SERVIÇO PÚBLICO FEDERAL

MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DO RECONCAVO DA BAHIA

PRÓ-REITORIA DE PLANEJAMENTO - PROPLAN

COORDENADORIA DE TECNOLOGIA DA INFORMAÇÃO - COTEC

POLÍTICA DE USO DA DMZ (*DEMILITARIZED ZONE*) DA UFRB

Dezembro de 2013

OBJETIVO

Este documento visa regular o uso seguro da DMZ (*DeMilitarized Zone*/Zona Desmilitarizada) da UFRB.

FUNDAMENTAÇÃO

Lei nº 8.112 de 11 de dezembro de 1990 - Regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

Decreto nº 8.027, de 12 de abril de 1990, Dispõe sobre normas de conduta dos servidores públicos civis da União, das Autarquias e das Fundações Públicas, e dá outras providências;

Decreto 1.171, de 24 de junho de 1994 - Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, e outras providências;

Instrução Normativa GSI nº 01, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta e demais normas complementares;

Norma Complementar nº 07/IN01/DSIC/GSIPR, Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

Decreto nº 7.845, de 14 de novembro de 2012, Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.

DA POLÍTICA DE USO DA DMZ

I. somente servidores da UFRB poderão ser autorizados a utilizar os serviços do *datacenter* da UFRB para hospedagem ou atualização de aplicação/sistema na DMZ (*DeMilitarized Zone*/Zona Desmilitarizada);
II. para que o servidor seja autorizado, será necessário a assinatura do TERMO DE RESPONSABILIDADE DE USO DA DMZ DO DATACENTER DA UFRB, concordando com os termos desta política;
III. devido as constantes atualizações que ocorrem em informática, o conteúdo deste documento poderá ser atualizado sem prévio aviso, com o objetivo de se adequar aos processos e procedimentos que visam oferecer mais Segurança da Informação e Comunicação;

IV. todos os usuários autorizados devem estar familiarizados com esta política, com a legislação vigente e com as consequências de sua violação ficando responsável por manter-se informado das suas atualizações;
V. este documento estará disponível para consulta no site da Coordenadoria de Tecnologia da Informação – COTEC;
VI. o sistema ficará hospedado em uma área de rede onde existem outros sistemas passíveis de invasão e que podem comprometer o sistema ou servidor que está sendo hospedado nessa rede;
VII. em caso de invasão: o servidor, assim como, os sistemas hospedados nele serão retirados do ar até que as correções das vulnerabilidades que implicaram na invasão sejam aplicadas;
VIII. o responsável pelo(s) sistema(s) hospedado(s), deverá manter atualizadas as correções de segurança da informação;
IX. a UFRB se isenta de qualquer responsabilidade para o caso de invasão com comprometimento de arquivos, roubo de informações do governo, roubo de informações de usuários do sistema, uso do sistema para ataques a outros sistemas ou quaisquer outras atividades ilegais que venham a ocorrer e que impliquem em negativação da instituição ou de terceiros;
X. o sistema ficará hospedado na DMZ até que o Núcleo de Gestão Segurança da Informação da UFRB – NUGSI tenha validado através de relatório de analise de vulnerabilidades que os problemas de segurança foram corrigidos;
XI. deverão ser respeitadas a Política de Uso da Rede Ipê/RNP, bem como as políticas e a legislação vigente sobre o assunto, ainda que não expressamente descritas neste documento;
XII. praticar quaisquer atos que possam afetar o sigilo ou a integridade das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito, não será permitido;
XIII. o uso do serviço está restrito a servidores da UFRB autorizados pela COTEC, que terão responsabilidade total pelos dados, informações e toda a infraestrutura disponibilizada, não podendo ser delegado a terceiros;
XIV. a realização de backup do sistema ou servidor que está sendo hospedado é de responsabilidade do usuário autorizado;
XV. por motivo de segurança o backup feito pelo usuário deverá estar protegido de acessos não autorizados e não poderá ser levado ou permanecer fora da UFRB;
XVI. a COTEC não se responsabilizará em nenhuma hipótese pela perda de dados; e
XVII. os casos omissos deverão ser acordados com a COTEC.

APROVAÇÃO

O Gestor de Segurança da Informação e Comunicação da UFRB, no uso de suas atribuições conferidas pela Portaria nº 320/2012, de 10/05/2012, do Magnífico Reitor da Universidade Federal do Recôncavo da Bahia.

Cruz das Almas, 13 de dezembro de 2013.