conecta
LEUCOTRON

Cartilha de
PREVENÇÃO À INVASÃO

POLÍTICA DE SENHAS E DIREITO DE ACESSO

Leucotron
TELECOM

INTRODUÇÃO

Os recursos da PLATAFORMA CONECTA LEUCOTRON são protegidos por senhas, isso garante acesso somente a pessoas autorizadas.

Cada usuário é responsável pela manutenção e guarda de sua senha, a qual não pode ser compartilhada e não deve ser anotada em arquivos físicos ou de fácil acesso. Cabe aos usuários a memorização de suas senhas, sendo sugerida a não utilização de códigos comuns, tais como: o próprio nome, data de nascimento, nomes de parentes, números telefônicos, palavras existentes no dicionário etc.

Com relação aos parâmetros para criação da senha de acesso, todo usuário deverá utilizar senha composta de no mínimo 6 dígitos, entre letras (utilizar maiúsculas e minúsculas), números e caracteres especiais que devem ser combinados para maior proteção.

Para maior segurança, limite o acesso a interface de configuração, gerenciamento e facilidades da PLATAFORMA CONECTA LEUCOTRON e siga as dicas abaixo:

COMO MANTER UM AMBIENTE SEGURO PARA AS INFORMAÇÕES DA EMPRESA

- Crie uma política de segurança e passe para todos os usuários, enfatizando a sua importância.
- Restrinja o acesso remoto de operações e manutenção técnica somente a pessoas autorizadas. Compartilhe com elas a responsabilidade de manter em sigilo as senhas do sistema.
- Procure criar senhas de diferentes níveis para identificar, via logs, quem acessou da PLATAFORMA CONECTA LEUCOTRON.
- Mantenha os softwares de seu ambiente computacional sempre atualizados.
- Efetue periodicamente cópias de segurança (backup) e simule periodicamente a validação do processo de restauração das cópias de segurança para garantir a eficácia do procedimento.

SENHAS DE PROTEÇÃO

- Alguns elementos que você deve usar na elaboração de suas senhas são: (a) Números aleatórios - quanto mais ao acaso forem os números usados melhor, principalmente em sistemas que aceitem exclusivamente caracteres numéricos. (b) Grande quantidade de caracteres - quanto mais longa for a senha mais difícil será descobri-la. Apesar de senhas longas parecerem, a princípio, difíceis de serem digitadas, com o uso frequente elas acabam sendo digitadas facilmente. (c) Diferentes tipos de caractere - quanto mais "bagunçada" for a senha mais difícil será descobri-la. Procure misturar caracteres, como números, sinais de pontuação e letras maiúsculas e minúsculas. O uso de sinais de pontuação pode dificultar bastante que a senha seja descoberta, sem necessariamente torná-la difícil de ser lembrada.

- Uma senha boa, bem elaborada, é aquela que é difícil de ser descoberta (forte) e fácil de ser lembrada. Desta forma, evite o uso de dados pessoais, sequencias alfanuméricas, sequencias de teclado, palavras que fazem parte de listas publicamente conhecidas, como nomes de músicas, times de futebol, personagens de filmes, dicionários de diferentes

idiomas, etc. Existem programas que tentam descobrir senhas combinando e testando estas palavras e que, portanto, não devem ser usadas.

• Utilize uma frase longa que faça sentido para você, que seja fácil de ser memorizada e que, se possível, tenha diferentes tipos de caracteres. Evite citações comuns (como ditados populares) e frases que possam ser diretamente ligadas à você (como o refrão de sua música preferida). Exemplo: se quando criança você sonhava em ser astronauta, pode usar como senha "1 dia ainda verei os anéis de Saturno!!!".

• Selecione caracteres de uma frase: “Eu trabalho na LEUCOTRON há 3 anos e 1 mês”: EtnLh3ae1m.

• Faça substituições de caracteres, invente um padrão de substituição baseado, por exemplo, na semelhança visual ("w" e "vv") ou de fonética ("ca" e "k") entre os caracteres. Crie o seu próprio padrão pois algumas trocas já são bastante óbvias. Exemplo: duplicando as letras "s" e "r", substituindo "o" por "0" (número zero) e usando a frase "Sol, astro-rei do Sistema Solar" você pode gerar a senha "SS0l, asstrr0-rrei d0 SSisstema SS0larr".

• Altere as senhas sempre que ocorrer troca de pessoal responsável da PLATAFORMA LEUCOTRON e demais dispositivos relacionados.

• Evite utilizar a mesma senha para acessar diferentes plataformas e/ou dispositivos, isso pode ser bastante arriscado, pois basta ao atacante conseguir a senha de uma conta para conseguir acessar as demais contas onde esta mesma senha foi usada.

• Utilize preferencialmente senhas distintas para usos distintos, evitando repetir senhas de uso pessoal para acessos corporativos.

POSSÍVEIS CONSEQUÊNCIAS DE UMA INVASÃO

• Utilização da PLATAFORMA CONECTA LEUCOTRON para enviar mensagens sem o conhecimento da empresa.

• Destruição, visualização ou acesso a dados confidenciais.

• Risco de paralisação da PLATAFORMA CONECTA LEUCOTRON, gerando desprogramação e transtornos para a empresa.

• Acesso a PLATAFORMA CONECTA LEUCOTRON por pessoas não autorizadas que fazem uso de atividades ilícitas, escondendo sua real identidade e localização.

• Modificação de recursos e facilidades da PLATAFORMA CONECTA LEUCOTRON.

CONSIDERAÇÕES FINAIS

Fique atento aos pequenos detalhes. Segurança da informação é muito importante, por isso, faça com que sua empresa utilize os mecanismos de defesa apropriados e siga sempre as melhores práticas de mercado para proteger seu ambiente.

Também recomendamos a leitura da cartilha de marketing por mensageria (boas práticas) disponibilizada pela LEUCOTRON em relação ao uso dos módulos de software não personalizado que integram a PLATAFORMA CONECTA LEUCOTRON, disponível em: https://downloads.leucotron.com.br/conecta/cartilha-boaspraticas-mktmensageria.pdf