Instrução Normativa ConTIC-IN-05/2019, de 04 de junho de 2019

Dispõe sobre as políticas para gestão de métodos de autenticação das contas dos usuários

O Conselho de Tecnologia de Informação e Comunicação (ConTIC), no uso das atribuições conferidas pela Resolução GR Nº GR-025/2018 de 19/03/2018, com base em proposta aprovada na 122ª Reunião Ordinária do ConTIC de 22/06/2018 resolve:

Artigo 1º - Para fins desta Instrução Normativa, considera-se que:

1. Administradores de sistemas e de redes de uma Unidade/Órgão são as pessoas designadas formalmente, pela autoridade máxima da Unidade/Órgão, com atribuição principal de ser o responsável técnico pelos seus recursos de TIC;
2. CITIC: Coordenadoria Integrada de Tecnologia da Informação e Comunicação;
3. Representante de usuários de uma Unidade/Órgão é a pessoa designada formalmente, pela autoridade máxima da Unidade/Órgão, com a atribuição de representar seus usuários, nos assuntos relacionados com a utilização dos recursos de TIC da Universidade;
4. TIC: Tecnologia da Informação e Comunicação;
5. Usuário é qualquer pessoa, física ou jurídica, com vínculo formal direto ou indireto com a Unicamp, ou em condição autorizada, que utiliza, de qualquer forma, algum recurso de TIC da Unicamp.

Artigo 2º – O gerenciamento de senhas constitui o mecanismo básico para a autenticação de usuários dos sistemas computacionais da Unicamp, podendo haver a adoção de outros tão ou mais seguros que este.

Artigo 3º – As senhas das contas pessoais são confidenciais, intransferíveis e é responsabilidade do usuário mantê-la como tal, observando mecanismos de segurança e integridade. São atribuídas a cada indivíduo como um mecanismo para controlar e monitorar seu acesso a sistemas e informações e não podem ser compartilhadas com outras pessoas.

Artigo 4º – As senhas das contas institucionais ficarão vinculadas à matrícula do funcionário indicado pela autoridade máxima da Unidade/Órgão, recaindo sobre este toda a responsabilidade pelo seu uso.

Artigo 5° – Novas senhas serão fornecidas e senhas já existentes serão liberadas apenas quando a identidade do requisitante estiver assegurada.

§ 1º – O usuário será responsabilizado pelas ações de outros se, desrespeitando o Artigo 2°, deliberadamente, compartilhar sua senha e/ou acesso.

§ 2º – Senhas devem ser trocadas imediatamente em caso de suspeita de violação.

§ 3º – As senhas devem possuir no mínimo 57 bits de entropia, considerando a fórmula abaixo:

$E = \log_2(C^N)$ onde:

”E” é o número de bits da entropia;
“C” é a quantidade de caracteres possíveis baseado nos caracteres digitados. Por exemplo: somente letras minúsculas=26, letras minúsculas e números=26, letras maiusculas, minusculas e números=56;
“N” é a quantidade de caracteres digitados.

§ 4º – Senha temporária é uma senha gerada pelos administradores de sistemas e de redes para um determinado usuário e que, só é válida até o primeiro acesso autenticado bem sucedido. Podem ser entregues ao titular, ao representante de usuários da Unidade/Órgão ou a outrem por procuração registrada em cartório.

§ 5º – Em caso de esquecimento da senha, uma senha temporária pode ser fornecida eletronicamente após o solicitante fornecer informações de caráter pessoal e não públicas que permitam sua autenticação.

§ 6º – Os sistemas não devem armazenar a senha do usuário, mas sim utilizar o hash criptográfico da mesma, sendo recomendado o uso do algoritmo SHA 256 ou superior.

§ 7º – É recomendado a adoção de *listas negras* de senhas, de forma a evitar que os usuários criem senhas fáceis de serem descobertas.

§ 8º – Cabe aos administradores de sistemas e de redes adotar procedimentos de administração de senhas específicos para o seu ambiente computacional, observando estas normas.

Artigo 6º - Os casos omissos serão avaliados pela CITIC e, caso necessário, levados ao ConTIC.

Artigo 7º - Esta Instrução Normativa entra em vigor nesta data.

Prof. Dr. Sandro Rigo
Presidente do Conselho de Tecnologia de Informação e Comunicação
ConTIC / UNICAMP