POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Introdução: A CEPE depende intensamente das informações armazenadas nos seus computadores para obter sucesso nos seus negócios.

É de sua responsabilidade proteger tais informações, seguindo os procedimentos de segurança apresentados nesta política. Leia-a atentamente e, caso persista alguma dúvida, comunique-se com a Superintendência de Tecnologia da Informação e Comunicação – SUTIC, por e-mail, pessoalmente ou por ramal.

Caso você tenha subordinado verifique o cumprimento desta política pelos mesmos, inclusive terceirizados.

Atenção: A não observância das recomendações aqui descritas caracterizará infração às normas da empresa, com as consequências pertinentes.

1. Requisitos para autorização e cancelamento: Antes que possa ter acesso a qualquer sistema, um login (identificação do usuário) deve ser criado para você. Seu superior deverá providenciar para que isto seja feito junto a Gestão de Recursos Humanos que abrirá um chamado técnico para o suporte de rede. Da mesma forma, em caso de desligamento ou transferência de setor, o DERHU é responsável em informar imediatamente o fato ao suporte de rede.

2. Entrando no sistema: De posse do login, você deve se identificar ao sistema para obter acesso, abrindo uma sessão. Essa identificação é feita através do seu nome de usuário (login), juntamente com a sua senha secreta (chamada de "password"), que é apenas do seu conhecimento e será feito o cadastramento pela SUTIC onde informará ao novo usuário qual será a sua primeira senha, na qual deverá, obrigatoriamente, ser alterada após o primeiro login.

3. <u>Uso de senhas "Password":</u>

3.1 Alterar sua senha frequentemente. Quanto mais tempo você utiliza a mesma, maior o risco de alguém descobri-la, por isso a cada 30 dias será enviado um lembrete, para mudança obrigatória da mesma;

3.2 Utilizar senhas não previsíveis. Não use nomes de pessoas, lugares ou coisas que possam facilmente ser associadas a você.

3.3 Escolher senhas contendo no **mínimo** 6 caracteres **(números e letras).**

3.4 **Nunca divulgue nem anote a sua senha**. Lembre-se: sua senha é tão valiosa quanto os dados que ela protege.

4. <u>Bloqueando computador</u>: Quando se ausentar da estação de trabalho deverá encerrar ou bloquear o seu computador pressionando as teclas CTRL+ALT+DELETE para não deixar a estação liberada com o uso de terceiros.

5. <u>Uso do correio eletrônico:</u> O uso do correio eletrônico nome_do_usuario@cepe.com.br deve ser exclusivamente para atividades profissionais da CEPE.

É terminantemente proibido envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da organização.

6. <u>Uso da rede</u>:

6.1. Verificar e apagar periodicamente os arquivos antigos e sem utilização, armazenados no público.

6.2. Qualquer uso de modem em microcomputador ou conexão externa à rede da **CEPE** (fornecedores, parceiros, desenvolvedores, etc.) deverá ser aprovada pela **SUTIC**.

7. Pragas eletrônicas: Em todo microcomputador é instalado um software antivírus. Se desconfiar de qualquer arquivo que possa infectar seu computador chame **imediatamente** a **SUTIC**.

8. Internet: O acesso a Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na CEPE. Sites que **não** contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados. O uso da Internet será monitorado pela Superintendência de Tecnologia da Informação e Comunicação.

Durante a navegação na Internet, será **proibido** uso de sites que visualizem, transfiram (downloads), copiem ou qualquer outro tipo de acesso a sites: pornografia, redes sociais e de mídias (vídeos, filmes), exceto para os casos previamente autorizados e documentados.

Existem seis grupos de acesso a Internet, que são: **Básico, Intermediário, Avançado, Mídia/streaming, Mídias/sociais e Whatsapp Web**. Quaisquer mudanças de grupo será necessário a abertura de chamado técnico, justificando a necessidade, onde a partir daí será encaminhado para o gestor responsável.

9. Uso de mídias externas: É **proibido** uso de mídias externas (pendrives, CD, DVD, etc.), **para uso pessoal**, uma vez que elas são as maiores causadoras de infecções. É permitido, portanto, o uso apenas para fins profissionais.

10. Boas práticas para os usuários:

10.1. Deve-se ler esta política sempre que tiver alguma dúvida relacionada à Segurança de Informação.

10.2. Buscar sempre a orientação da equipe de tecnologia que lhe atenderá, antes de implementar novas aplicações. Observe os padrões de hardware e software adotados pela companhia.

10.3. Os setores Comercial, Marketing, Diário Oficial e Pré-Impressão devem fazer o uso do protocolo FTP (Protocolo de Transferência de Arquivos) como padrão para transferência de arquivos, uma vez que a entrega é segura e íntegra.

11. <u>Categorias de acesso web:</u> O acesso à determinada categoria é estabelecido de acordo com as atribuições funcionais.

DECLARAÇÃO DE CIÊNCIA
SOBRE SEGURANÇA DA INFORMAÇÃO

Confirmo que recebi, li e entendi **a Política de Segurança da Informação** da CEPE.

Outrossim, obrigo-me a observar fielmente as instruções/ recomendações no mesmo contidas, ciente de que violações das mesmas, por ação ou por omissão, poderão acarretar sanções de caráter cível, penal e/ou trabalhista.

Nome: _____

Departamento: _____

Matrícula: _____

Recife, _____de_____ de _____.

_____

Assinatura do Funcionário