INSTRUÇÃO NORMATIVA

CCUEC *Nº 01/2011, DE 04 DE NOVEMBRO DE 2011*

Define conceitos e estabelece regras e procedimentos para a utilização do serviço de diretório oferecido pelo CCUEC. ***(Atualizada em 24/08/2017)***

O Superintendente do CCUEC - Centro de Computação da UNICAMP, no uso de suas atribuições e, considerando a necessidade de:

- disponibilizar o serviço de diretório para autenticação via protocolo LDAP,
- definir conceitos e terminologias usados no serviço de autenticação e
- definir a abrangência deste serviço,

resolve:

- estabelecer regras, critérios e procedimentos para o uso do serviço de diretório para autenticação LDAP oferecida pelo CCUEC.

1 - INTRODUÇÃO

O Centro de Computação oferece aos órgãos da UNICAMP um serviço de diretório para autenticação, permitindo os seguintes usos:

- autenticação de Sistemas de Informação;
- autenticação de serviços de internet e intranet;
- autenticação para equipamentos de rede (autenticadores), como switches, controladores e pontos de acesso para rede sem fio (Wi-Fi);
- disponibilização para outros serviços de autenticação, como por exemplo, servidor baseado no protocolo RADIUS;
- outros usos, mediante a consulta.

2 - CONCEITOS E TERMINOLOGIAS

Para fins desta Instrução, consideram-se os seguintes conceitos e terminologias.

2.1.**Autenticação** - processo para reconhecimento da identidade digital do usuário, baseado em um par de credenciais (username e senha).

2.2.**LDAP -** Lightweight Directory Access Protocol - É um protocolo de aplicação utilizado para acesso e manutenção de um diretório de informações em uma rede IP.

2.3.**RADIUS** - Remote Authentication Dial In User Service – protocolo para autenticação, autorização e *accounting* (AAA), utilizado no controle de acesso à rede.

2.4.**DGRH** – Diretoria Geral de Recursos Humanos.

2.5.**DAC** – Diretoria Acadêmica.

2.6.**Funcamp** – Fundação de Desenvolvimento da Unicamp.

2.7.**TIC** - Tecnologia da Informação e Comunicação

2.8.**Máquina cliente**: é a máquina que enviará solicitação de autenticação para o servidor LDAP e que obterá, em caso de sucesso, algumas informações básicas relacionadas às credenciais enviadas.

3 - Regras e Procedimentos para a Utilização do Serviço de Diretório

3.1 Este serviço está disponível para as Unidades, Órgãos, Centros e Núcleos da Unicamp e para a Funcamp, os quais são chamados simplesmente "órgãos" neste documento.

3.2 Para utilizar o serviço de diretório será necessário formalizar uma solicitação por meio de ofício ao CCUEC assinado pelo dirigente do órgão. Neste ofício deverá ser indicado o contato técnico com o qual o CCUEC tratará a implementação do serviço (administrador de redes ou outro representante do órgão).

3.3. O Centro de Computação disponibilizará as instruções necessárias para permitir a autenticação no serviço de diretório.

3.4. Os serviços solicitados no ofício e autorizados terão acesso ao seguinte conjunto de atributos corporativos, descritos em detalhes no Anexo1:

- dn, uid, employeeNumber, employeeType, cn, sn, ou, departmentNumber, shadowFlag, givenName, objectClass.

3.4.1. O acesso a qualquer outro atributo corporativo somente será liberado por meio de um acordo a ser assinado entre o órgão solicitante, o CCUEC e o responsável pela informação, que pode ser a DGRH, DAC ou Funcamp.

3.4.2. Não será permitido acesso ao atributo de senha *userPassword***.**

3.5. O acesso de autenticação ao Serviço de Diretório do Centro de Computação somente será feito por meio de um canal de comunicação seguro com apoio criptográfico.

3.5.1 É de responsabilidade do responsável da unidade que a autenticação entre usuário final e o serviço e/ou aplicação da unidade seja feita por meio de conexão segura (conforme descrito no item 3.5)

3.6. Não é permitida em nenhuma hipótese, a disponibilização de dados do diretório a terceiros sem a prévia autorização do CCUEC.

3.7. O serviço só será disponibilizado depois do aceite/assinatura do Termo de Compromisso com o Sigilo dos Dados do Serviço de Diretório Corporativo da Unicamp pelo representante indicado pela direção do órgão solicitante.

4 - Competência e Responsabilidades

4.1. Cabe ao dirigente do órgão solicitar ao CCUEC, o uso do serviço de diretório.

4.2. É de responsabilidade do CCUEC viabilizar o acesso ao serviço de diretório, mediante a conformidade da solicitação com esta instrução normativa.

4.3. O CCUEC é o responsável pela administração do serviço de diretório corporativo.

4.4. O CCUEC envidará todos os esforços no sentido de disponibilizar este serviço de autenticação em regime 24 X 7, mas ressalta que interrupções poderão ocorrer por motivos de força maior.

4.5. Cabe ao CCUEC disponibilizar as instruções necessárias para o acesso ao serviço de diretório.

4.6. O órgão deve prover as instalações/configurações de hardware e software recomendadas pelo CCUEC, para acesso ao Serviço de Diretório.

4.7. O órgão se compromete a manter as versões de softwares das máquinas clientes atualizadas conforme recomendação do CCUEC.

4.8. O órgão deve ter controle de segurança física, operacional e de acesso à máquina cliente.

4.9. No caso de incidente de segurança que envolva a máquina cliente, o órgão deverá permitir a realização de auditoria por parte do CCUEC, quando esta for solicitada.

5. Considerações Finais

As informações armazenadas nos atributos dos pacotes do serviço de diretório que são provenientes das tabelas públicas da DGRH, RH-Funcamp e DAC, são mantidas por estes órgãos e replicadas no diretório assim que detectados pelos sistemas do CCUEC, podendo haver um intervalo de tempo entre uma alteração de dados e sua disponibilização no diretório.

Anexos

Anexo 1 da Instrução Normativa CCUEC *nº 01/2011, de 04 de novembro de 2011*

Anexo 2 - Termo de Compromisso com sigilo de dados no serviço de diretório corporativo da Unicamp da Instrução Normativa CCUEC *nº 01/2011, de 04 de novembro de 2011*

Esta Instrução Normativa entra em vigor a partir desta data.

Prof. Sandro Rigo
Superintendente do Centro de Computação
UNICAMP

ANEXO 1 DA INSTRUÇÃO NORMATIVA CCUEC *Nº 01/2011, DE 04 DE NOVEMBRO DE 2011*

DESCRIÇÃO DOS ATRIBUTOS DO PACOTE BÁSICO E LINUX

dn:(*Distinguished Name)*	O DN é um conjunto de pares "atributo=valor" usado para definir entradas sem ambiguidade no serviço de diretório. Exemplo: dn: uid=fulano, ou=people, dc=unicamp, dc=br
uid:	É o nome de login que identifica um usuário
objectClass:	Especifica a classe de objeto da entrada. A classe define quais atributos ou *schema*'s são permitidos ou obrigatórios para a entrada. Exemplo: objectClass: person
departmentNumber:	Contém o código (em 7 níveis) da unidade de lotação do funcionário da Unicamp, Funcamp e da unidade de ensino dos alunos.
employeeNumber:	Matrícula na DGRH, quando funcionário da Unicamp, matrícula na Funcamp, quando funcionário da Funcamp, e RA na DAC, quando for aluno.
employeeType:	atributo multivalorado (Funcionário Unicamp, Funcamp, estagiário, Funcamp-Bolsista, aluno Unicamp)
ou:	Atributo multivalorado que identifica o vínculo do usuário, contendo a primeira ocorrência da sigla do órgão (para funcionários) ou da unidade de ensino (para alunos)
cn:*(Common Name)*	Nome completo do usuário
sn:(*Surname)*	Último sobrenome do usuário obtido no atributo LDAP "cn" da classe de objeto "Person"
givenName:	Primeiro nome obtido do atributo LDAP "cn" da classe de objeto "Person"
shadowFlag:	Corresponde à situação do username do usuário (1-ativo, 2-senha expirada, 3-Inativo)

ANEXO 2 DA INSTRUÇÃO NORMATIVA CCUEC *Nº 01/2011, DE 04 DE NOVEMBRO DE 2011*

TERMO DE COMPROMISSO COM O SIGILO DOS DADOS DO SERVIÇO DE DIRETÓRIO CORPORATIVO DA UNICAMP

Eu,_____, matrícula _____ ( ) Unicamp ( ) Funcamp, lotado no (Órgão/Departamento) _____ na Função de _____, assumo o compromisso de assegurar o sigilo dos dados do Serviço de Diretório Corporativo da UNICAMP que serão disponibilizados a partir desta data pelo Centro de Computação, com a autorização das unidades titulares dos mesmos (DGRH, FUNCAMP e DAC), para os sistemas de informática sob minha responsabilidade abaixo descritos.

Estou ciente e de acordo com a normativa de uso do Serviço de Diretório que está no link:
http://www.ccuec.unicamp.br/ccuec/sites/default/files/tutoriais/instrucaonormativa_LDAP_2011_11_04.PDF

Computador(es) autorizado(s) a acessar o serviço:

nome de domínio completo	endereço IP	principal finalidade
_____	_____	_____
_____	_____	_____
_____	_____	_____

Por meio deste termo comprometo-me a

- não divulgar a terceiros ou a sistemas que não estejam relacionados neste termo as informações do Serviço de Diretório sem consentimento por escrito do Centro de Computação;
- informar ao Centro de Computação toda e qualquer mudança neste Termo ou no(s) computador(es) que acessa(m) os dados do Serviço de Diretório Corporativo em um prazo de pelo menos (3) três dias úteis antes da efetivação da mudança.

Campinas, ___ de _____ de 20___.

_____