UNIVERSIDADE FEDERAL DO RECÔNCAVO DA BAHIA
CONSELHO UNIVERSITÁRIO

RESOLUÇÃO Nº 004 /2020

Dispõe sobre a atualização da Política de Segurança da Informação e Comunicações da Universidade Federal do Recôncavo da Bahia e dá outras providências.

O Presidente do Conselho Universitário - CONSUNI da Universidade Federal do Recôncavo da Bahia - UFRB, no uso de suas atribuições e tendo em vista a deliberação extraída da sessão extraordinária, ocorrida em 12 de novembro de 2020.

RESOLVE:

Art. 1º Instituir nova redação para a Política de Segurança da Informação e Comunicações da Universidade Federal do Recôncavo da Bahia, nos termos do Anexo, que passa a fazer parte desta Resolução.

Art. 2º Revogar a Resolução 005/2014 que dispõe sobre a aprovação da Política de Segurança da Informação e Comunicação – POSIC da Universidade Federal do Recôncavo da Bahia.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

Cruz das Almas, 16 de novembro de 2020

SERPRO
Assinado digitalmente por:
FABIO JOSUE SOUZA DOS SANTOS
Sua autenticidade pode ser confirmada no endereço :
<http://www.serpro.gov.br/assinador-digital>

Fábio Josué Souza dos Santos
Reitor
Presidente do Conselho Universitário

ANEXO ÚNICO DA RESOLUÇÃO CONSUNI 004/2020

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

CAPÍTULO I

DO ESCOPO

Art. 1º A Política de Segurança da Informação e Comunicação – PoSIC, da Universidade Federal do Recôncavo da Bahia - UFRB, consiste na normatização e disciplinamento de mecanismos que promovam e assegurem a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados, informações e conhecimentos no âmbito de sua atuação.

Art. 2º Para os fins da PoSIC, a segurança da informação abrange:

I - a segurança cibernética;

II - a defesa cibernética;

III - a segurança física e a proteção de dados e informações organizacionais;

IV - a proteção de dados e privacidade das informações pessoais; e

V - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação, visando garantir a continuidade dos processos.

Art. 3º A PoSIC aborda o uso, tratamento, controle, compartilhamento e a proteção de dados, informações e conhecimentos produzidos, acumulados, armazenados ou transmitidos por quaisquer meios, visando preservar os ativos de atos acidentais ou intencionais de acesso não autorizado, destruição, modificação, apropriação ou divulgação indevida de informações, a imagem institucional e a continuidade dos processos da UFRB, em conformidade com a legislação vigente, normas, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança.

Art. 4º Esta Política, suas normas complementares e procedimentos se aplicam a todas as unidades administrativas da UFRB e devem ser cumpridas por servidores efetivos, discentes, funcionários terceirizados, estagiários, visitantes,

colaboradores externos que prestam serviço em razão de contratos firmados e quaisquer outros usuários não mencionados anteriormente que utilizem ou tenham acesso a ativos de informação.

Art. 5º O relacionamento com outros órgãos públicos ou entidades privadas na celebração de parcerias, acordos de cooperação, contratos, convênios ou demais instrumentos, devem atender o disposto nesta PoSIC.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 6º Para os efeitos desta instrução aplicam-se as seguintes definições:

I - Área de Arquivo: unidade central responsável pela gestão de documentos e arquivos;

II - Área de TI: unidade central que atua na gestão de atividades, soluções e serviços de tecnologia da Informação;

III - Atividades críticas: conjunto de processos vinculados às atividades precípuas da UFRB, cuja interrupção poderá ocasionar severos transtornos;

IV - Atividades precípuas: conjunto de procedimentos e tarefas que utilizam recursos tecnológicos, humanos e materiais, inerentes à atividade fim da UFRB, contemplando todos os ambientes existentes;

V - Ativo de informação:os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso;

VI - Ativo de processamento: é o patrimônio composto por todos os elementos de hardware, software e infra-estrutura de comunicação, necessários para a execução das atividades precípuas da UFRB;

VII - Ativo de sistema: patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução de sistemas e processos da UFRB;

VIII - Comunicação: processo de compartilhamento de informações;

IX - Controle de Acesso: conjunto de políticas e procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais;

X - Criticidade: grau de importância da informação, para a continuidade das atividades precípuas da UFRB;

XI - Custódia: consiste na responsabilidade de se guardar um ativo sem, contudo, permitir o acesso ou o direito de conceder acesso;

XII - Dado: representação de todo e qualquer elemento de conteúdo cognitivo, passível de ser comunicada, processada e interpretada de forma manual ou automática;

XIII - Direito de Acesso: privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo;

XIV - Documento: unidade de registro de informações, qualquer que seja o suporte ou formato;

XV - Incidente de segurança: qualquer evento ou ocorrência, confirmados ou sob suspeita, que comprometam ou ameacem a integridade, autenticidade ou disponibilidade;

XVI - Informação: conjunto de dados organizados, elemento referencial, noção, ideia ou mensagem contidos num documento;

XVII - Não repúdio: impossibilidade da negação da autoria da informação;

XVIII - Política de Segurança da Informação e Comunicação – PoSIC: documento aprovado pela autoridade responsável pelo órgão ou entidade da APF, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da Segurança da Informação;

XIX - Processo: agregação de atividades e comportamentos executados por humanos ou máquinas para alcançar um ou mais resultados;

XX - Processo de negócio: trabalho que entrega valor para os clientes ou apoia/gerencia outros processos;

XXI - Proteção dos ativos: processo pelo qual os ativos recebem classificação quanto ao grau de sensibilidade, sendo que o meio de registro de um ativo de informação deve adotar, no mínimo, a mesma classificação de proteção dada ao ativo que o contém;

XXII - Recurso: além da própria informação, todo o meio direto ou indireto utilizado para o seu tratamento, tráfego e armazenamento;

XXIII - Responsabilidade: obrigações e deveres de quem ocupa determinada função em relação ao acervo de informações;

XXIV - Segurança da Informação: preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento;

XXV - Tecnologia da Informação e Comunicação - TIC: meios técnicos e/ou quaisquer formas de transmissão usados para tratar a informação e auxiliar na comunicação por meio de tecnologias que interferem e medeiam os processos informacionais e comunicativos dos seres, o que inclui hardware e softwares de computadores, rede e telecomunicação.

XXVI - Usuário: quem utiliza, de forma autorizada, recursos inerentes às atividades precípuas da UFRB;

CAPÍTULO III

DOS PRINCÍPIOS

Art. 7º A PoSIC é estruturada utilizando os princípios básicos da administração pública, sendo regida também pelos princípios:

I - Disponibilidade: a informação deve estar segura, acessível e utilizável sob demanda por usuários devidamente autorizados;

II - Integridade: a informação só pode ser alterada por pessoas autorizadas, de forma a garantir o controle da manutenção das características originais de forma e conteúdo estabelecidas na produção ou acumulação;

III - Autenticidade: a informação deve ser produzida e armazenada sem sofrer alteração não controlada, corrompimento ou adulteração, garantindo a veracidade de sua autoria e o não repúdio;

IV - Confidencialidade: a informação somente deve ser fornecida e acessada por usuários devidamente autorizados;

CAPÍTULO IV

DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 8º A PoSIC da UFRB foi elaborada com base nas seguintes referências e sua aplicação deve considerar as alterações posteriores:

I - Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

II - Decreto nº 10.332, de 28 de abril de 2020, que institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências;

III - Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

IV - Decreto nº 10.148, de 2 de dezembro de 2019, que Institui a Comissão de Coordenação do Sistema de Gestão de Documentos e Arquivos da administração pública federal, dispõe sobre a Comissão Permanente de Avaliação de Documentos e dá outras providências;

V - Lei nº 13.853, de 8 de julho de 2019, que altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências;

VI - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;

VII - Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

VIII - Decreto nº 8.539, de 8 de outubro de 2015, que dispõe sobre o uso do meio eletrônico para a realização do processo administrativo no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional;

IX - Decreto nº 7.845, de 14 de novembro de 2012, que 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;

X - Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição;

XI - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal e dá outras providências;

XII - Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

XIII - Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências;

XIV - Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

XV - Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988.

CAPÍTULO V

DIRETRIZES GERAIS

Art. 9º A informação é recurso vital para o adequado funcionamento da UFRB, devendo ser tratada como patrimônio a ser protegido e preservado.

Art. 10 Os recursos não podem ser utilizados para constranger, assediar, ofender, discriminar, caluniar, ameaçar ou causar prejuízos a qualquer pessoa física ou jurídica, bem como para veicular opiniões político-partidárias, preconceito étnico, religioso ou sexual;

Art. 11 Os processos de negócio ou recursos não devem ser de conhecimento e responsabilidade exclusiva de apenas um usuário.

Art. 12 As informações de propriedade ou sob custódia da UFRB, devem ser utilizadas apenas no estrito interesse desta, não podendo os usuários a qualquer tempo ou sob qualquer pretexto, apropriar-se dessas informações ou transmiti-las para fora do âmbito da instituição, salvo em situações específicas ou com autorização do dirigente competente.

Art. 13 As publicações realizadas em qualquer meio de comunicação, em desacordo com as diretrizes e normas da UFRB, legislação vigente ou diretrizes da Administração Pública Federal, serão de inteira responsabilidade da unidade ou do usuário que autorizar a realização do ato para todos os efeitos legais.

Art. 14 A retirada ou transporte de bem integrante do patrimônio da UFRB, fica condicionada à anuência das autoridades competentes, nos termos das legislações e normativas internas, referentes à gestão de patrimônio;

Seção I

Do tratamento e classificação da informação

Art. 15 A produção, classificação, tramitação, uso, avaliação, arquivamento e descarte de dados e informações deverão ser realizados conforme a Política de Gestão de Documentos e Arquivos da UFRB, as normas e procedimentos relacionados à Gestão de Documentos emanadas pela área de Arquivo.

Art. 16 Os dados e as informações sob custódia ou de propriedade da UFRB devem ser classificados quanto aos aspectos de sigilo, disponibilidade e

integridade de forma a receber nível de proteção adequado em atendimento a legislação vigente.

Art. 17 O tratamento de dados pessoais deve assegurar a titularidade e garantir os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos da legislação vigente.

Art. 18 Ficam proibidos os atos de divulgação, guarda, arquivamento de documentos confidenciais sem a devida proteção e o descarte sem destruição documental.

Art. 19 Todo usuário deve ser capaz de identificar a classificação atribuída a uma informação e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

Art. 20 O acesso, uso, divulgação e tratamento da informação classificada ficarão restritos aos usuários autorizados.

Art. 21 No planejamento e na execução do tratamento da informação deverão ser priorizadas:

I - A utilização dos sistemas oficiais disponibilizados pela Área de TI;

II - Tecnologias, padrões, processos, informações e dados interoperáveis;

III - Ações e procedimentos de produção, uso, manutenção e preservação de forma integrada, relacionada e contínua, de modo a manter e registrar toda a cadeia de custódia e preservação.

IV - Recursos criptográficos adequados aos graus de sigilo exigidos;

V - Técnicas de certificação e assinatura digital; e

VI - Técnicas e procedimentos de protocolização eletrônica de documentos.

Art. 22 Deverão ser realizadas cópias de segurança dos dados e informações da UFRB;

Parágrafo único. As cópias de segurança deverão ser validadas e armazenadas, local e remotamente, de forma a minimizar a perda de informações;

Art. 23 É responsabilidade do usuário a realização de cópias de segurança (*backups*) e proteção das informações contidas no equipamento sob sua responsabilidade.

Art. 24 O descarte de dados e informações, independente do suporte, deverá seguir os procedimentos determinados pela Comissão Permanente de Avaliação de Documentos (CPAD-UFRB).

Seção II

Da Segurança Física e do Ambiente

Art. 25 Compete à Reitoria classificar as dependências da instituição, quanto ao nível de restrição necessária, considerando as atividades críticas e a criticidade das informações, observando os seguintes níveis de classificação:

I - Livre: locais em que o acesso de qualquer cidadão está autorizado;

II - Semi-restrito: locais em que o acesso é permitido apenas a pessoas portando identificação;

III - Restrito: locais em que o acesso necessita de expressa autorização;

Art. 26 As áreas classificadas com nível de restrição devem estar munidas de mecanismos de segurança que garantam a proteção contra acessos indevidos.

Art. 27 As dependências restritas e seu entorno devem receber preparação especial contra desastres naturais ou causados por intervenção humana.

Art. 28 O armazenamento e utilização de materiais ou substâncias inflamáveis deve ser monitorado e controlado pelas unidades de forma a minimizar os danos possíveis.

Parágrafo único. Nas dependências com acesso restrito e em seu entorno, preferencialmente, não devem ser armazenados os materiais e substâncias citadas no caput.

Art. 29 Equipamentos de emergência, como os de detecção e combate a incêndios, devem estar presentes em plenas condições de uso e posicionados em espaços com fácil acesso.

Art. 30 As unidades com controles de segurança elétricos devem possuir sistema de redundância de modo a garantir a proteção contínua do ambiente.

Seção III

Dos Controles de Acesso

Art. 31 Deverão ser implementados mecanismos de controle de acesso, com objetivo de proteger os recursos contra danos, perda, modificação ou divulgação não autorizada.

Art. 32 Os servidores efetivos, terceirizados, estagiários, discentes e visitantes deverão portar identificação fornecida pela instituição em local visível enquanto estiverem em área de acesso semi-restrito ou restrito.

Parágrafo único. É responsabilidade da empresa contratada o fornecimento do crachá de identificação de seus profissionais terceirizados.

Art. 33 O usuário receberá direito de acesso apenas aos recursos necessários ao desempenho de suas funções.

Art. 34 Deverão ser implementados mecanismos de controle e registro do acesso, que permitam a identificação, a finalidade e o período de permanência, em áreas classificadas como restritas.

Art. 35 Deverão ser adotados mecanismos que garantam a integridade e autenticidade da identificação do usuário.

Art. 36 Todos os usuários devem possuir identificação, pessoal e intransferível, que atenda aos critérios definidos pela Área de TI para acessar os recursos e serviços de TIC.

Art. 37 As solicitações de acesso ou restrição a sistemas ou áreas físicas específicas, inclusive as relacionadas a movimentação de pessoal, que sejam necessárias ao exercício do cargo, função ou desenvolvimento de atividades acadêmicas, devem ser realizadas pelos gestores das unidades.

Parágrafo único. Nos casos em que seja necessário o acesso a sistemas ou áreas físicas específicas por parte de servidores lotados em outras unidades, cabe ao gestor do ativo realizar a solicitação ou autorização do direito de acesso especial.

Art. 38 Os responsáveis pela custódia dos ativos de informação deverão realizar constantemente a verificação e atualização dos direitos de acessos dos usuários.

Seção IV

Da Gestão de Incidentes em Segurança da Informação

Art. 39 A gestão dos incidentes é de responsabilidade do gestor do ativo, do CSIC e do Gestor de Segurança da Informação, respeitando os limites de suas competências.

Art. 40 Os incidentes de segurança são classificados com base na sua gravidade, e a comunicação da sua ocorrência será de acordo com o nível de comprometimento:

I - baixo: ao comprometer apenas do usuário, tal ocorrência será comunicada a ele e a área responsável pela custódia da informação;

II - médio: ao comprometer o desempenho da unidade, onde além da comunicação feita em caso de baixa, também será comunicada à respectiva Pró-Reitoria/Direção do Centro de Ensino;

III - alto: ao comprometer a segurança e disponibilidade dos serviços com repercussão em toda a Universidade ou externa, além da comunicação feita em caso de baixa e média, também será comunicada à Reitoria;

Art. 41 A área de TI manterá Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR, que comporá a rede de equipes formada pelos órgãos e entidades da administração pública federal, coordenada pelo Centro de Tratamento de Incidentes de Redes do Governo do Gabinete de Segurança Institucional da Presidência da República.

Art. 42 A regulamentação da ETIR deve ser realizada por meio de documento de constituição aprovado pelo titular da Área de TI.

Seção V

Da Gestão de Ativos

Art. 43 Os ativos da UFRB devem ser mantidos em condições de uso, inventariados com classificação em relação aos níveis de proteção e sua documentação deve ser atualizada sempre que ocorrerem modificações ou fatos relevantes.

Parágrafo único. Os critérios para classificação serão definidos em normas específicas, considerando a necessidade de identificação, localização e atribuição de valor, visando garantir a aplicação de proteção personalizada com identificação clara para os usuários.

Art. 44 A proteção dos ativos é de responsabilidade do seu gestor ou de servidor por ele designado formalmente, ficando a cargo deste a aplicação de procedimentos de controle e uso em conformidade com as políticas, normas e legislação vigente.

Seção VI

Da Gestão do Uso de Recursos Computacionais e de Comunicações

Art. 45 Salvo disposição em contrário, no tocante aos recursos de tecnologia da Informação, só é permitido fazer o que seja expressamente autorizado pela Área de TI e de acordo com a PoSIC;

Art. 46 O setor responsável pelos recursos de TIC deve controlar o seu uso com identificação de usuários.

Art. 47 Todos os recursos e serviços de TI são fornecidos para uso profissional e acadêmico, no cumprimento dos objetivos institucionais, passíveis de auditoria;

Art. 48 É proibida a utilização dos recursos de TIC da Universidade para obter acesso não autorizado ou que venha a comprometer o ambiente interno ou externo.

Art. 49 A instalação e uso de recursos de TIC de propriedade ou sob custódia da UFRB, devem ser previamente homologados ou autorizados pela área de TI.

Art. 50 O suporte e manutenção dos recursos de TIC serão executados pela área de TI, ou pessoas por ela autorizada, salvo nos casos de contratos de garantia ou manutenção.

Art. 51 Fica proibido, salvo com autorização da área de TI, a alteração ou modificação da configuração de *hardware,* bem como, a instalação ou remoção de *software* dos recursos de TIC.

Art. 52 As condições e termos de licenciamento de software e os direitos de propriedade intelectual devem ser respeitados conforme legislação vigente;

Art. 53 O acesso à redes virtuais privadas (Virtual Private Network - VPN), redes externas e a retransmissão de sinal de rede da UFRB somente poderão ser realizados pelos meios autorizados e configurados pela Área de TI ou sob sua supervisão.

Art. 54 O uso das redes sociais sob responsabilidade da UFRB deverá respeitar o disposto nas Diretrizes para o uso seguro das redes sociais nos órgãos e entidades da Administração Pública Federal, direta e indireta.

Art. 55 As comunicações institucionais, deverão garantir o sigilo, a confidencialidade, o não-repúdio, a autenticidade e a disponibilidade do serviço.

Seção VII

Da relação com terceiros

Art. 56 Nos editais de licitação, na celebração de parcerias, acordos de cooperação, contratos, convênios e demais instrumentos congêneres, deverá constar cláusula específica sobre a obrigatoriedade de atendimento ao disposto nesta PoSIC.

Parágrafo único. É responsabilidade dos gestores das áreas que celebram os instrumentos, a verificação da conformidade e a adoção de medidas cabíveis para o cumprimento da PoSIC.

Art. 57 Além do cumprimento dos outros itens desta política, as empresas e prestadores de serviços terceirizados devem:

I - Manifestar ciência do seu dever de cumprir esta PoSIC e Normas de Segurança da Informação;

II - Obter de seus colaboradores a comprovação de conhecimento desta PoSIC;

III - Responsabilizar-se pelos equipamentos e softwares que utilizarem ou instalarem no ambiente da Universidade;

IV - Formalizar necessidade de utilizar áreas de acesso restrito ou equipamentos da Universidade não especificados em contrato, com manifestação de finalidade, relação de profissionais envolvidos e periodicidade de acesso;

V - Capacitar regularmente seus profissionais, sob a supervisão da UFRB, quanto aos comportamentos que promovam a Segurança da Informação.

Art. 58 As prestadoras serão penalizadas pela quebra de sigilo causada por seus colaboradores, assim como, pelo mau uso, instalação ou manutenção não autorizada de recursos de TIC.

Parágrafo único. É responsabilidade dos gestores de contrato a verificação da conformidade com a PoSIC e a aplicação de penalidades pelo seu descumprimento.

Seção VIII

Da Gestão de Riscos

Art. 59 Serão considerados como riscos à Segurança da Informação, a ocorrência de um evento, que em termos de impacto e probabilidade, comprometa o disposto nesta política.

Art. 60 Entende-se como gestão de riscos o processo de identificação, análise, avaliação, tratamento e monitoramento de riscos.

Art. 61 As normas e procedimentos para implantação e gerenciamento de riscos estão definidas na Política de Gestão de Riscos da UFRB.

Art. 62 As unidades deverão incluir em seus planos de gerenciamento de riscos os aspectos relacionados a esta política.

Seção IX

Da Gestão de Continuidade

Art. 63 Entende-se como Gestão da Continuidade do Negócio o conjunto de estratégias preventivas e corretivas que visam identificar potenciais ameaças de impacto ao funcionamento da instituição.

Art. 64 As normas e procedimentos para implantação e gestão da continuidade do negócio estão definidas na Política de Gestão de Continuidade - PGCN da UFRB.

Art. 65 Os recursos contemplados no Plano de Continuidade do Negócio – PCN devem ser preferencialmente redundantes e mantidos em condições técnicas e ambientais determinadas pela área técnica responsável, de forma a garantir a sua máxima disponibilidade;

Parágrafo único. Os PCN desenvolvidos pelas unidades devem contemplar os aspectos relacionados a esta política.

Seção X

Auditoria e Conformidade

Art. 66 O cumprimento desta política deverá ser avaliado periodicamente por meio de verificações de conformidade;

Art. 67 Deverá ser realizada pela auditoria interna auditorias periódicas, de forma a aferir o correto cumprimento da PoSIC;

Art. 68 A auditoria interna deve verificar a efetividade dos controles e o gerenciamento dos riscos relacionados ao cumprimento da PoSIC;

Art. 69 Todos os usuários estão sujeitos à auditoria pela utilização dos recursos da UFRB;

Art. 70 As unidades responsáveis pela custódia dos ativos de informação, ou definidas como competentes, deverão realizar periodicamente auditoria, monitoramento e verificação da aplicação desta PoSIC.

CAPÍTULO VI

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 71 Compete aos usuários:

I - ter pleno conhecimento e seguir a PoSIC;

II - propor mudanças na PoSIC;

III - responder por toda atividade executada com o uso de sua identificação;

IV - notificar, com a maior brevidade possível, o gestor do ativo, o CSIC ou o Gestor de Segurança da Informação, qualquer incidente ou indício relacionado à segurança da informação, que tenha conhecimento, através dos canais oficiais de comunicação;

V - zelar pela segurança e bom funcionamento dos ativos.

Art. 72 Compete à todas as unidades:

I - promover ações de fomento à cultura e conscientização sobre Segurança da Informação em seus níveis de atuação para os membros da comunidade;

II - apoiar e dar suporte ao cumprimento das ações estabelecidas na PoSIC, propor melhorias, revisões, e implementar ações de proteção a informação;

III - manter ações no sentido de promover o uso consciente dos ativos;

IV - incluir os aspectos desta PoSIC nos projetos de construção ou reforma.

Art. 73 Compete à Administração Central da UFRB:

I. subsidiar e destinar recursos a aplicação das ações estabelecidas na PoSIC e aquelas previstas na legislação pertinente;

II. designar um gestor de segurança da informação;

III. criar a Política de Gestão de Continuidade do Negócio;

IV. publicar e manter atualizada a lista de espaços classificados como semi-restritos ou restritos;

V. coordenar e executar as ações de segurança da informação no âmbito de sua atuação;

VI. consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão de segurança da informação; e

VII. aplicar as ações corretivas e disciplinares cabíveis nos casos de violação da segurança da informação.

Art. 74 Compete ao CSIC da UFRB:

I - assessorar a implementação das ações de segurança da informação;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III - participar da elaboração e propor alterações da PoSIC, bem como das normas internas de segurança da informação; e

IV - deliberar sobre normas internas de segurança da informação.

Art. 75 Compete ao gestor de segurança da informação:

I - coordenar o CSIC;

II - coordenar a elaboração da PoSIC e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

III - assessorar a alta administração na implementação da PoSIC;

IV - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

V - promover a divulgação da PoSIC e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade;

VI - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VII - propor recursos necessários às ações de segurança da informação;

VIII - acompanhar os trabalhos da ETIR;

IX - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e (acompanhar e dar suporte a aplicação)

XI - manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República - GSI/PR em assuntos relativos à segurança da informação.

Art. 76 Compete à área de TI, regulamentar, instituir, manter e dar subsídio ao trabalho da ETIR;

Art. 77 Compete à ETIR:

I - integrar a rede de equipes, integrada pelos órgãos e pelas entidades da administração pública federal, coordenada pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo do Gabinete de Segurança Institucional da Presidência da República;

II - monitorar e agir preventivamente de forma a mitigar ou quando não for possível, minimizar impacto dos incidentes de segurança;

III - facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança em Tecnologia da Informação e Comunicação – TIC; e

IV - apoiar a elaboração, promoção e disseminação de práticas de segurança da informação no âmbito da UFRB.

Art. 78 É responsabilidade da Pró-Reitoria de Gestão de Pessoal - PROGEP:

I - Incluir em seu treinamento introdutório, módulos específicos de Segurança da Informação e Comunicação com o objetivo de reforçar uma cultura organizacional voltada para este aspecto.

II - Manter ações de estímulo e rotina de capacitação periódica obrigatória que contemple os aspectos de segurança da informação para os servidores, estagiários e terceirizados, e disponível para toda comunidade acadêmica.

III - Obter dos servidores e estagiários ingressantes comprovação de conhecimento da PoSIC da UFRB.

Art. 79 É responsabilidade da Superintendência de Registros Acadêmicos – SURRAC, estabelecer procedimentos para obter a comprovação de conhecimento da PoSIC da UFRB e suas atualizações pelos estudantes.

CAPÍTULO VII

DISPOSIÇÕES FINAIS

Art. 80 Quando evidenciados riscos à Segurança da Informação e Comunicação ou mau uso, aquele que incorrer no descumprimento desta PoSIC, das normas e procedimentos estabelecidos pela UFRB, estará sujeito a aplicação das sanções e penalidades previstas na legislação vigente, bem como a suspensão dos direitos de acesso;

Art. 81 A PoSIC, deve ser revisada pelo CSIC sempre que se fizer necessária, não devendo exceder o prazo de 04 (quatro) anos.

Cruz das Almas, 16 de novembro de 2020

SERPRO
Assinado digitalmente por:
FABIO JOSUE SOUZA DOS SANTOS
Sua autenticidade pode ser confirmada no endereço :
<http://www.serpro.gov.br/assinador-digital>

Fábio Josué Souza dos Santos
Reitor
Presidente do Conselho Universitário