COOPANEST.CE
COOPERANDO PARA A VIDA

MAILING – PROGRAMA DE *COMPLIANCE*

PROTEÇÃO DE DADOS

Dia 16 de janeiro estivemos na Coopanest CE tratando de algumas rotinas de segurança de dados que são importantes para que tenhamos conformidade com a Lei Geral de Proteção de Dados, que deve ter eficácia em todo território nacional a partir de agosto de 2020.

A Lei vem para assegurar que organizações se esforcem no sentido de gerir dados e dados sensíveis, porque há evidências (a partir de casos polêmicos como o escândalo do vazamento de dados do Facebook®) de que os dados podem ser usados em estratégias de manipulação.

Após nosso treinamento, achamos muito importante o registro das rotinas de proteção de dados que foram indicadas durante a apresentação, até para que sempre possam ser consultadas por todos.

- Todos os computadores precisam estar bloqueados por senhas fortes (que envolvam números, letras e símbolos);
- Sempre que se ausentar de seu equipamento, o colaborador deve fechar todos os programas ou bloquear manualmente o computador para não deixar nenhuma informação exposta, nem mesmo aos demais colegas;
- Todos os equipamentos precisam estar com sistema de firewall ou antivírus ativo;
- Os documentos devem ser guardados em ambientes seguros: sendo físicos em sala com acesso controlado; sendo digitais, em espaços digitais não expostos;
- Não se deve fornecer qualquer senha a colegas ou familiares;

- E-mails suspeitos não devem ser abertos (mesmo que tenham sido enviados por remetentes conhecidos);
- O e-mail corporativo é para uso exclusivo em interesse da Coopanest-CE. Não deve ser utilizado para cadastros pessoais dos colaboradores. Para isso, os colaboradores devem manter e-mail pessoal ativo;
- O e-mail pessoal não deve ser manuseado nas máquinas da Coopanest-CE, para que não as deixe expostas a qualquer antígeno que possa chegar pelos e-mails pessoais, como vírus;
- Redes sociais pessoais não devem ser acessados pelo computador utilizado no ambiente profissional;
- As redes sociais da Coopanest-CE só poderão ser acessadas pelo computador do setor de comunicação e marketing e/ou por pessoa formalmente autorizada;
- O *whatsapp*® não deve ser aberto no equipamento utilizado no ambiente profissional (a não ser *whatsapp*® dos celulares corporativos daqueles colaboradores que o utilizam mediante autorização expressa);
- Não devem ser utilizados *pen drives* pessoais no equipamento corporativo;
- Todos os colaboradores devem participar de treinamentos específicos quanto à proteção de dados, que serão oferecidos periodicamente por profissionais da área da tecnologia de informação;
- Todos os colaboradores devem cumprir as rotinas indicadas pelos treinadores e implementadores de processos de segurança de dados.

ÚLTIMAS LINHAS...

Vamos unir forças para que sejamos referência no quesito proteção de dados. Havendo dúvidas quanto a este *mailing* e o conteúdo do treinamento de janeiro, não deixe de fazer contato pelo Canal de Confiança!

Um abraço e até março!