ORIENTAÇÕES SOBRE PRÁTICAS DE SEGURANÇA DA INFORMAÇÃO

1. Procedimentos de composição, guarda e troca de senhas

A LEV DTVM nunca entrará em contato solicitando suas senhas, dados ou outras informações confidenciais.

A composição, guarda e troca de senhas são procedimentos importantes para garantir a segurança da informação dos clientes institucionais da LEV DTVM. A seguir, apresentamos algumas recomendações de boas práticas para esses procedimentos:

- Composição de senhas: oriente os usuários a criarem senhas fortes, que incluam letras, números e caracteres especiais, com no mínimo, 8 caracteres. É importante que as senhas não contenham informações pessoais, como nome, data de nascimento, entre outros;
- Guarda de senhas: Recomendamos que os usuários não compartilhem suas senhas com outras pessoas e não as armazenem em locais de fácil acesso. Além disso, sugerimos que não anotem senhas em papéis ou documentos, já que isso facilita na perda ou roubo de dados;
- Troca de senhas: Política de troca de senhas periodicamente, a cada 90 dias. Não podendo reutilizar senhas por no mínimo 5 trocas e não ser senhas similares às anteriores;
- Utilização de gerenciadores de senhas: É uma opção para que os usuários possam manter suas senhas em segurança, permitindo que armazenem suas senhas de forma criptografada e gerem senhas fortes automaticamente.

2. Riscos envolvidos no uso da internet e métodos de prevenção

- Evite clicar em links suspeitos e sempre verifique a autenticidade do remetente antes de fornecer informações pessoais.
- Sempre que possível evite redes Wi-Fi públicas e se não for possível utilize uma Rede Privada Virtual (VPN), para garantir a segurança de seus dados.
- Mantenha seus dispositivos sempre protegidos por senha ou fatores biométricos, como por exemplo, FaceID ou impressões digitais.
- Evite utilizar aplicativos de origem desconhecida ou duvidosa; opte sempre pela utilização de aplicativos fornecidos por empresas de confiança.
- Esteja ciente de golpes de *phishing*, onde os atacantes tentam enganar os usuários para que divulguem informações pessoais por meio de e-mails falsos ou mensagens de texto
- Sempre que possível, realize backups de dados importantes, de modo que você possa recuperá-los em caso de perda ou roubo.
- Use conexões seguras, ao navegar na internet, verifique se o site está usando uma conexão segura com criptografia SSL (Secure Socket Layer)

3. Segurança e atualização em computadores e dispositivos móveis

- Mantenha o software e o sistema operacional sempre atualizados com as últimas atualizações de segurança
- Auditorias regulares: a LEV DTVM realiza auditorias regulares de segurança para garantir que as medidas de segurança sejam eficazes e que todas as informações confidenciais estejam protegidas adequadamente.
- Monitoramento de atividades de usuários: as atividades dos usuários são monitoradas para detectar atividades suspeitas ou incomuns. Isto pode ajudar a identificar possíveis ameaças de segurança e proteger informações confidenciais.
- Controle de acesso: a LEV DTVM adota um controle rigoroso de acesso, permitindo que apenas usuários autorizados tenham acesso a informações confidenciais. Os usuários têm acesso apenas aos recursos e informações que são necessários para realizar suas tarefas.
- Autenticação: os usuários precisam fornecer credenciais de autenticação para acessar informações confidenciais. Isso ajuda a garantir que somente usuários autorizados tenham acesso a essas informações.

Ao adotar estas práticas recomendadas, a LEV DTVM pode ajudar a garantir a segurança da informação de seus clientes institucionais e mitigar os riscos de acesso não autorizado a seus sistemas e informações confidenciais.

4. Proteção da confidencialidade dos dados cadastrais, operações e posição de custódia de seus clientes

A LEV DTVM utiliza controles de acesso lógico para garantir que apenas usuários autorizados tenham acesso a informações confidenciais de seus clientes institucionais. Isso inclui o uso de sistemas de autenticação forte, como o uso de senhas, tokens de segurança ou biometria, para garantir que apenas usuários autorizados possam acessar as informações.

- Criptografia: todas as informações transmitidas entre os clientes e a LEV DTVM são criptografadas para proteger a privacidade dos dados.
- Autenticação: os usuários precisam fornecer credenciais de autenticação para acessar informações confidenciais. Isso ajuda a garantir que somente usuários autorizados tenham acesso a essas informações.
- Use autenticação de dois fatores: use autenticação de dois fatores para acesso aos sistemas e plataformas online.
- Controle de acesso: a LEV DTVM adota um controle rigoroso de acesso, permitindo que apenas usuários autorizados tenham acesso a informações confidenciais. Os usuários têm acesso apenas aos recursos e informações que são necessários para realizar suas tarefas.
- Política de senha: a empresa implementa políticas de senha fortes para garantir que as senhas dos usuários sejam difíceis de adivinhar.
- Segurança física: a LEV DTVM adota medidas de segurança física para proteger as informações confidenciais dos clientes. As áreas onde as informações confidenciais são armazenadas são restritas e protegidas para evitar o acesso não autorizado.

- Monitoramento de atividades de usuários: as atividades dos usuários são monitoradas para detectar atividades suspeitas ou incomuns. Isso pode ajudar a identificar possíveis ameaças de segurança e proteger informações confidenciais.
- Treinamento de funcionários: a empresa fornece treinamento aos funcionários para garantir que eles compreendam as políticas e procedimentos de segurança e estejam cientes dos riscos de segurança.
- Auditorias regulares: a LEV DTVM realiza auditorias regulares de segurança para garantir que as medidas de segurança sejam eficazes e que todas as informações confidenciais estejam protegidas adequadamente.

Essas medidas de segurança são importantes para garantir a proteção da confidencialidade dos dados cadastrais, operações e posição de custódia dos clientes da LEV DTVM. A empresa está comprometida em manter a privacidade de seus clientes e adota medidas rigorosas para proteger suas informações.