I. Título

A. Nome: Instrução Normativa CITIC IN-04/2021

B. Assunto: Dispõe sobre o tratamento da Informação referente a autenticação de usuários e controle de acesso a ativos de informação e processamento

C. Número: IN-04/2021

D. Autores: Comitê de Segurança da Informação

E. Status: [ ] proposta [ ] em revisão [X] aprovada [ ] rejeitada [ ] obsoleta

F. Quando foi proposta: 2021-06-15

G. Quando foi revisada: não se aplica

H. Quando foi aprovada: 2021-11-26

I. Quando entrou em vigor: 2021-12-06

II. Definições

- **Ativo de Informação** – é o patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos da Unicamp.
- **Ativo de Processamento** – é o patrimônio composto por todos os elementos de *hardware* e *software* necessários para a execução dos sistemas de informação e processos da Unicamp, tanto os produzidos internamente quanto os adquiridos.
- **CITIC:** Coordenadoria Integrada de Tecnologia da Informação e Comunicação.
- **ConTIC:** Conselho de Tecnologia da Informação e Comunicação.
- **CSIRT UNICAMP**: do inglês, Computer Security Incident Response Team.
- **Gerentes da Tecnologia da Informação:** são os colaboradores da UNICAMP com designação de representação ativa para este papel.
- **Gestores da Informação:** são os colaboradores da UNICAMP apontados como geradores e mantenedores da informação, abrangendo desde usuários de negócio, bem como Profissionais de TIC responsáveis pelos ativos de informação e de processamento.
- **Gestores e Coordenadores:** são os colaboradores da UNICAMP com designação de representação ativa para este papel.
- **Profissional de Recursos Humanos:** são os colaboradores da UNICAMP apontados e que atuam no Departamento Pessoal.
- **UNICAMP**: Universidade Estadual de Campinas.
- **Duplo fator ou múltiplo fator de autenticação**: técnica de segurança da informação que vincula o processo de autenticação do usuário com um ou mais meios de comunicação para liberação de acesso, sendo este meio de posse exclusiva do usuário como seu celular, cartão inteligente dentre outros. Associado ao meio de comunicação geralmente emprega-se o uso de OTP (*One Time Password*), código ou senha gerado para liberar um acesso por vez num curto prazo de validade.

III. Autoridade e Responsabilidade

Todos os colaboradores apontados como Gestores da Informação, Profissionais de Recursos Humanos, Gestores e Coordenadores e Gerência da Tecnologia da Informação, detêm autoridade e responsabilidade relativas ao controle de acesso sobre os ativos de informação e processamento sob sua responsabilidade.

Responsabilidades do Gestor da Informação:

- Receber e analisar as solicitações para criação de contas de usuários para colaboradores e terceiros/prestadores de serviços.
- Autorizar a concessão e revogação de acesso aos colaboradores e terceiros/prestadores de serviços para os ativos de informação e processamento sob sua responsabilidade;
- Autorizar a concessão e revogação de acesso ADMINISTRATIVO aos colaboradores e terceiros/prestadores de serviços para os ativos de informação e processamento sob sua responsabilidade;
- Realizar a revisão periódica de autorizações e credenciais de acesso aos colaboradores e terceiros/prestadores de serviços para os ativos de informação e processamento sob sua responsabilidade e fornecendo informações sobre os privilégios atualmente efetivados em ativos/sistemas de informação.

Responsabilidades do profissional de Recursos Humanos:

- Iniciar o processo para a concessão de acesso a novos colaboradores;
- Iniciar em no máximo 48 horas úteis o processo de desligamento de servidores da UNICAMP para que contas de acesso possam ser bloqueadas/revogadas;
- Apoiar a gestão de identidades com imediata atualização, em no máximo 48 horas úteis, sobre colaboradores que mudaram de lotação física na UNICAMP;
- Apoiar a revisão de validação de credenciais de acesso a ativos / sistemas de informação fornecendo informações sobre os colaboradores.

Responsabilidades dos responsáveisl por Tecnologia da Informação:

- Receber e analisar as solicitações para criação de contas de usuários e concessão de permissões de acesso para colaboradores e terceiros/prestadores de serviços;
- Conceder o acesso aos colaboradores e terceiros/prestadores de serviço, conforme indicado pelos Gestores e Coordenadores;
- Revogar o acesso aos colaboradores e terceiros/prestadores de serviço, conforme indicado pelos Gestores e Coordenadores;
- Apoiar a revisão da validade de credenciais de acesso a ativos/sistemas de informação dos colaboradores e terceiros/prestadores de serviço fornecendo informações sobre os privilégios atualmente efetivados em ativos/sistemas de informação.

Responsabilidades dos Gestores e Coordenadores:

- Autorizar ou iniciar o processo de concessão de novos acessos a colaboradores que os necessitem conforme mudanças em suas atividades;
- Autorizar ou iniciar o processo de concessão de acesso a terceiros/prestadores de serviços contratados, justificando a necessidade de acesso a ativos/sistemas de informação e respeitando as regras e restrições de cada serviço;

- Retirar privilégios de acesso, iniciando o processo de revogação quando ocorrer mudança na equipe ou encerramento do contrato com terceiros/prestadores de serviços contratados que tenham acesso a ativos/sistemas de informação.

IV. Resumo

A política de controle de acesso complementa a Instrução Normativa ConTIC – IN - 01/2019, de 04 de junho de 2019, definindo as diretrizes para a gestão de identidade e acesso aos ativos da UNICAMP.

V. Propósito

Esta política tem o propósito de estabelecer diretrizes para gestão de identidade e acesso aos ativos de informação e de processamento, pertencentes à UNICAMP em suas várias áreas de atuação, por seus usuários autorizados.

VI. Riscos do não cumprimento

O não cumprimento desta política poderá gerar prejuízos para a UNICAMP em suas várias áreas de negócio, tais como: prejuízo financeiro decorrente do vazamento de informações estratégicas, ou intelectuais de pesquisa e inovação, e prejuízos à imagem institucional.

VII. Escopo

1. Acesso a ativos de informação e a ativos de processamento.
2. Identidade de acesso (usuário e senha) ou “conta”.
3. Autorização de acesso (perfis e permissões de acesso).
4. Clientes externos e prestadores de serviços.

VIII. Declaração da Política

1. Acesso a ativos e sistemas de informação

A UNICAMP fornecerá a seus colaboradores identidade e autorizações de acesso que permitam o uso de ativos de informação e de processamento.

As referidas identidades de acesso são fornecidas exclusivamente para que os usuários possam executar suas atividades, sendo o usuário integralmente responsável por sua utilização, respondendo por qualquer violação ou ato ilícito, mesmo que exercido por outro indivíduo e/ou organização de posse de sua identidade de acesso.

Os usuários deverão adotar medidas de prevenção para garantir o acesso seguro a ativos e serviços de informação, incluindo:

- Não anotar ou registrar senhas em locais inseguros, tais como papéis, post-it, bloco de notas e afins;
- Não utilizar sua identidade de acesso, ou tentar utilizar qualquer outra, para violar controles de segurança estabelecidos pela UNICAMP;

- Não compartilhar a identidade de acesso (usuário e senha) com outro usuário, colaborador e/ou terceiro;
- Informar imediatamente a equipe de tecnologia da informação caso identifique qualquer falha ou vulnerabilidade que permita a utilização não autorizada de ativos de informação, de processamento ou recursos computacionais da UNICAMP;
- Proteger sua identidade com recursos adicionais de segurança, como por exemplo, autenticação em dois fatores, sempre que o ambiente permitir.

O usuário será responsabilizado pelas ações de outros se, deliberadamente, compartilhar sua identidade de acesso.

Qualquer violação na utilização de identidades ou autorizações de acesso a recursos computacionais será tratada como um incidente de segurança da informação, cabendo à Gerência da Tecnologia da Informação, apoiada pelo CSIRT Unicamp, a análise e providência para solução deste incidente.

2. Credenciais de acesso

Credencial de acesso constitui-se no meio para autenticação de usuários de sistemas ou serviços computacionais da Unicamp e serão associadas aos indivíduos com vínculos junto à UNICAMP, recaindo sobre estes toda a responsabilidade pelo seu uso.

2.1. Senhas

As senhas são confidenciais, intransferíveis e é responsabilidade do usuário mantê-las 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.

As senhas das contas institucionais (relacionadas a sistemas de informação, processos de negócio) ficarão vinculadas à matrícula do funcionário indicado pela autoridade máxima da Unidade/Órgão, recaindo sobre este toda a responsabilidade pelo seu uso, enquanto manter vínculo com a Unicamp.

Novas senhas serão fornecidas apenas quando a identidade do requisitante estiver assegurada.

- Em caso de suspeita de violação, as senhas devem ser trocadas imediatamente.

- Senha temporária (ou provisória) é uma senha utilizada pelo usuário somente para possibilitar o cadastro de uma senha pessoal antes do primeiro acesso autenticado bem sucedido. Podem ser entregues ao titular, ao representante de usuários da Unidade/Órgão.

- Em caso de esquecimento da senha, uma senha nova deve ser fornecida eletronicamente somente após o solicitante fornecer informações de caráter pessoal, e não públicas, que permitam sua autenticação.

- Os sistemas não devem armazenar a senha do usuário em texto claro, mas sim utilizar o hash criptográfico da mesma, sendo mandatório o uso de algoritmo notoriamente reconhecido como seguro.

- É mandatório a adoção de critérios mínimos em relação a número de caracteres, presença de símbolos e números, e listas com palavras proibidas para a formação de senhas, evitando que os usuários criem senhas fáceis de serem descobertas.

- Sempre que possível, o responsável pela conta ou identidade de acesso deve utilizar recursos adicionais de proteção, como a autenticação com dois fatores.

- Cabe aos Gerentes da Tecnologia da Informação garantir a adoção de procedimentos de administração de senhas específicos para os ambientes computacionais sob sua gestão, observando estas normas.

A UNICAMP adota os seguintes padrões para geração de senhas de acesso a seus ativos de informação e ativos de processamento.

Ao criar uma nova senha, os usuários devem estar atentos às seguintes recomendações:

- Não utilizar nenhuma parte da sua identidade de acesso (nome de usuário) na composição da senha;
- Não utilizar qualquer um de seus nomes, sobrenomes, nomes de familiares, animais de estimação e colegas de trabalho, ou informação a seu respeito de fácil obtenção como, por exemplo, data de aniversário ou endereço;
- Não utilizar repetição ou sequência de caracteres, números ou letras;
- Não utilizar qualquer variação dos itens descritos acima como duplicação ou escrita invertida.

A Deliberação CAD-A-005/2017 instituiu para a universidade o uso da Senha Única, a fim de evitar a proliferação de distintas bases de usuários, melhorar a experiência dos usuários, promover a integração de processos e sistemas, promover a racionalização de recursos humanos e computacionais, bem como mitigar riscos à segurança da informação. Vide abaixo referências ao Portal Senha Unicamp e Autenticação Unicamp (Central), recursos derivados desta deliberação.

2.2. Outros tipos de autenticação

Além do método descrito no item 2.1, tem-se também outros métodos como múltiplo fator de autenticação, validação de identidade de acesso através de *smartcard* ou biometria entre outros. Em todos os casos mencionados, devem ser observados os métodos de segurança para armazenagem e transmissão das credenciais.

3. Autorização de acesso

A autorização de acesso aos ativos de informação ou aos ativos de processamento é feita com base em perfis, que definem o nível de privilégio dos usuários. O Gestor da Informação, Profissional de Recursos Humanos, Gestor e Coordenador ou Gerência da Tecnologia da Informação definirá as permissões baseadas nas necessidades dos usuários.

Os sistemas de informação devem tratar o ciclo de autorização de acesso, prevendo os eventos de concessão, revogação definitiva ou provisória das autorizações e mantendo registros para auditoria de cada um destes eventos.

A autorização de acesso deve considerar e distinguir acessos públicos, sem exigência de credenciais para acesso, no caso de informações para transparência por exemplo, dos acessos com obrigatoriedade de autorização.

A autorização de acesso deve contemplar os diferentes níveis ou permissões de acesso:

- apenas para consulta ou leitura;
- apenas para inclusão;
- apenas para alteração;
- apenas para exclusão lógica;
- apenas para exclusão física;
- ou uma composição destes níveis.

Neste contexto, também é necessário autorizar não somente em termos da operação que é permitida, mas também autorizar qual escopo da informação pode ser acessado, ou seja, qual o nível de detalhe da informação pode ser consultada, alterada e excluída. Exemplo: acesso somente de leitura dos dados cadastrais do funcionário, exceto dados de seus dependentes.

No caso da autorização de acesso não ser solicitada via sistema de informação, as solicitações deverão ser encaminhadas pelos gestores dos usuários aos responsáveis de cada ativo de informação ou processamento. É necessário que a solicitação possa ser recuperada para fins de auditoria e ela deve especificar claramente a necessidade, o destinatário do acesso e o prazo. E da mesma forma deve ser registrado cada uma das permissões concedidas para fins de auditoria.

3.1 Delegação de acesso

Os sistemas de informação devem prover mecanismo de delegação de controle de acesso entre os perfis de usuários do sistema para uso das funcionalidades. É imprescindível evitar o compartilhamento de senha entre usuários para que um contemple o trabalho do outro num determinado período. Exemplo: Permissão de acesso do docente para atribuir notas aos alunos da(s) sua(s) disciplina(s) é delegado para a secretária de graduação e/ou pós-graduação da sua unidade por um determinado período.

4. Clientes externos e prestadores de serviços

A criação de identidades de acesso para clientes externos e/ou prestadores de serviços se dará nos termos acima citados, observando porém, o perfil necessário ao serviço a ser realizado e o tempo pelo qual o referido acesso/serviço será executado.

Para os casos nos quais o prestador de serviços precisar conectar equipamento próprio dentro da rede da UNICAMP, o Gestor ou Coordenador será o responsável por buscar soluções junto aos **Gerentes da Tecnologia da Informação** de cada Órgão.

5. Assinatura digital

A assinatura digital, a partir do uso da infraestrutura de chaves públicas do ICP-Brasil ou do ICPEdu - RNP, é a forma efetiva de aferir a integridade de um documento eletrônico, desde a última aposição de assinatura nele, bem como confirmar indubitavelmente a identidade dos signatários envolvidos. A garantia do processo se dá tanto pelo uso de criptografia simétrica e assimétrica, bem como pela emissão da identidade digital seguindo um protocolo bem definido e controlado.

Sempre que possível os sistemas de informação e processos de negócio devem priorizar o uso de e-CPF ou e-CNPJ como meio para um ator de sistema ou processo ser signatário de uma mensagem, documento ou transação com maior legitimidade.

Os objetivos de segurança da informação obtidos são: autenticação e autorização, não repúdio, integridade dos dados e privacidade.

O Certificado Pessoal ou Jurídico do ICP-Brasil possui validade jurídica, documentos assinados com este tipo de certificado apresentam a mesma validade de um documento com firma reconhecida em cartório.

O Certificado Pessoal do ICPEdu da RNP não tem custo e é reconhecido entre as universidades públicas que participam desta iniciativa.

IX. Conformidade

A. Verificação: A UNICAMP atuará sob demanda na verificação de não conformidade do controle de acesso e, também, nos casos de não conformidade descobertos durante as atividades normais de trabalho do dia a dia.
B. Notificação:
    a. O CSIRT UNICAMP notificará os administradores de TI das Unidades/Órgãos sobre possíveis vazamentos de identidades de acesso em ativos sob sua responsabilidade;
    b. Em caso de identificação de violação ou vazamento, o CSIRT UNICAMP deverá ser notificado;
    c. Em casos omissos, a CITIC deverá ser notificada.

C. Remediação: Nos casos em que forem identificados vazamento de identidades de acesso, às autoridades relacionadas poderão suspender temporariamente qualquer identidade de acesso, sempre que julgarem necessário para a preservação da integridade dos ativos de informação e processamento, mediante justificativa escrita devidamente fundamentada e aprovada pela CITIC; nos demais casos de não conformidade o responsável deverá se adequar às normas vigentes.

X. Referências

1 - ConTIC–IN-01/2019
https://www.citic.unicamp.br/sites/default/files/normas/ConTIC-IN-01%202019%20-%20normas_uso_TIC.pdf

2 - Deliberação CAD-A-005/2017

https://www.pg.unicamp.br/mostra_norma.php?id_norma=9149

3 - Portal Senha Unicamp
https://www.unicamp.br/senhaunicamp/

4 - Autenticação Unicamp (Central)
https://www.ccuec.unicamp.br/ccuec/servicos/autenticacao-centralizada

5 - Certificado Pessoal ou Jurídico do ICP-Brasil - por exemplo:
https://certificadodigital.imprensaoficial.com.br/governo/como-comprar

6 - Certificado Pessoal do ICPEdu da RNP:
https://pessoal.icpedu.rnp.br/home

Documento assinado eletronicamente por **Ricardo Dahab**, **DIRETOR GERAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO**, em 10/12/2021, às 11:53 horas, conforme Art. 10 § 2º da MP 2.200/2001 e Art. 1º da Resolução GR 54/2017.

A autenticidade do documento pode ser conferida no site: sigad.unicamp.br/verifica, informando o código verificador:
4FA8DFD6 5B31451C 969997FD B43146EF

UNICAMP
SIGAD