MANUAL BÁSICO DE BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

Objetivo: colaborar com os funcionários, estagiários, menores aprendizes e diretoria do Grupo Bortone a proteger os dispositivos eletrônicos da empresa contra incidentes de segurança envolvendo dados pessoais.

O Grupo Bortone já possui enraizada uma atenção especial com a segurança da informação por contas da atividade empresarial realizada, mas algumas atitudes ainda são necessárias e devemos documentar àquelas jpa adotadas.

E abaixo existem algumas dicas e recomendações que a Dual Tech Informática preparou.

1. Senhas, armazenamento, alteração e assinatura eletrônica

É através de contas e senhas que os sistemas conseguem identificar quem é o usuário naquele momento em tempo real, confirmar sua identidade e definir o que cada pessoa pode ou não fazer dentro daquele programa.

Por essa razão, listamos alguns cuidados para resguardar suas credenciais:

• Use senhas bem elaboradas, com grande quantidade de caracteres e que não contenham dados pessoais como nomes, sobrenomes, datas comemorativas, números de documentos, placas de carros, números de telefones e similares. Exemplo: V6*cd72#;

• Se o sistema permitir, utilize 02 (dois) fatores de autenticação (SMS, token, e-mail, etc.);

• Mantenha sua senha segura fazendo a troca no mínimo a cada 90 (noventa) dias;

• Ative a proteção por senha ou biometria em seus dispositivos móveis e computadores;

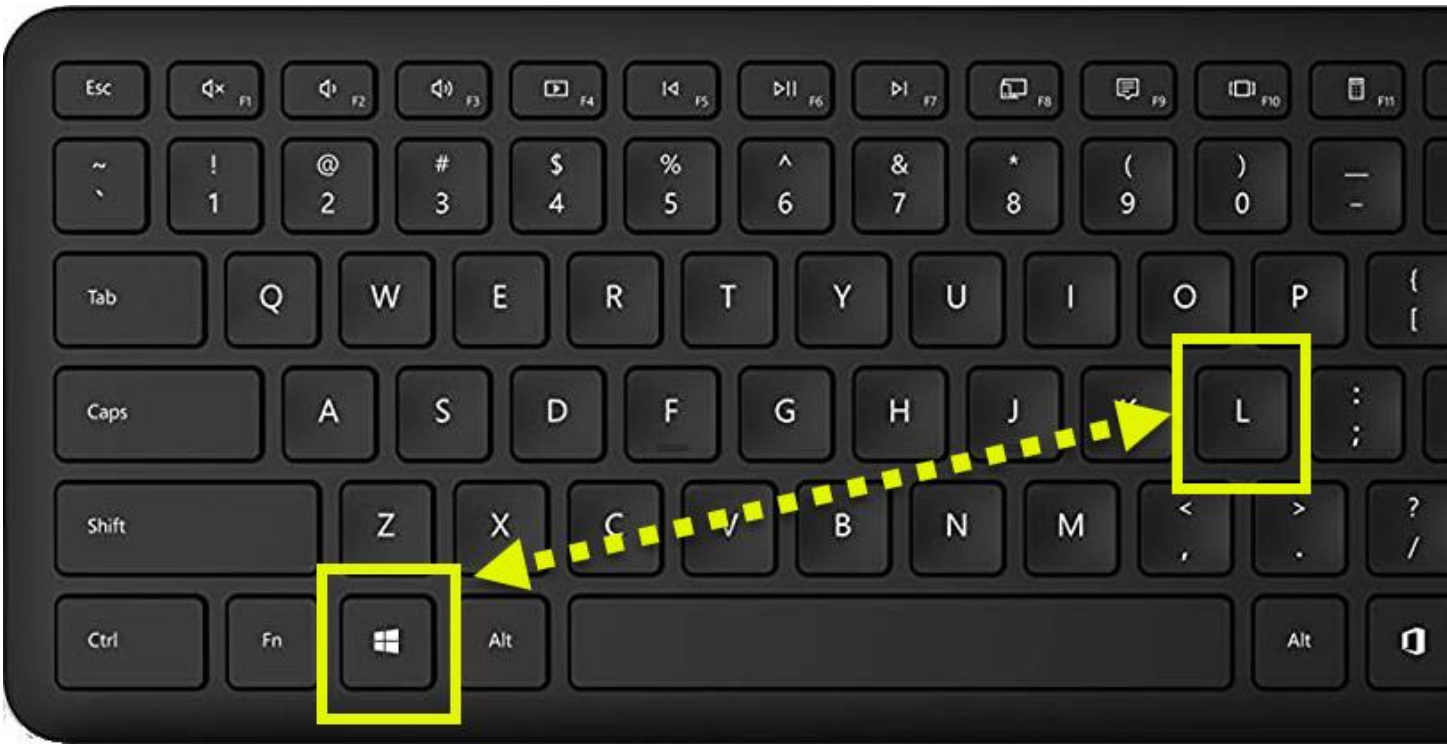
• Não anote sua senha e nem a compartilhe com outras pessoas;

3. Proteja o seu computador

Mantenha a opção de **bloqueio automático** da máquina ativo, é possível parametrizar para que isso ocorra de acordo com a sua necessidade.

Para definir o tempo de bloqueio, busque por “Alterar a proteção de Tela”, deixe a opção de nenhum selecionado, a quantidade de minutos desejada sem interação para que o bloqueio ocorra, e marque a opção "Ao reiniciar, exibir a tela de logon", depois basta aplicar e está configurado.

É possível ainda bloquear o seu usuário utilizando o conjunto de teclas: Windows + L.



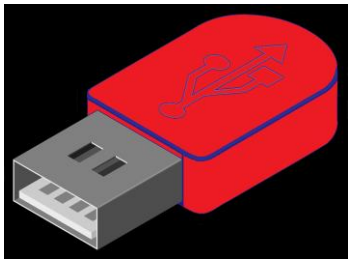
Torne isso um hábito! Saiu para pegar um café? Bloqueie a sua máquina;

OUTRAS DICAS

Na dúvida, sempre desconfie e não clique em nada: tire um print do e-mail ou link que você recebeu e envie para Dual Tech. Os golpes e fraudes na internet estão cada vez mais “perfeitos”, utilizam o nome da empresa, dados conhecidos, técnicas de engenharia social, tudo para parecer verdadeiro, por isso, nosso “desconfiômetro” deve estar sendo ativo e da mesma forma, orientar nossos colegas, caso recebam algum item suspeito;

• **Atenção redobrada para Phishing e SPAM:** Aqueles e-mails indesejáveis ou aquele pedido urgente para você preencher algum formulário e receber algo, tenha muito cuidado! Ligue o alerta ao receber um recado do gestor ou colega pedindo algo incomum, como a sua senha de acesso ao sistema. É importante também ficar atento ao clássico phishing com endereço de e-mail, ou site, que tenta imitar o real. Na dúvida, procure confirmar a solicitações com a pessoa por telefone e sempre procure nosso time de segurança (13) 4042-0997;

• **Atualização sempre!** Nada de colocar a atualização na "soneca". Antes começar a trabalhar é importante validar que todos os equipamentos e programas estão com as mais recentes atualizações de segurança;



• **Evite o uso de dispositivos externos:** Se for possível, evite ao máximo o uso de pen-drives e HDs externos, pois eles são uma grande porta de entrada para vírus e devem ser evitados;

• **Evite a perda das informações:** Mantenha os arquivos salvos nas pastas destinadas aos setores no servidor, ele possui backup diário, em vez de salvar em um diretório local da sua máquina;

• **Separe o mundo profissional x pessoal:** Costume utilizar sempre nossas ferramentas oficiais para comunicação interna ou com clientes. Não devemos utilizar por exemplo, nosso WhatsApp pessoal ou redes sociais pessoais, para atender solicitações de clientes, fornecedores, dúvidas, problemas ou falar em nome da empresa. E cuidado com as fotos tiradas no local de trabalho, pois podem conter ao fundo notas fiscais, cópias de documentos pessoais, entre outras informações

• **Não acesse sites com conteúdo pornográficos e/ou pirataria:** Sites com conteúdos pornográficos podem conter imagens não autorizadas de vítimas da invasão de privacidade, o que pode prejudicar a reputação da empresa caso a conexão seja verificada durante uma investigação criminal. E sites com pirataria de filmes, séries, entre outros materiais, geralmente, estão associados à organizações criminosas que lucram com este tipo de conteúdo e numa investigação policial, caso o IP da empresa seja indicado pela polícia, o pode prejudicar o Grupo Bortone.

Seguimos o seguinte mantra: ***"Tudo é proibido a menos que expressamente permitido"***