NORMA CTI – SEGURANÇA DA INFORMAÇÃO

Estabelece as regras e procedimentos para a segurança e integridade das informações da UNIVATES, no que diz respeito às operações com o uso de recursos de Tecnologia da Informação

SUMÁRIO

1 FINALIDADE

Estabelecer as regras e os procedimentos para a segurança e integridade das informações da UNIVATES, no que diz respeito às operações com o uso de recursos de TI, de acordo com o prescrito nas Diretrizes de Segurança e Integridade de Informações constantes do documento Diretrizes Gerais para uso dos recursos de Tecnologia da Informação da UNIVATES (DIR- TI- REITORIA).

2 ÂMBITO DE APLICAÇÃO

Este documento tem aplicação na UNIVATES, em todos os seus setores e para todos os usuários dos serviços de TI.

3 SEGURANÇA OPERACIONAL

Os itens abaixo tratam dos requisitos indispensáveis para a correta autenticação dos usuários, habilitando os mesmos a utilizar os sistemas de informação da UNIVATES, sendo a sua utilização passível de ser auditada.

3.1 Usuários

São considerados usuários:

1. Alunos regularmente matriculados nos cursos de Graduação, Pós Graduação, Técnicos e Extensão;

2. Egressos → alunos formados, até 365 dias depois da conclusão do curso;

3. Professores contratados CLT;

4. Integrantes do Corpo Técnico – Administrativo;

5. Estagiários do Corpo Técnico – Administrativo e da área acadêmica;

6. Bolsistas da UNIVATES e de convênios externos;

7. Terceiros, prestadores de serviços à UNIVATES, que necessitem acesso aos recursos de TI;

8. Visitantes que participarão de alguma atividade da UNIVATES, atividade essa que necessite acesso aos recursos de TI;

9. Comunidade → outros usuários da biblioteca e de laboratórios de informática, mediante comprovação de pagamento da taxa de serviço, pelo período acordado.

Obs.: Terão tratamento especial outros casos não enquadrados anteriormente, a critério da Pró-reitoria envolvida

Os direitos de acesso de cada papel, função exercida pelo usuário em determinado momento, estão definidos nas Normas de Acesso à Rede.

3.2 Identificadores

O identificador do usuário ("userid") deve permitir reconhecer a sua identidade, mas nunca os seus níveis de privilégio.

Para isso deverá ser utilizado um identificador com as seguintes regras de construção:

a) Será formado por no máximo “40” caracteres (alfanuméricos) segundo a regra: “nome.sobrenome”;

Observação.:

1. A partícula “sobrenome” será o último nome de família;

2. Em caso de homônimos, deverá ser acrescentado um numeral correspondente ao nível de coincidência ocorrido;

3. Casos de combinações “nome.sobrenome” que possibilitem interpretações

de duplo sentido ou pejorativas, deverão ser tratados pontualmente pelo Coordenador do NTI, mediante solicitação da pessoa interessada;

4. Os identificadores em uso serão gradativamente convertidos para esta regra, ou a qualquer momento por solicitação do interessado.

b) O identificador deve ser pessoal, intransferível e único para todos os sistemas.

c) Os identificadores pertencentes a usuários que forem desligados de suas funções não deverão ser atribuídos a outros usuários.

3.3 Senha (Password)

A senha, juntamente com o identificador do usuário (userid), autentica o usuário e habilita o acesso aos sistemas, de acordo com seus direitos de acesso (papel).

O NTI, como fiel depositário das senhas, deverá resguardar o sigilo das mesmas, armazenando-as, criptografadas, em suporte magnético.

Regras de construção:

a) As senhas são pessoais e intransferíveis, sendo de responsabilidade do usuário assegurar que a sua senha seja secreta e que não seja conhecida por mais ninguém;

b) As senhas fornecidas por padrão, na criação de um novo usuário ou implantação de um sistema ou aplicação, deverão ser imediatamente alteradas pelo usuário, garantindo sua privacidade;

c) A escolha da senha é a critério do usuário, ficando este, no entanto, obrigado a cumprir com as normas de construção de uma senha segura, descritas na página de recadastro (www.univates.br/recadastro). A segurança da senha será testada automaticamente, quando da alteração da senha;

d) A Área de TI deve implementar mecanismos que limitem o número de tentativas consecutivas de falhas de autenticação, após o que o identificador deve ser bloqueado;

e) A Área de TI deve implementar mecanismo de reativação de senhas mediante a identificação do usuário.

3.4 Certificado digital

O NTI deverá providenciar a aquisição e uso de certificados digitais adequados, para aplicações de TI da UNIVATES que exijam esse nível de segurança.

4 SEGURANÇA FÍSICA

Os itens abaixo tratam dos requisitos indispensáveis para o controle do acesso físico, contingência e proteção da infraestrutura e equipamentos de TI da UNIVATES.

4.1 Acesso físico

a) O NTI deverá manter atualizada, junto ao Setor de Engenharia e Manutenção, a lista das pessoas autorizadas a ter acesso às instalações físicas que abrigam os ativos e instalações de TI;

b) Os acessos aos datacenters da UNIVATES deverão ser controlados diretamente pelo NTI;

c) Os procedimentos que detalham os controles de acesso estão disponíveis no NTI;

d) O controle do acesso físico às estações de trabalho é de responsabilidade das áreas e usuários;

e) A área de TI deve providenciar mecanismos de proteção lógica de acesso aos equipamentos, cabendo ao usuário o uso de tais mecanismos.

4.2 Contingência

a) O NTI é responsável pela disponibilidade da infraestrutura e equipamentos centrais, que garantam a oferta dos serviços essenciais de TI, definidos pela Reitoria, com

recuperação em até 6 horas;

b) A UNIVATES e o NTI não podem assumir a garantia de serviços prestados por terceiros, como comunicações, energia elétrica, ar condicionado e outros.

4.3 Proteção da infraestrutura

a) O NTI deverá providenciar as instalações e equipamentos necessários, incluindo manutenção e conservação, para a proteção dos equipamentos e instalações de TI como:

1. Aterramento elétrico das instalações;

2. Proteção contra incêndio;

3. Ar condicionado;

4. Inundações e umidade;

5. Insetos, roedores e outros.

b) As tubulações e caixas de passagem para uso de instalações de TI deverão seguir as especificações EIA/TIA e NBR, atinentes.

5 SEGURANÇA LÓGICA

Os itens abaixo tratam dos mecanismos de proteção para garantir a disponibilidade segura dos sistemas de informação da UNIVATES, sendo a sua utilização passível de ser auditada.

5.1 Armazenamento de dados

O NTI deverá providenciar condições para que os arquivos corporativos sejam armazenados em equipamentos adequados, conectados aos servidores de dados;

b) O NTI não se responsabiliza por dados armazenados em estações de trabalho,

equipamentos particulares ou nos dispositivos móveis;

c) O NTI não se responsabiliza por dados pessoais, armazenados em qualquer forma ou local de armazenamento;

d) O NTI não se responsabiliza por dados de alunos armazenados nos laboratórios de informática, na sua unidade de armazenamento da rede (pasta /home) ou nos dispositivos móveis;

e) O NTI disponibilizará produtos ou serviços para que arquivos corporativos da UNIVATES quando armazenados em equipamentos móveis (notebooks, pen drives e outros) possam ser criptografados;

f) O NTI realizará auditorias periódicas, visando identificar e remover arquivos não vinculados às atividades da UNIVATES sejam armazenados nos equipamentos de TI da UNIVATES.

5.2 Backup

O NTI deverá garantir o backup dos arquivos corporativos armazenados nos servidores de dados, com as seguintes periodicidades e respectivos prazos de retenção:

a) Diário: todos os bancos de dados de produção, arquivos de usuários administrativos, e-mails administrativos, sistemas web e arquivos de configuração de servidores, que tiveram alguma alteração de conteúdo desde a última cópia semanal;

b) Semanal: logs de produção e cópia total de todos os bancos de dados de produção, arquivos de usuários administrativos, e-mails administrativos, sistemas web e arquivos de configuração de servidores e ativos de rede;

c) Mensal: arquivos de alunos, logs de produção e cópia total de todos os bancos de dados de produção, arquivos de usuários administrativos, e-mails administrativos, sistemas web e arquivos de configuração de servidores e ativos de rede;

d) Anual: é a preservação por 5 anos do último backup mensal de dezembro;

e) Eventual: sob demanda de setores.

O NTI deverá dispor de mecanismos de auditoria dos procedimentos acima descritos.

5.3 Segmentação de redes

a) A segmentação da rede local será feita em VLANs (Virtual Lans), permitindo uma estrutura de segurança em zonas, de modo que cada zona permita o acesso às informações necessárias e suficientes aos usuários daquela VLAN;

b) Troca de tráfego entre VLANs será permitida mediante análise do NTI;

c) Fluxo de tráfego externo (de fora para dentro): o NTI deverá implementar ferramentas anti-vírus, firewall, IDS e IPS para todo e qualquer tráfego oriundo do ambiente externo. Tráfego rejeitado será ignorado (dropado);

d) Fluxo de tráfego interno/interno (de dentro para dentro): o NTI deverá implementar ferramentas que permitam apenas tráfego entre VLANs previamente autorizado;

e) Fluxo de tráfego interno/externo (de dentro para fora): o NTI deverá implementar ferramentas que permitam a circulação restrita a URLs (sítios da web) autorizados;

f) Acesso Remoto (extensão dos direitos de usuário interno para o seu uso em local fora do campus): o NTI deverá implementar ferramentas que garantam o uso seguro nessas condições;

g) Todas as necessidades de fluxo de tráfego não previstas deverão ser solicitadas pelo chefe da área interessada ao NTI. Estas necessidades específicas deverão vir acompanhadas de justificativas claras que permitam o estudo de seu atendimento.

5.4 Malware

a) O NTI deverá implementar ferramentas que permitam a detecção da presença de

malware, evitar a sua atuação e facilitar a sua eliminação. A ferramenta deverá ser ativada automaticamente durante o processo de inicialização dos sistemas;

b) Todos os programas de proveniência duvidosa, oriundos de e-mail, web, pendrive ou outras mídias quaisquer, deverão estar sujeitos a um processo de detecção de malware, ou não deverão ser executados;

c) Cabe a Área de TI definir a política de proteção contra malware e manter os mecanismos anti-malware disponíveis para todas estações de trabalho e núcleo da rede;

d) Os dispositivos conectados à rede de dados da Univates que tiverem identificação positiva de vírus poderão ter o seu acesso bloqueado;

e) Cabe aos usuários comunicarem imediatamente toda e qualquer suspeita de malware. Nesses casos, os equipamentos suspeitos devem ser desligados imediatamente;

f) Cabe ao NTI a remoção de malware em equipamentos patrimoniados.

6 CONCEPÇÃO LÓGICA E CONCEPÇÃO FÍSICA

6.1 Concepção Lógica

Mostra de forma esquemática a disponibilidade das informações estruturadas e não estruturadas da Univates.

Considera-se informações estruturadas aquelas disponibilizadas pelos sistemas descritos no diagrama sistêmico.

Considera-se informações não estruturadas as informações armazenadas em mídia papel e ou não controladas pelos sistemas descritos no diagrama sistêmico. As presentes normas não são aplicáveis a este tipo de informações (informações não estruturadas).

Compõem a concepção lógica:

a) Diagrama sistêmico: mostra os sistemas que permitem o acesso às informações estruturadas;

b) Diagrama das Informações Estruturadas;

c) Diagrama das Informações Não Estruturadas.

6.2 Concepção Física

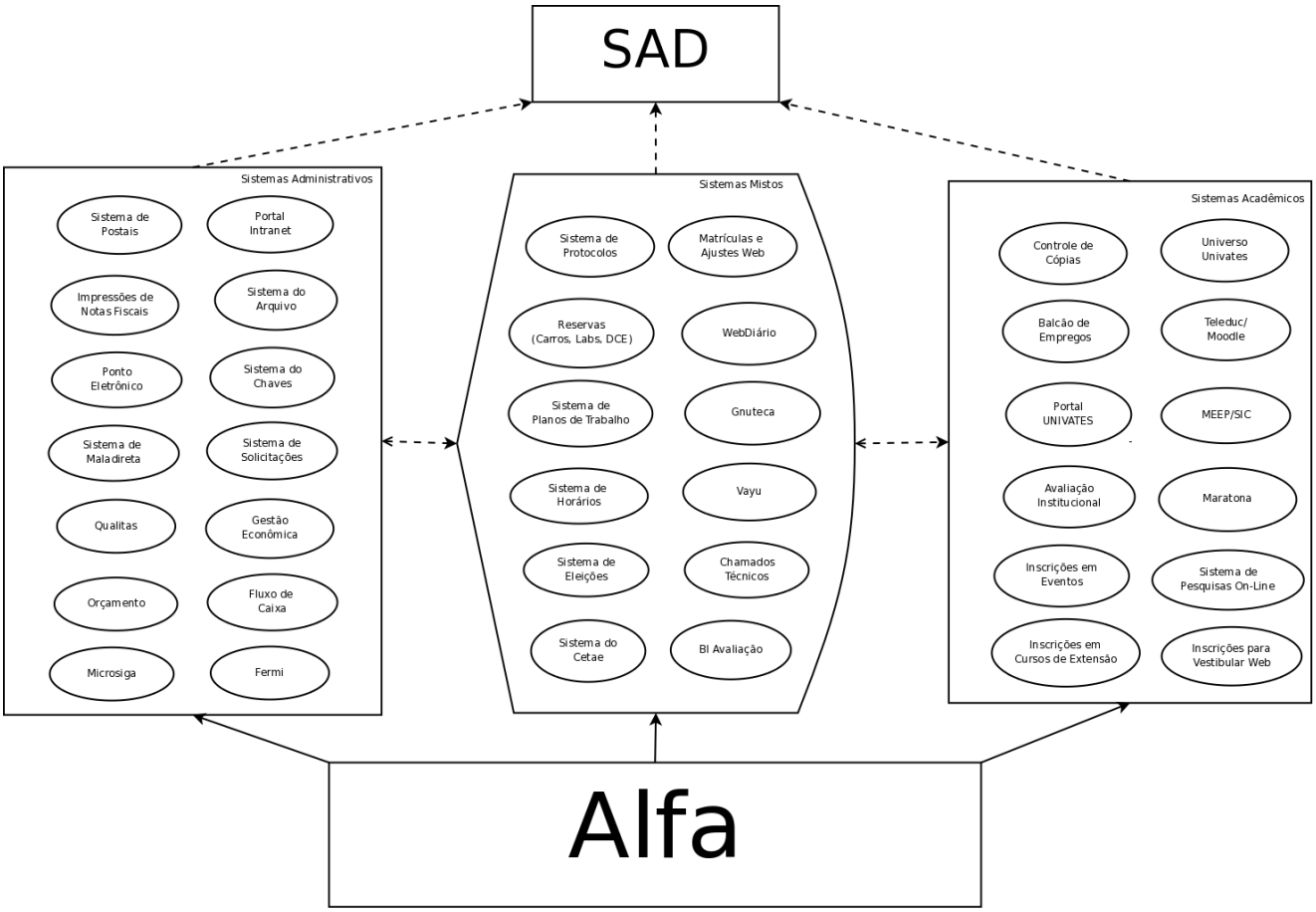
Mostra de forma esquemática a infraestrutura e suas ligações que permitem a implementação da concepção lógica.

7 CONCLUSÃO

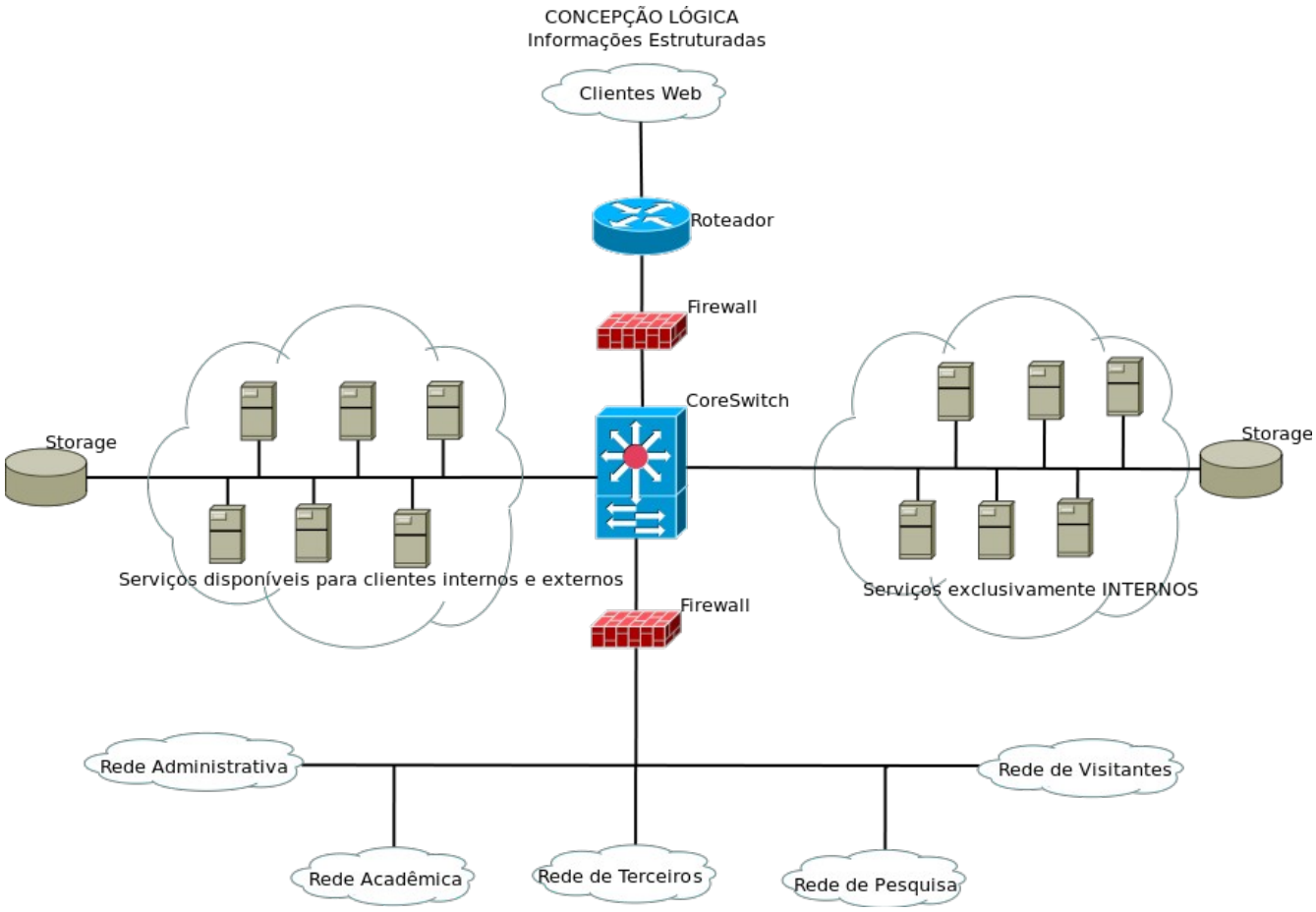
a) Assuntos não previstos na presente Norma deverão ser submetidos à Câmara de TI para análise e posterior encaminhamento à decisão da Reitoria.

b) Estas Normas deverão ser amplamente divulgadas e tornarão sem efeito disposições anteriores sobre o uso dos recursos de TI da Univates.

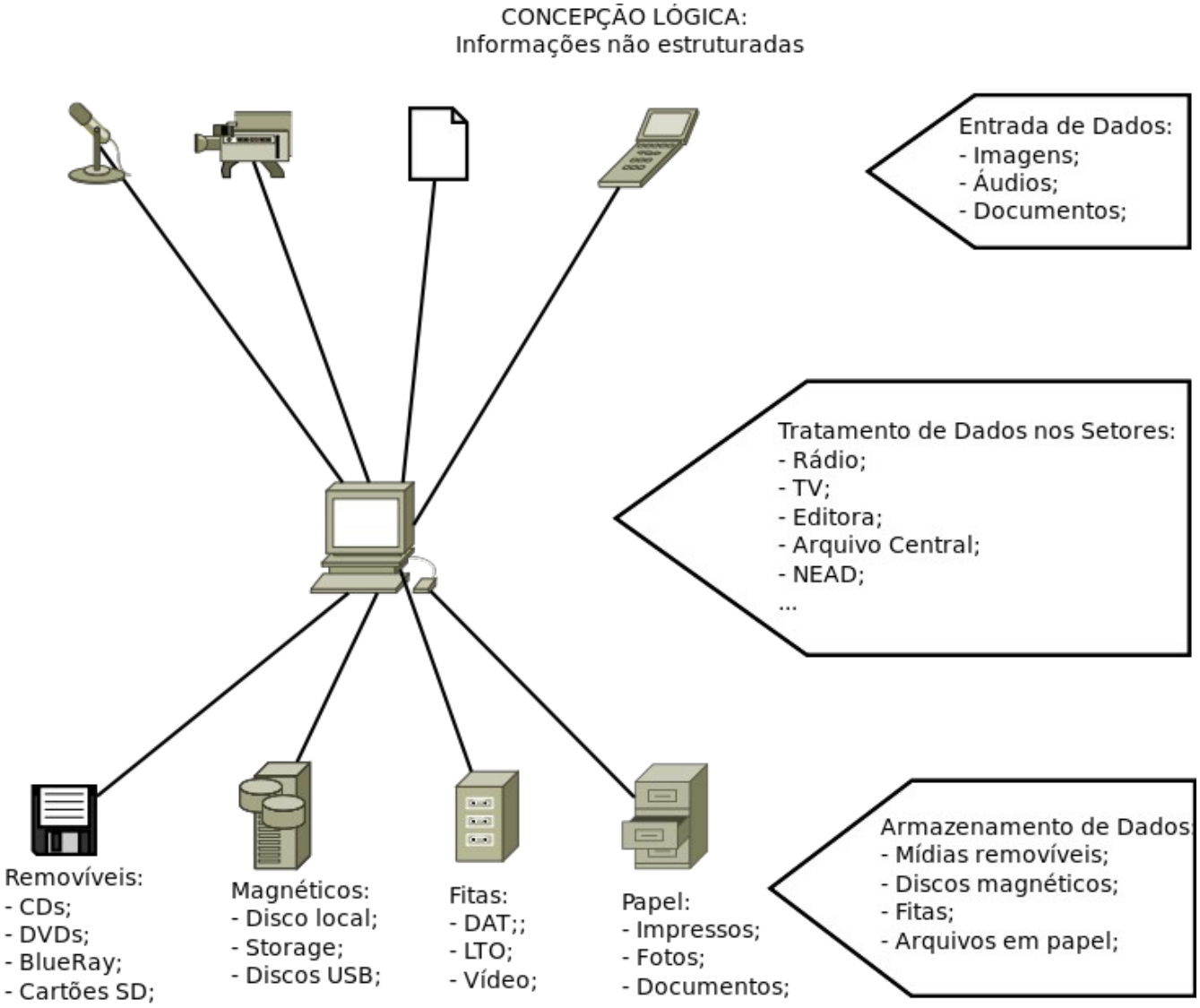
ANEXO A1
Concepção Lógica – Diagrama Sistêmico



ANEXO A2
Concepção Lógica – Informações Estruturadas



ANEXO A3
Concepção Lógica – Informações Não Estruturadas



ANEXO A4
Concepção Física