletrônico;
- O mau uso de uma conta de correio por terceiros será responsabilidade de seu titular;
- É de exclusiva responsabilidade do usuário o conteúdo de seus arquivos;

Políticas em Relação a LGPD

- Por tratarmos dados pessoais de associados e funcionários acabamos enquadrados na Lei Geral de Proteção de Dados Pessoais (LGPD);
- Por este motivo temos que assegurar que estes dados sejam tratados dentro das definições ditas pela Lei;
- Desta forma algumas regras devem ser seguidas para estarmos adequados a Lei em relação ao e-mail;
- Quando à envio de documentos que contenham dados pessoais, o destinatário deve constar nos contratos de operadores da Cergapa e estar de acordo com os artigos da Lei.

Uso da Internet - A Quem se Aplica

- Esta política se aplica a todos os usuários (colaboradores e/ou terceiros) que utilizam o serviço de internet da Cergapa.

Objetivos

- Definir os requisitos e as regras de segurança para o uso da internet no âmbito da Cergapa.
- Conscientizar os usuários de suas responsabilidades com as informações da Cergapa.
- Sugerir maneiras adequadas para o bom uso da internet.

Responsabilidades Quanto ao Uso da Internet

- Todas as regras atuais da Cergapa, 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 Cergapa, 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.

Responsabilidades Quanto ao Uso da Internet

- A Cergapa, 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 as 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 nas unidades.

Responsabilidades Quanto ao Uso da Internet

- Como é do interesse da Cergapa 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.
- Somente os colaboradores que estão devidamente autorizados a falar em nome da Cergapa, para os meios de comunicação, poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por 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 LDPD, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

Responsabilidades Quanto ao Uso da Internet

- 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 responsabilidades exercidas na Cergapa e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados.
- 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 pela TI.
- Os colaboradores não poderão em hipótese alguma utilizar os recursos da Cergapa para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Responsabilidades Quanto ao Uso da Internet

- 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 a Cergapa ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável da TI.
- Os colaboradores não poderão utilizar os recursos da Cergapa 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.