GRAN FACULDADE

POLÍTICA NIB - SEGURANÇA E CONTINGÊNCIA

CURITIBA/PR
2023

Sumário

POLÍTICA NIB – SEGURANÇA E CONTINGÊNCIA
GRAN CENTRO UNIVERSITÁRIO

1 - OBJETIVO

Este documento tem a finalidade de descrever as ações tomadas para garantir à comunidade acadêmica acessibilidade e segurança nas informações e recursos disponibilizados para atender suas práticas.

2 – ESTRUTURA INTERNA – HARDWARE & SOFTWARE

O GRAN CENTRO UNIVERSITÁRIO utiliza o software de Gerenciamento TOTVS da Linha RM que atende tanto a Gestão Acadêmica compreendendo os Núcleos Acadêmicos, atendimento ao Aluno e Professor, controle bibliotecário, como também atende a Gestão Administrativa da Instituição. Esta ferramenta está instalada e configurada em servidores locais que ficam no prédio da Mantenedora, e o acesso a este sistema se dá através de Conexão de área Remota para a equipe interna, com usuários devidamente cadastrados pela equipe interna de TI.

O acesso aos alunos é por meio do Portal do Aluno, contido no site da Instituição.

O acesso aos professores é através do Portal do Professor disponível no site da Instituição.

A instituição utiliza o PFSense que uma ferramenta open source, licenciado sob BSD license, baseado no sistema operacional FreeBSD e adaptado para assumir o papel de um firewall e/ou roteador de redes, para segurança da rede interna e externa que é gerida por equipe parceira da MSWI - https://www.mswi.com.br.

A instituição possui equipe interna para gestão e manutenção dos Servidores e softwares agindo preventivamente com base neste documento e corretivamente com base nas solicitações dos usuários através do Helpdesk, conforme política descrita neste documento
A instituição utiliza 5 Servidores físicos, sendo 2 destinados ao Sotfware de Gestão, estes servidores possuem com 5 máquinas virtualizadas (VM) – Hyper V 2x1, fazendo com que caso haja algum problema em um equipamento as VMs iniciam automaticamente em outro equipamento. Os outros 2 servidores são responsáveis pelo armazenamento dos arquivos de usuários (Files Server), controle de DNS, Ambiente de teste, a Instituição mantém um equipamento para backup caso ocorra algum imprevisto em algum equipamento. Estes servidores contam com suporte estendido do Fabricante DELL, garantindo assim a análise de logs, a manutenção dos equipamentos e a atualização dos Firmware (uma classe específica de software de computador que fornece controle de baixo nível para o hardware específico do dispositivo).
Os Servidores estão ligados de forma redundante a dois Nobreak com autonomia mínima de duas horas (02:00 h.).

A infraestrutura ainda conta com um link dedicado da Horizons Telecon de 100 MB.

3 – SERVIÇO DE LMS – AVA

O GRAN CENTRO UNIVERSITÁRIO disponibiliza cursos na categoria EAD (Ensino a Distância) e para isso utiliza o software **MOODLE** que é uma plataforma de aprendizagem projetada para fornecer a educadores, administradores e alunos um único sistema robusto, seguro e integrado para criar ambientes de aprendizagem personalizados, utilizado o software no servidor web alocado no Microsoft Azure,

seguindo as políticas de acessibilidade e redundância da Microsoft disponibilizado em: https://docs.microsoft.com/pt-br/azure/storage/common/storage-redundancy. O ambiente pode ser acessado pelo Professor ou Aluno através do site da IES disponibilizado no sit5e da IES.

4 – POLÍTICA DE ACESSOS USUÁRIOS

Denomina-se usuários qualquer pessoa que possa utilizar os serviços oferecidos pela instituição ou aqueles que prestam serviços e que precisam utilizar dos recursos oferecidos, podendo ser classificados em:

a) Alunos: Cadastro criado pela ***Secretaria Acadêmica*** após a confirmação da matricula do aluno na instituição, dando-lhe permissão a acesso ao portal do Aluno, Biblioteca e Ambiente de Ensino a Distância (conforme modalidade do curso). O código de usuário é o Registro Acadêmico (RA) e a senha é o CPF do Aluno sendo solicitado pelo sistema a alteração no primeiro acesso, tendo como única premissa possuir no mínimo 6 caracteres.

b) Professores: Cadastro criado pela ***Secretaria Acadêmica*** após a confirmação do cadastro pelo departamento de Recursos Humanos quando funcionário, ou após o aval da Mantenedora quando professores convidados. O código do usuário é escolhido pelo Profissional conforme documento disponibilizado pelo departamento de Recursos Humanos, e a senha é o CPF do colaborador sendo solicitado pelo sistema a alteração no primeiro acesso, tendo como única premissa possuir no mínimo 6 caracteres.

c) Colaboradores: Cadastro criado pela Equipe de TI, com base na solicitação do departamento de Recursos Humanos via portal de Chamados. O código do usuário é escolhido pelo Profissional conforme documento disponibilizado pelo departamento de Recursos Humanos, e a senha é o CPF do Aluno sendo solicitado pelo sistema a alteração no primeiro acesso, tendo como única premissa possuir no mínimo 6 caracteres.

5 – POLÍTICA PREVENTIVA

Os Sistemas operacionais dos servidores internos são atualizados mensalmente, conforme disponibilização da Microsoft.

O Firmware dos servidores são atualizados semestralmente, conforme disponibilização da fabricante DELL.

O Sistema de Gestão é Atualizado a versão anualmente, e aplicados pacotes corretivos chamados de PATCH pela provedora do Software, conforme identificado alguma melhoria no processo.

O sistema de Resfriamento da Sala do Servidor é revisado semestralmente.

Os demais equipamentos (computadores, monitores) são revisados semestralmente ou com base no calendário dos fornecedores quando o equipamento é de terceiro.

Anualmente o nobreak e seu banco de baterias deverá receber manutenção preventiva realizada por empresa técnica especializada;

Anualmente os projetores deverão receber manutenção preventiva especializada;

Os backups de bancos de Dados do sistema de gestão são realizados diariamente sendo um full no período da noite e diferencial cinco vezes ao dia.

Os backups das maquinas virtuais são realizadas a cada alteração de configuração necessária.

6 – POLÍTICA CORRETIVA

6.1 Problemas com computadores nos laboratórios de informática

a). Professores que estão utilizando ou que irão utilizar o referido laboratório, informam. ao Setor de TI da Instituição através do Sistema de Suporte ou enviando um e-mail para o endereço do núcleo.

b). O chamado de suporte chega até o setor de TI e o atendimento é agendado;

c). Após o atendimento o solicitante é informado da conclusão/resolução do problema informado;
d). Caso o problema impeça o andamento da aula, o Setor de TI vai até o local fazer uma primeira verificação do problema e tenta solucioná-lo in-loco.

6.2 Problemas com computadores administrativos
a). O colaborador que está utilizando o equipamento, informa ao Setor de TI da Instituição através do Sistema de Suporte ou enviando um e-mail para o endereço do núcleo.
b). O chamado de suporte chega até o setor de TI e o atendimento é agendado;
c). Após o atendimento o solicitante é informado da conclusão/resolução do problema informado;
d). Caso o problema impeça o andamento do trabalho do colaborador, o Setor de TI vai até o local fazer uma primeira verificação do problema e tenta solucioná-lo in-loco. Caso não seja possível a resolução do problema, é disponibilizado um computador provisório para o colaborador poder continuar desenvolvendo suas atividades.

6.3 Problemas de conexão com a rede interna
a). Identificar em qual andar do Campus está ocorrendo o problema;
b). Analisar a conexão do servidor central até o bloco afetado;
c) Identificar a causa do problema;
d) Caso o problema de conexão seja em todo o campus, verificar se os servidores de endereços DHCP e de autenticação estão funcionando adequadamente.

6.4 Problemas de conexão com a internet
a) Identificar em qual andar do prédio está ocorrendo o problema;
b) Analisar a conexão do servidor central até o andar afetado
c) Identificar a causa do problema;
d) Caso o problema de conexão seja em todo o prédio, verificar se há conexão até o Roteador e até o Modem da Operadora. Caso haja conexão interna até os referidos equipamentos, deverá ser aberto um chamado de suporte com a Operadora e alterar a conexão para a rede alternativa.

6.5 Problemas com acesso aos sistemas internos da Instituição
a) Identificar qual o sistema está apresentando problema de acesso;
b) Verificar se a VM onde o mesmo está instalado está em execução;
c) Caso esteja em execução, verificar a conexão de rede da VM;
d) Caso não esteja em execução, iniciá-la no servidor (Monitor de Máquina Virtual) e testar seu acesso novamente;
e) Por fim, identificar e resolver o problema informando a solução aos demais servidores.

6.6 Problemas com acesso à internet pelos alunos em equipamentos particulares
a) Verificar se a rede acadêmica está online e funcionando em caso negativo reiniciar serviços ou voltar backup;
b) Verificar se o roteador/access point ao qual o aluno está se conectando está funcional;
c) Se o problema for no equipamento do aluno orientá-lo a procurar uma assistência técnica;
d) É aberto um chamado técnico para estatística e feedback futuro.

6.7 Problemas com acesso à internet pelos colaboradores em equipamentos particulares
a) Verificar configurações definidas de forma manual no equipamento;
b) Verificar se a rede administrativa está online e funcionando em caso negativo reiniciar serviços ou voltar backup;
c) Verificar se o roteador/access point ao qual o colaborador está se conectando está funcional;
d) Se o problema for no equipamento do colaborador orientá-lo a procurar uma assistência técnica.

6.8 Problemas com acesso a algum site específico

a) O colaborador que está utilizando o equipamento, informa ao Setor de TI da Instituição através do Sistema de Suporte e informando o site que está com problemas ao abrir;
b) O chamado de suporte chega até o setor de TI e o atendimento é agendado;
c) O Setor verifica o site e o motivo do problema de acesso procedendo com a liberação no firewall caso não entre em conflito com outras regras ou normativas;
d) Após a resolução o solicitante é informado da conclusão/resolução do problema informado.

6.9 Problemas com UPS/nobreak
a) Verificado problema ou anormalidade informado pelo próprio no-break, com o multímetro testa-se a entrada de energia no equipamento pela porta trifásica (entrada da fornecedora) bem como pela porta do banco de baterias;
b) Intervenção imediata para problemas adicionais deve-se contatar de imediato o Departamento de Administração e planejar medidas corretivas junto a empresa técnica especializada externa;
c) Verificar a possibilidade de desligar equipamentos e/ou serviços não essenciais enquanto o funcionamento do no-break não é normalizado;
d) Em caso de desligamento total proceder com o passo "B" e, em paralelo ligar o servidor que possui o firewall e a internet em fonte de energia alternativa para que pelo menos o DHCP e a internet continuem disponíveis no prédio;
e) É aberto um chamado técnico para estatística e feedback futuro.

6.10 Problemas com equipamentos de rede
a) Identificar qual equipamento está apresentando problema;
b) Caso possível realizar a manutenção do mesmo;
c) Caso não tenha como consertar, realizar a troca do equipamento de forma que haja o menor transtorno possível no desempenho das atividades dos demais colaboradores da Instituição.
d) Verificar o estoque do ativo substituído e providenciar aquisição de equipamento de reposição.

6.11 Problemas físicos com cabeamento da rede interna e externa
a) Identificar qual o problema e onde está ocorrendo;
b) Verificar as ligações (Switches) do cabeamento que está com defeito e testá-lo, bem como os conectores RJ45;
c) Se necessário refazer a crimpagem dos conectores RJ45 imediatamente;
d) Caso haja necessidade, efetuar a troca do cabo ou cabos que estão apresentando falhas.

6.12 Problemas físicos com cabeamento da rede de fibra óptica externa e interna
a) Identificar qual o problema e onde está ocorrendo;
b) Verificar as ligações (Switches e Conversores) do cabeamento que está com defeito e testá-lo, bem como seus conectores;
c) Acionar empresa terceirizada para consertos e fusões de fibra;
d) Caso haja necessidade, efetuar a troca do cabo ou cabos que estão apresentando falhas.

6.13 Problemas com falta de energia elétrica
a) Caso seja identificada queda ou falta total de energia elétrica no prédio efetuamos o chamado para a Companhia de Energia elétrica para as devidas providências;
b) Se a falta de energia for de curta duração os sistemas e servidores de rede continuam em funcionamento, pois estão ligados em um nobreak;
c) Caso a falta de energia dure mais de 1 hora aproximadamente, os sistemas são desligados, bem como os equipamentos e serão religados assim que a energia for restabelecida.

6.14 Incidentes de Segurança e Ataques Cibernéticos
a) Caso sejam detectadas anomalias de tráfego de rede pela central de tratamentos de ameaça, o tráfego deve ser monitorado, se necessário, origem e destino podem ser colocados em quarentena ou banidos da rede.

b) Salvar relatórios e logs de acesso para investigação futura.

6.15 Outros Problemas

Para qualquer outro tipo de problema que envolva a TI, como configurações de e-mail, impressoras, problemas de acesso que envolvam login e senha e etc.
Os passos a serem seguidos são os seguintes:
a) Informar o problema ao Setor de TI da Instituição através do Sistema de Suporte.
b) O chamado de suporte chega até o setor de TI e o atendimento é agendado;
c) Após o atendimento o solicitante é informado da conclusão/resolução do problema reclamado;

7 – CONTINGÊNCIA
ACESSIBILIDADE DE SISTEMAS E RECURSOS TECNOLOGICOS

O GRAN CENTRO UNIVERSITÁRIO possui dois links de internet em sua infraestrutura para possibilitar a redundância da conexão com internet dentro do prédio. Além de possuir nobreaks para garantir o funcionamento dos equipamentos quando há queda de energia temporária.
Caso ocorra uma programação de manutenção da rede elétrica de longa duração será locado um gerador para atender a demanda.
Os bancos de dados devem possuir backups regulares para recuperação rápida dos dados em caso de eventual problema mesmo com pequena perda de dados.
As Vms possuem backups para recuperação imediata em caso de eventual problema.

Curitiba, 2023.

GRAN CENTRO UNIVERSITÁRIO