Norma de Segurança Física de Data Center da Unifesspa

UNIFESSPA
Universidade Federal do Sul e Sudeste do Pará

HISTÓRICO DE ALTERAÇÕES

Data	Versão	Descrição	Autor
01/11/2018	1.0	Documento de referência 1, Versão inicial	Fábio de oliveira Torres
01/12/2018	1.1	Revisão	Luiz Felipe de Sousa, Jamildo dos Santos Carvalho, Vitor de Souza Castro
01/02/2019	1.2	Revisão	Luiz Felipe de Sousa, Vitor de Souza Castro
13/03/2019	2.0	Revisão e padronização da norma	Ralfh Alan Gomes Machado, Luiz Felipe de Sousa, Vitor de Souza Castro

Apresentação

Esta norma estabelece os padrões que deverão ser utilizados quando do gerenciamento físico dos Data Centers da Unifesspa.

Título I

Conceitos e Objetivos

Art. 1º Um *Data Center* é uma infraestrutura física projetada para abrigar servidores e outros recursos computacionais, como sistemas de armazenamento de dados (*storages*), ativos de redes (*switches* e roteadores) e passivos de redes (cabeamento de redes de dados e eletricidade).

Art. 2º O objetivo principal dos *Data Centers* da Unifesspa é garantir a disponibilidade de equipamentos que suportem sistemas fundamentais para o funcionamento da instituição, garantindo assim a continuidade dos serviços prestados pela mesma.

Art. 3º A Segurança Física dos *Data Centers* tem como objetivos específicos:

a) Proteger edificações e equipamentos;
b) Prevenir perda, dano ou comprometimento dos ativos de rede;
c) Manter a continuidade das atividades institucionais; e
d) Prevenir as ameaças que coloquem em risco o bom funcionamento dos sistemas.

Título II

Normas de utilização e de acesso

Art. 4º Dada a criticidade dos *Data Centers*, o acesso às suas infraestruturas e aos seus sistemas deve ser totalmente controlado, onde a administração de dados e de serviços constitui uma tarefa tecnicamente complexa e sua realização deve balizar-se nas melhores práticas de mercado e na alocação de profissionais com perfil técnico adequado.

Art. 5º Quando houver acesso às dependências dos *Data Centers,* este deverá ser realizado através de um forte esquema de autenticação, usando alguns destes métodos: biometria, cartão magnético, crachá, entre outros.

I - O extravio ou roubo de cartões de acesso ou crachás deve ser informado imediatamente ao Centro de Tecnologia da Informação e Comunicação – CTIC para as devidas providências, sendo esta credencial de acesso de uso pessoal e intransferível.

II - Todo o acesso aos *Data Centers* mediante esquema de autenticação deverá ser registrado (usuário, data e hora) em software de autenticação ou na falta deste, através de formulário próprio.

III - Adicionalmente convém que o Controle de Acesso utilize sistemas eletrônicos complementares como:

a) Circuito Fechado de TV: nas áreas consideradas estratégicas, havendo registro da imagem local por meio de câmeras de vídeo, que deverão estar sendo armazenadas em alguma mídia, de forma que as imagens possam ser resgatadas em caso de alguma ocorrência ou auditoria; e

b) Alarme que envie alguma mensagem a uma estação de gerenciamento remota caso ocorra algum acesso não autorizado.

IV - Os acessos de visitantes e terceiros aos *Data Centers* da Unifesspa somente poderão ser realizados com expressa autorização por escrito do Gestor de Segurança da Informação da Unifesspa, com acompanhamento de um membro do CTIC.

V - Deverá ser realizada mensalmente uma auditoria nos acessos aos *Data Center* por meio de relatórios informatizados ou na ausência deste através de um registro manual.

VI - Um servidor lotado no CTIC deverá ser o Gestor do Sistema de Segurança dos *Data Centers* e do Sistema de Autenticação e Acesso, o qual manterá uma lista de procedimentos de controle de acesso com funções de direitos de acesso que deverá ser periodicamente atualizada.

Art. 6º O Gestor do Sistema de Segurança dos *Data Centers* estabelecerá mecanismos de proteção às instalações físicas e as áreas de processamento de dados contra danos e interferências, não devendo ser permitida a entrada de nenhum tipo de alimento, líquido, produto fumígeno ou inflamáveis no ambiente.

Art. 7º A função de Gestor do Sistema de Segurança dos *Data Centers* e do Sistema de Autenticação e Acesso deverá ser atribuída exclusivamente a servidor público efetivo, preferencialmente vinculado à área de infraestrutura de TI.

Art. 8º Os *Data Centers* deverão ser mantidos limpos e organizados, qualquer procedimento que gere lixo ou sujeira no ambiente, somente poderá ser realizado com a colaboração do pessoal de serviço terceirizado devidamente autorizado e com produtos obrigatoriamente não inflamáveis e limpeza a seco.

Art. 9º A entrada ou retirada de qualquer equipamento dos *Data Centers* se dará com o preenchimento da solicitação de liberação e autorização formal deste instrumento pelo diretor do CTIC, de acordo com os termos do procedimento e controle de transferência patrimonial.

Art. 10º Todo o cabeamento e equipamentos que estiverem nas dependências dos *Data Centers*, além de identificados, devem ser documentados para o correto gerenciamento das conexões.

Art. 11º Os *Data Centers* devem ser dotados de um sistema de geração de energia elétrica em *standby* (com redundância) com *nobreaks*, geradores e baterias, capazes de fornecer

energia elétrica de qualidade e suprir toda a necessidade dos *Data Centers* em caso de falha no fornecimento externo de energia.

Art. 12º No ambiente de geração de energia elétrica *standby* (com redundância) haverá:

I - Adequada refrigeração, evitando assim a sobrecarga térmica e desligamento dos equipamentos.

II - Uso de diesel nos geradores, dado que a sua combustão é mais rápida que o gás.

III - Controles do armazenamento de combustível, onde o re-abastecimento dos geradores deve ser monitorado, a fim de que não ocorram falhas.

IV - sistema de nobreaks em módulos individuais ou em grupos paralelos com um sistema de baterias que pode ser fornecido para cada módulo ou para um grupo de módulos.

Art. 13º Os geradores devem estar configurados para fornecer a tensão e corrente adequados para os sistemas *nobreaks*.

Art. 14º Os sistemas geradores deverão ter a capacidade mínima de fornecimento de energia de 5 a 30 minutos, devido a eventos imprevisíveis, que possam ocasionar falhas nos geradores.

Art. 15º A estrutura dos geradores deve possuir um sistema de monitoramento capaz de identificar a capacidade atual de armazenamento das baterias e gravar as tensões, impedância, ou resistência que passam para o sistema de UPS.

Art. 16º Os *Data Centers* devem conter mecanismos de prevenção e combate a incêndios com vistas a evitar e prevenir que os equipamentos sejam danificados.

I - O sistema de combate e prevenção contra incêndios deve ser composto por sistema de detecção de fumaça e extintores, gases inibidores e procedimentos de brigada de incêndio.

Art. 17º Quando possível, as portas de acesso aos *Data Centers* devem permanecer fechadas, com mecanismos de autenticação individual.

Art. 18º O acesso às dependências dos *Data Centers* com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, poderá ser feito somente com autorização por escrito do Gestor de Segurança da Informação da Unifesspa e mediante supervisão.

Art. 19º O acesso aos *Data Centers* sem identificação prévia só poderá ocorrer em situações de emergência, quando a segurança física dos *Data Centers* estiver comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação não estiver funcionando.

Art 20º Sempre que houver possibilidade financeira e administrativa, os *Data Centers* da Unifesspa deverão estar protegidos por um sistema contra descargas atmosféricas (pára-raios) os quais possuam sistema de aterramento eficiente, observando-se o seguinte:

I - Todo sistema de proteção deve receber manutenção preventiva e inspeção anualmente;

II - O projeto, instalação e manutenção do sistema devem estar em conformidade com a norma NBR-5419-2000;

III - A função do pára-raio é proteger edificações e pessoas, não abrangendo necessariamente equipamentos eletro-eletrônicos; e

IV - Recomenda-se a utilização de protetores para os equipamentos considerados essenciais.

Art 21º Para o grupo-gerador e nobreaks, convém que seja firmado um contrato de manutenção para que as peças e componentes do sistema estejam sempre em perfeito estado e de acordo com as recomendações do fabricante;

Art 22º As salas de *Data Centers* da Unifesspa devem possuir iluminação de emergência e interruptores elétricos de emergência que permitam o desligamento em caso de necessidade;

Art 23º Em relação à Segurança Ambiental recomenda-se que:

I - Sensores de monitoria ligados aos fatores ambientais estejam integrados a um sistema que permita a monitoração remota, assim como o disparo de alarme;

II - Haja uso de um desumidificador em cada instalação de *Data Center* da Unifesspa;

Art 24º A permissão para o acesso remoto aos *Data Centers* da Unifesspa será fornecida pelo Gestor do Sistema de Segurança dos *Data Centers* e do Sistema de Autenticação e Acesso e em caso de ausência legal deste, o seu substituto, o qual deverá ter o controle sobre os acessos visando o acompanhamento dos trabalhos e a execução adequada da finalização das sessões remotas.

Art 25º A autenticação e o log de conexão de rede através de acesso remoto devem ser feitos via sistema de relatório e autenticação.

Art 26º O terminal público deve estar numa rede separada de acesso restrito, será provido apenas de um navegador de internet para disponibilizar acesso a sistemas e sites.

Título III

Das auditorias

Art 27º O CTIC deve adotar um esquema de auditorias nos *Data Centers* da Unifesspa. Nestes casos, os servidores públicos devem ter ciência e cooperar com os procedimentos e diretivas adotadas.

I - As auditorias serão realizadas principalmente em servidores e equipamentos de rede para assegurar a configuração e atualização adequadas;

II - Os auditores serão preferencialmente servidores lotados no CTIC, porém em casos especiais, estes poderão ser terceirizados, desde que devidamente contratados e autorizados pela direção do CTIC.

III - Auditorias nas linhas telefônicas devem ocorrer regularmente para verificar a funcionalidade dos modems existentes e qualquer outra atividade planejada;

IV - As auditorias podem ser notificadas ou não.

Art 28º As auditorias notificadas são anunciadas previamente aos servidores, de modo que tenham tempo para preparar o ambiente e rever suas práticas. Seus propósitos são:

I - Analisar os sistemas em relação aos componentes de segurança;

II - Verificar se as práticas dos usuários são impróprias ou desafiam a segurança e se ocorrer notificar o Chefe Imediato; e

III - Assegurar que as informações são apropriadas e cumprem aos objetivos.

Art 29º As auditorias não anunciadas são aleatórias, buscando a identificação de vulnerabilidades e a constante conscientização com a segurança. Podem ser implementadas na forma de ataques simulados, desde que permaneçam no escopo da rede local.

Art 30º Esta Norma entra em vigor a partir da aprovação junto ao CGD.