

**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

**RESOLUÇÃO Nº 005/2014**

Dispõe sobre a aprovação da Política de Segurança da Informação e Comunicação – POSIC da Universidade Federal do Recôncavo da Bahia.

**O Presidente do Conselho Universitário - CONSUNI** da Universidade Federal do Recôncavo da Bahia, no uso de suas atribuições legais e tendo em vista a deliberação do Conselho Universitário, em reunião extraordinária realizada no dia 17 de novembro de 2014,

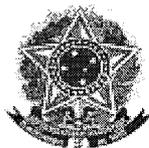
**RESOLVE:**

**Art. 1º** Instituir a Política de Segurança da Informação e Comunicação – POSIC da Universidade Federal do Recôncavo da Bahia, conforme anexo único desta Resolução.

**Art. 2º** Esta Resolução entra em vigor a partir da data de sua publicação, revogadas as disposições em contrário.

Cruz das Almas, 19 de novembro de 2014

  
**Paulo Gabriel Soledade Nacif  
Reitor  
Presidente do Conselho Universitário**



Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário

---

## ANEXO ÚNICO DA RESOLUÇÃO CONSUNI Nº 005/2014

### CAPÍTULO I

#### DAS DISPOSIÇÕES GERAIS E DEFINIÇÕES

**Art. 1º** Fica instituída a Política de Segurança da Informação e Comunicação – POSIC, da Universidade Federal do Recôncavo da Bahia - UFRB, que consiste na normatização e no disciplinamento de mecanismos que promovam a integridade da estrutura de rede e demais recursos de TIC nos quais trafegam informações e dados comuns ou restritos, neles incluídos os equipamentos que armazenam tais informações, sendo aplicável a todos os bens e serviços e a todo o pessoal que se utiliza dos recursos de TIC no âmbito da UFRB.

**Art. 2º** Para os efeitos desta instrução aplicam-se as seguintes definições:

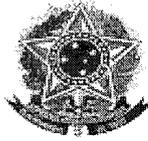
**I** - Política de Segurança da Informação e Comunicação – POSIC: documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, que dá suporte administrativo na implementação e manutenção da segurança da informação e comunicação, fornece diretrizes, normas, critérios, monitoramento e controle, para a preservação da autenticidade, confiabilidade, confidencialidade, disponibilidade, privacidade e integridade dos dados e das informações processadas, armazenadas e dos recursos de TIC custodiados pela UFRB;

**II** - Atividades críticas: conjunto de processos vinculados às atividades precípuas da UFRB, cuja interrupção ocasiona severos transtornos;

**III** - 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;

**IV** - Ativo de informação: é o patrimônio composto por todos os dados e informações geradas, adquiridas, utilizadas ou armazenadas pela UFRB;

**V** - Ativo de processamento: é o patrimônio composto por todos os



**Ministério da Educação**  
**Universidade Federal do Recôncavo da Bahia**  
**Conselho Universitário**

---

elementos de hardware, software e infra-estrutura de comunicação, necessários para a execução das atividades precípuas da UFRB;

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

**VII** - Confidencialidade: a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização;

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

**IX** - Disponibilidade: a informação será acessível e utilizável sob demanda da entidade autorizada;

**X** - Integridade: proteção à precisão e à perfeição de recursos;

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

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

**XIII** - Segurança da informação: preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade podem também estar envolvidas.

**XIV** - Controle de Acesso: restrições ao acesso às informações de um sistema, exercido pela Coordenadoria de Tecnologia da Informação - COTEC;

**XV** - Custódia: consiste na responsabilidade de se guardar um ativo sem, contudo, permitir automaticamente o acesso ao ativo ou o direito de conceder acesso a outros;

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



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

**XVII** - Recursos de TIC: conjunto de equipamentos, programas, procedimentos, normas e demais dispositivos por meio dos quais se aplica a Política de Segurança da Informação e Comunicação;

**XVIII** - Incidente de segurança: qualquer evento ou ocorrência que promova uma ou mais ações que comprometa, ou que seja uma ameaça à integridade, autenticidade ou disponibilidade de qualquer ativo da UFRB;

**XIX** - Proteção dos ativos: processo pelo qual os ativos devem receber classificação quanto ao grau de sensibilidade, sendo que o meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém;

**XX** – Responsabilidade: obrigações e deveres da pessoa que ocupa determinada função em relação ao acervo de informações.

## **CAPÍTULO II**

### **DA FUNDAMENTAÇÃO LEGAL**

**Art. 3º** Conforme o decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

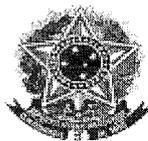
## **CAPÍTULO III**

### **DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO**

**Art. 4º** Deve ser empregada para preservação da autenticidade, confiabilidade, confidencialidade, disponibilidade, privacidade e integridade dos ativos de informação da UFRB.

**Art. 5º** Visa combater atos acidentais ou intencionais de destruição, modificação, apropriação ou divulgação indevida de informações.

**Art. 6º** Aplica-se a todos os usuários de recursos materiais e tecnológicos no



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

âmbito da TIC na UFRB.

**Parágrafo único.** Todos os usuários são co-responsáveis pela segurança da informação, devendo, para tanto, conhecer e seguir a POSIC da UFRB não podendo a qualquer tempo alegar desconhecimento ou ignorância da mesma ou das suas normas complementares.

#### **CAPÍTULO IV**

#### **DA SEGURANÇA DA INFORMAÇÃO**

**Art. 7º** O gerenciamento de informações, documentos e materiais sigilosos da UFRB deverá estar em conformidade com a Lei 12.527, publicada em 18 de novembro de 2011 que dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios para garantir o acesso a informações previsto na Constituição Federal, Lei nº 8.159/1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências e com o 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.

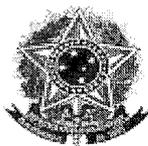
**Art. 8º** Deverão ser realizadas auditorias periódicas dos ativos de informação da UFRB, de forma a aferir o correto cumprimento da Política de Segurança da Informação e Comunicação.

#### **CAPÍTULO V**

#### **DO USO DOS RECURSOS TECNOLÓGICOS**

**Art. 9º** No que se refere à Segurança da Informação, não será permitido o que não esteja expressamente autorizado pela COTEC e/ou esteja em desacordo a POSIC da UFRB.

**Art. 10** É vedado o uso de recursos de TIC da UFRB para constranger,



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

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** É vedado que apenas um usuário possua controle exclusivo de um processo de negócio ou recurso.

**Art. 12** Todos os ativos de informação ou processamento da UFRB devem ser inventariados, classificados em relação o nível de proteção, atualizados periodicamente e mantidos em condição de uso.

**Art. 13** Cada ativo deverá ter um gestor formalmente designado.

**Art. 14** Os ativos críticos devem ser mantidos em ambiente de acesso restrito, respeitando as condições técnicas e ambientais determinadas pelo fabricante, de forma a garantir a sua máxima disponibilidade.

**Art. 15** Os ativos críticos devem ser redundantes e possuir Plano de Continuidade das Atividades – PCA, elaborado pela equipe responsável pelo ativo, para manutenção dos serviços.

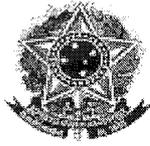
**Art. 16** Só será concedida a credencial de administração local de recursos de TIC através de solicitação formal à COTEC.

**Parágrafo único.** Caberá à COTEC, após análise da solicitação, conceder ou não a credencial solicitada.

**Art. 17** Devem ser precedidos de autorização ou licença da COTEC, mediante solicitação formal do interessado:

I - o acesso à rede da UFRB via Virtual Private Network (VPN), que deve ser feito de acordo com os critérios e procedimentos específicos estabelecidos pela COTEC;

II - o acesso de redes externas à rede UFRB deve ser feito, pelos meios autorizados e configurados pela área especializada da COTEC ou sob sua supervisão, sendo vedado o uso de qualquer forma de conexão alternativa;



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

**Art. 18** Qualquer indício de falha na segurança da informação deve ser formalmente registrado e notificado ao gestor do ativo, bem como ao gestor de Segurança da Informação e Comunicação.

**Art. 19** 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. 20** O uso de recursos de TIC deverá ser controlado de forma a identificar quem está utilizando. Esse controle deverá ser feito pelo setor responsável pelo recurso.

**Art. 21** A instalação e o uso de recursos de TIC de propriedade ou sob custódia da UFRB, devem ser previamente homologados ou autorizados pela COTEC.

**§ 1º** Fica proibida a conexão de recursos de TIC não autorizados na rede da UFRB.

**§ 2º** Os recursos de TIC que não são de propriedade da UFRB devem ser cadastrados para ter acesso à rede de dados, de acordo com a Norma Complementar nº 12/IN01/DSIC/GSIPR.

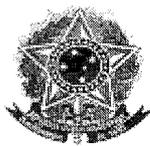
**§ 3º** Fica proibido retransmitir o sinal de rede para outros equipamentos.

## **CAPÍTULO VI**

### **DOS USUÁRIOS DE RECURSOS TECNOLÓGICOS**

**Art. 22** Todo usuário deve estar cadastrado e possuir identificação pessoal, intransferível, protegida por senha e com validade estabelecida para ter acesso aos recursos e serviços de TIC da UFRB.

**§ 1º** A senha deverá ser modificada no máximo a cada 180 (cento e oitenta) dias.



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

**§ 2º** Não será permitido na criação de senhas:

I - a reutilização das últimas 3 (três) senhas;

II - senhas com menos de 8 (oito) caracteres;

III - senhas sem o mínimo de complexidade (utilização de no mínimo 3 (três) tipos de dado (numérico, literal maiúsculo, literal minúsculo e especial);

IV - definir senhas fazendo uso de dados pessoais, próprio telefone, data de nascimento, nome, entre outros.

**§ 3º** Deverá ser formalizada uma solicitação junto à COTEC, para cadastro temporário de visitantes informando os dados do usuário e por quanto tempo será necessário o acesso para que sejam dadas as permissões adequadas.

**§ 4º** Quando houver a necessidade de acesso aos recursos de TIC por parte de prestadores de serviço ou estagiários, o chefe do setor em que ele estiver lotado deverá solicitar formalmente à COTEC, fornecendo os dados do usuário e o tempo que fará acesso para a efetivação do seu cadastro como usuário.

**Art. 23** Deverão ser adotados mecanismos que garantam a integridade e autenticidade da identificação do usuário.

**Art. 24** O usuário receberá permissão de acesso apenas aos recursos necessários e indispensáveis ao desempenho de suas funções.

**Parágrafo único.** As permissões de acesso do servidor deverão ser bloqueadas ou alteradas, mediante informação da Pró-Reitoria de Gestão de Pessoal à Coordenadoria de Tecnologia da Informação em caso de remoção, aposentadoria ou desligamento.

**Art. 25** A todos os usuários cadastrados fica franqueado o acesso à internet, este deverá ser feito exclusivamente para fins diretos e complementares às atividades da instituição, para o enriquecimento intelectual ou como ferramenta para busca por informações que venham contribuir para o desenvolvimento de suas atividades.



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

**Parágrafo único.** Fica proibido acessar ou armazenar material que violem a legislação nacional, o código de ética do servidor público e as normas internas da Universidade.

**Art. 26** Toda informação publicada em meios de comunicação da UFRB será de responsabilidade do usuário que realizou a publicação.

**Art. 27** Fica proibida a circulação, a guarda e o arquivamento de documentos confidenciais sem a devida proteção, e o descarte sem destruição documental.

**Art. 28** Toda solicitação de suporte em recursos de TIC, deverá ser feita através de um sistema para abertura e acompanhamento de chamados.

**Art. 29** Fica proibido, sob qualquer alegação, salvo com autorização da COTEC e/ou do Gestor de Patrimônio, a retirada ou transporte de recurso de TIC para fora das instalações da UFRB.

**Art. 30** Fica proibido, sob qualquer alegação, salvo com autorização da COTEC e/ou do Gestor de Patrimônio, a alteração ou modificação da configuração de *hardware*, bem como, a instalação ou remoção de *software* nos recursos de TIC.

**Art. 31** É de inteira responsabilidade do usuário, a realização de cópias de segurança ou backups e a proteção das informações contidas no equipamento sob sua responsabilidade, obrigatoriamente em mídia de propriedade da UFRB.

**Art. 32** Cada usuário é responsável pelo equipamento e as suas informações durante o período em que estiver fazendo uso deste.

**Art. 33** Não são permitidas cópias, distribuição ou uso indevido de softwares licenciados à Universidade.

**Art. 34** As condições e termos de licenciamento de software e os direitos de propriedade intelectual devem ser respeitados conforme legislação específica vigente.

**Art. 35** O usuário deverá encerrar a sessão de trabalho, fazer logoff, bloquear o computador ou desligar o equipamento, ao término da utilização ou em ausências prolongadas.



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

**Art. 36** Não será permitido utilizar os recursos de TIC da Universidade para ter acesso não autorizado a qualquer outro computador, rede, banco de dados ou informação armazenada eletronicamente em ambiente interno ou externo.

**Art. 37** O uso das redes sociais sob responsabilidade da UFRB deverá respeitar o disposto na Norma Complementar Nº 15/IN01/DSIC/GSIPR que estabelece as Diretrizes para o uso seguro das redes sociais nos órgãos e entidades da Administração Pública Federal, direta e indireta.

## **CAPÍTULO VII**

### **DOS SERVIÇOS TERCEIRIZADOS**

**Art. 38** Além do cumprimento dos outros itens desta política, as empresas e prestadores de serviços terceirizados obrigam-se ao cumprimento das seguintes diretrizes:

I – os contratos de prestação de serviços deverão conter cláusulas onde a contratada manifesta ciência e o cumprimento da Política e das Normas de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento;

II – as empresas contratadas serão responsáveis pelos equipamentos que utilizar ou instalar no ambiente da Universidade;

III – deverá ser formalizada pelas empresas contratadas, a necessidade de utilizar áreas de acesso restrito ou equipamentos da Universidade não especificados em contrato, através de documento que conste a finalidade, os profissionais e o tempo de acesso;

IV – 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 Fiscais de Contrato a verificação da conformidade com a POSIC.



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

**CAPÍTULO VIII**

**DOS PROJETOS, CONSTRUÇÕES E INSTALAÇÕES**

**Art. 39** Todo projeto de construção ou reforma nas instalações da Universidade deverão atender a requisitos de Segurança da Informação e Comunicação de acordo com a norma ABNT NBR ISO/IEC 27002:2005.

**CAPÍTULO XIX**

**DO ACESSO ÀS DEPENDÊNCIAS**

**Art. 40** Deverá haver controle de acesso físico, com objetivo de proteger os ativos de informação contra danos, perda, modificação ou divulgação não autorizada;

**§1º** As dependências devem ser classificadas e identificadas quanto ao acesso.

**§2º** O acesso deve ser classificado em alguma das seguintes categorias:

- I - Livre, locais em que o acesso de qualquer cidadão está autorizado;
- II - Semi-restrito, locais em que o acesso é permitido apenas a servidores, estagiários e terceirizados portando identificação;
- III - Restrito, locais em que o acesso seja expressamente autorizado.

**Art. 41** Os servidores e estagiários deverão estar identificados com crachá fornecido pela instituição, que deverá ser utilizado em local visível.

**Art. 42** Os profissionais de serviços terceirizados deverão utilizar crachá de identificação em local visível, que deverá ser fornecido pela empresa que o contratou.



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

**CAPÍTULO X**

**DAS COMPETENCIAS E RESPONSABILIDADES**

**Art. 43** São responsabilidades de todos os usuários de recursos de TIC da UFRB:

I – discutir e propor mudanças na Política de Segurança da Informação e Comunicação da Universidade;

IV – notificar, com a maior brevidade possível, a chefia imediata e a COTEC, ao tomar conhecimento de qualquer incidente de segurança.

**Art. 44** São responsabilidades dos coordenadores, diretores, e outros titulares de funções de chefia ou de assessoramento superior na UFRB:

I - cumprir e fazer cumprir a POSIC em relação aos seus subordinados;

II - disponibilizar os recursos necessários à implantação da POSIC;

III - apoiar ativamente a execução da POSIC na Universidade.

**Art. 45** É responsabilidade da Pró-Reitoria de Gestão de Pessoal - PROGEP:

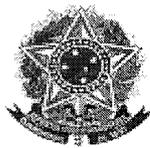
I - notificar à COTEC quando do afastamento ou desligamento de servidor para o cancelamento ou alteração imediata dos direitos de acesso e uso da informação no âmbito da UFRB;

II - providenciar que os servidores e estagiários ingressantes tenham conhecimento desta POSIC;

III – incluir em seu Programa de Capacitação (PACAP) módulos específicos de Segurança da Informação e Comunicação com o objetivo de reforçar uma cultura organizacional voltada para este aspecto;

IV - obter dos servidores e estagiários ingressantes a assinatura do Termo de conhecimento da POSIC da UFRB.

**Art. 46** É responsabilidade da Pró-Reitoria de Administração – PROAD:



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

I - dar conhecimento desta Política de Segurança da Informação e Comunicação quando houver ingresso de terceirizados que desenvolverão atividades em áreas administrativas;

II – promover palestra a terceirizados ingressantes com o objetivo de dar entendimento necessário a comportamentos que promovam a Segurança da Informação;

III - adicionar aos contratos cláusulas da necessidade de atender à POSIC;

IV - notificar a COTEC quando do afastamento ou desligamento de usuários ligados a contratos terceirizados para o cancelamento ou alteração imediata dos direitos de acesso e uso da informação no âmbito da UFRB;

V - obter das empresas responsáveis pelos terceirizados ingressantes a assinatura do Termo de conhecimento da POSIC da UFRB.

**Art. 47** É responsabilidade da Superintendência de Regulação e Registros Acadêmicos – SURRAC;

I - obter dos estudantes ingressantes a assinatura do Termo de conhecimento da POSIC da UFRB;

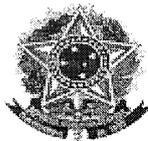
II - notificar a COTEC quando do afastamento ou desligamento de estudantes para o cancelamento ou alteração imediata dos direitos de acesso e uso da informação no âmbito da UFRB.

**Art. 48** É responsabilidade da Pró-Reitoria de Graduação – PROGRAD:

I - promover palestra a estudantes de graduação com o objetivo de dar entendimento necessário a comportamentos que promovam a Segurança da Informação.

**Art. 49** É responsabilidade da Pró-Reitoria de Pesquisa e Pós-Graduação – PRPPG:

I - obter dos estudantes de pós-graduação ingressantes a assinatura do Termo de conhecimento da POSIC da UFRB;



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

II - notificar a COTEC quando do afastamento ou desligamento de estudantes de pós-graduação para o cancelamento ou alteração imediata dos direitos de acesso e uso da informação no âmbito da UFRB;

III - promover palestra a estudantes de pós-graduação com o objetivo de dar entendimento necessário a comportamentos que promovam a Segurança da Informação.

## **CAPÍTULO XI**

### **DAS COMPETÊNCIAS**

**Art. 50** Compete a Coordenadoria de Tecnologia da Informação - COTEC:

I - prover o apoio necessário à implementação e compreensão da POSIC da UFRB;

II - executar as orientações técnicas e procedimentos estabelecidos pelo Comitê de Segurança da Informação e Comunicação;

III - prover os ativos necessários ao cumprimento da Política da Segurança da Informação e Comunicação;

IV - subsidiar o Comitê de Segurança da Informação e Comunicação com informações de cunho tecnológico, aplicadas à execução da POSIC;

V - apoiar a realização de auditorias, conforme plano de auditoria periódica;

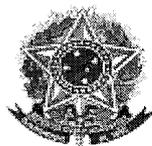
VI - avaliar de forma constante as vulnerabilidades de segurança, a fim de identificar riscos e ameaças à segurança da informação e comunicação.

VII - elaborar as seguintes normas:

a) manutenção de estações de trabalho, que contemple controle do parque computacional, homologação de softwares e utilização de antivírus;

b) uso do correio eletrônico;

c) para os ambientes de homologação e testes dos aplicativos semelhante ao ambiente de produção;



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

**d)** acesso remoto;

**VIII** - solicitar anuência do usuário para acesso remoto aos recursos de TIC, com a finalidade de suporte técnico;

**XIX** - administrar os recursos de TIC observando as orientações da POSIC, suas normas ou as melhores práticas de segurança;

**X** - garantir que os recursos de TIC considerados inservíveis para UFRB, não contenham dados ou informações institucionais;

**XI** - adotar o uso de técnicas e sistemas criptográficos para proteção de ativos considerados de risco e para os quais outros controles não sejam suficientes;

**XII** - elaborar e manter planos de contingência para serviços considerados críticos;

**XIII** - expedir atos normativos complementares à aplicação dessa política;

**XIV** - fiscalizar a aplicação, acompanhar as avaliações e auditorias para assegurar o cumprimento da POSIC;

**XV** - propor programas de treinamento e de conscientização em Segurança da Informação e Comunicação;

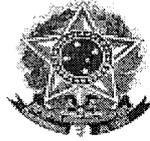
**XVI** - divulgação de boas práticas quanto ao uso seguro da tecnologia da informação no âmbito da Universidade;

**XVII** - agregar melhores práticas de segurança ao processo de desenvolvimento de software e à infraestrutura de rede;

**XVIII** - assegurar que os softwares desenvolvidos e as infraestruturas implementadas possuam controle apropriado e trilhas de auditoria ou registro de atividades;

**XIX** - criar procedimentos que visem controlar e conhecer a estrutura de rede de dados, a fim de permitir a rápida identificação e localização de quaisquer ativos existentes;

**XX** - monitorar o tráfego de rede;



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

**XXI** - planejar ações ou projetos que tenham como produto o incremento da Segurança da Informação, além de participar do planejamento de outros projetos, onde se faz necessária a observância de aspectos de segurança de TIC;

**XXII** - adotar e manter mecanismos que garantam o intercâmbio científico-tecnológico com outras autarquias Federais, Universidades, Institutos Federais, Instituições públicas e privadas, favorecendo assim as ações de Segurança da Informação e Comunicação;

**XXIII** - auxiliar os responsáveis técnicos a identificar e definir as informações críticas e os requerimentos de confidencialidade, integridade, disponibilidade e autenticidade dos ativos de informação sob controle ou custódia da UFRB;

**XXIV** - participar das decisões relacionadas a qualquer violação de segurança dos ativos sob controle ou custódia da UFRB;

**XXV** - propor abertura de sindicância, quando da suspeita de mau uso dos recursos de TIC;

**XXVI** - solicitar recursos necessários para implantação da POSIC;

**Art. 51** Compete à Administração Central da UFRB apoiar e subsidiar a aplicação das ações estabelecidas na Política de Segurança da Informação e Comunicação e normas correlatas.

**Art. 52** Compete ao Comitê de Segurança da Informação e Comunicação da UFRB:

**I** - elaborar, analisar criticamente, revisar periodicamente a POSIC da UFRB e normas complementares, bem como submeter à aprovação da instância competente;

**II** - manter atualizada a POSIC em consonância com as políticas difundidas pelo Governo Federal;

**III** - avaliar o impacto das mudanças sobre os recursos de TIC quanto aos riscos, identificando as principais ameaças;



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

**IV** - analisar os incidentes de segurança da informação e comunicação bem como as ações corretivas correlatas;

**V** - propor iniciativas para aumentar o nível da segurança da informação;

**VI** - fomentar a divulgação da POSIC, bem como ações para disseminar a cultura em Segurança da Informação;

**VII** - participar da elaboração do Plano de Continuidade das Atividades;

**VIII** - participar da elaboração de planos para realizações de auditorias periódicas;

**IX** - elaborar normas para retenção de logs e informações de utilização de serviços e ativos.

**Art. 53** Compete ao Núcleo de Gestão de Segurança da Informação - GSI:

**I** - avaliar, promover, implementar estratégias voltadas para a segurança da informação e comunicação;

**II** - investigar a ocorrência de falha de segurança da informação e comunicação;

**III** - elaborar propostas de solução aos danos decorrentes da falha de segurança;

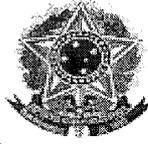
**IV** - propor recursos necessários às ações de segurança da informação e comunicação;

**V** - participar do Comitê de Segurança da Informação e Comunicação;

**VI** - compor a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETRIRC;

**VII** - realizar e acompanhar estudos da aplicação de novas tecnologias, apresentando os possíveis impactos na segurança da informação e comunicação;

**VIII** - manter contato direto com o Departamento de Segurança da Informação e Comunicações - DSIC do Gabinete de Segurança Institucional da Presidência da



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

República - GSIPR para tratar de assuntos relativos à segurança da informação e comunicação;

**IX** - propor normas relativas à segurança da informação e comunicação;

**X** - zelar pela segurança dos recursos de TIC da UFRB;

**XI** - manter um canal de divulgação dos problemas detectados e as respectivas soluções em relação à segurança da informação e comunicação;

**XII** - recomendar a atualização da POSIC em consonância com as políticas difundidas pelo Governo Federal;

**XIII** - criar, divulgar e manter atualizada política de backup institucional;

**XIV** - promover o Plano de Continuidade das Atividades para os recursos de TIC da UFRB.

**Art. 54** Compete aos usuários:

**I** - ter pleno conhecimento e seguir a POSIC;

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

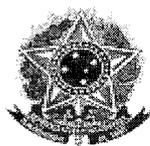
**III** - informar ao Núcleo de Segurança da Informação através dos canais formais de comunicação da UFRB, qualquer indício ou falha na segurança da informação;

**IV** – executar os procedimentos previstos na política de backup institucional.

## **CAPÍTULO XII**

### **DO TRATAMENTO DA INFORMAÇÃO**

**Art. 55** Deverão ser realizados procedimentos de tratamento, armazenamento, identificação e classificação das informações da instituição de tal forma a garantir a integridade, facilidade de localização e evitar o uso dessas informações por pessoas não autorizadas.



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

**Art. 56** O descarte de informações deverá ser realizado através de trituração, incineração ou remoção dos dados de forma segura.

**Art. 57** Deverão ser realizadas cópias de segurança dos dados e informações tomando como base a política de backup da UFRB.

**Parágrafo único.** As cópias de segurança das informações deverão ser testadas, verificadas e armazenadas, local e remotamente, de tal forma a evitar a perda da informação por alguma eventualidade.

### **CAPÍTULO XIII**

#### **DOS RISCOS**

**Art. 58** Serão considerados riscos, toda e qualquer atividade que comprometa a segurança, integridade, estabilidade, acessibilidade, disponibilidade, confidencialidade e autenticidade das informações e dos recursos de TIC da UFRB.

**Parágrafo único.** Compete a COTEC identificar os riscos.

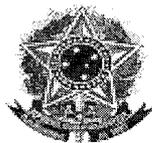
**Art. 59** Quando razões tecnológicas ou determinação superior tornarem impossível o uso apropriado de controles mínimos adequados à garantia da segurança dos ativos, a COTEC implantará medidas alternativas que deverão ser devidamente documentadas a fim de minimizar os riscos.

### **CAPÍTULO XIV**

#### **DA GESTÃO DE RISCOS E TRATAMENTO DE INCIDENTES**

**Art. 60** Entende-se como gerenciamento de riscos o processo que visa à proteção dos serviços da UFRB, por meio da eliminação ou redução dos riscos, conforme seja economicamente e estrategicamente viável, observando os seguintes pontos:

- I - o que deve ser protegido;
- II - análise e classificação de riscos;
- III - plano de ação.



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

**Art. 61** A COTEC apresentará ao CSIC e executará o plano de gerenciamento de riscos e de ação de resposta a incidentes.

## **CAPÍTULO XV**

### **DA GESTÃO DE CONTINUIDADE**

**Art. 62** O Plano de Continuidade das Atividades – PCA – tem como objetivo manter em funcionamento os serviços e processos críticos da UFRB na possibilidade da ocorrência de desastres naturais, falhas de equipamentos, furto, roubo, falhas humanas e incidentes que venham a ocorrer.

**Art. 63** Os procedimentos operacionais relativos a serviços e processos críticos devem estar documentados e sob a responsabilidade de um núcleo, coordenadoria ou gerência.

**Art. 64** O PCA da UFRB será definido pela COTEC com base na análise de riscos e terá a aprovação do CSIC.

## **CAPÍTULO XVI**

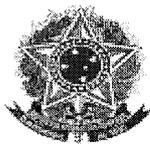
### **AUDITORIA E CONFORMIDADE**

**Art. 65** Todos os usuários estão sujeitos à auditoria em sua utilização dos recursos de TIC da UFRB.

**Art. 66** Os procedimentos de auditoria e de monitoramento de uso dos recursos TIC da UFRB serão realizados periodicamente pela COTEC, com o apoio técnico da Auditoria Interna e do CSIC, com o objetivo de observar o cumprimento das políticas pelos usuários e com vistas à gestão de desempenho e segurança.

**Art. 67** Havendo evidência de atividade que possa comprometer o desempenho e/ou a segurança dos recursos ou que infrinja a POSIC e normas complementares, será permitido à COTEC auditar e monitorar atividades de usuários, inspecionar arquivos e registros de acesso:

I - A COTEC poderá restringir o acesso à fonte causadora do problema, remover dados, desativar servidores e implementar filtros, devendo o fato ser



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

imediatamente comunicado à chefia imediata do usuário, à sua respectiva Pró-Reitoria/Direção do Centro de Ensino e/ou a Administração Central da UFRB, dependendo da gravidade.

**a)** será considerada gravidade baixa a atividade que comprometa apenas os recursos de TIC utilizados pelo usuário, devendo tal ocorrência ser comunicada à chefia imediata;

**b)** gravidade média a atividade que comprometa o desempenho da rede, devendo tal ocorrência ser comunicada à chefia imediata e à sua respectiva Pró-Reitoria/Direção do Centro de Ensino; e

**c)** gravidade alta aquela que comprometa a segurança e disponibilidade dos serviços de toda a Universidade, devendo tal ocorrência ser comunicada à chefia imediata do usuário, à sua respectiva Pró-Reitoria/Direção do Centro de Ensino e a Administração Central da UFRB;

**Art. 68** Será mantido pela COTEC um canal de comunicação para receber denúncias de infração a qualquer parte desta Política de Segurança.

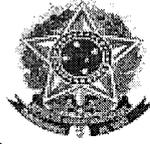
**Art. 69** As aquisições de soluções de TIC deverão ser alinhadas ao Plano de Desenvolvimento Institucional - PDI, tendo como prioridade à interoperabilidade entre os sistemas computacionais utilizados na Universidade e ao Plano Diretor de Tecnologia da Informação - PDTI quando da sua elaboração.

## CAPÍTULO XVII

### CORREIO ELETRÔNICO

**Art. 70** Os serviços de correio eletrônico hospedados em máquinas servidoras da UFRB são oferecidos como um recurso profissional para apoiar seus usuários autorizados, no cumprimento dos objetivos institucionais e esses serviços são passíveis de auditoria.

**Art. 71** Os serviços de correio eletrônico, deverão garantir o sigilo, a confidencialidade, o não-repúdio, a autenticidade, a disponibilidade geral do serviço.



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

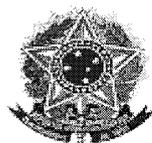
---

**Art. 72** Não será permitido o envio de mensagens do tipo corrente, que se multiplicam sucessivamente, através de recomendações, para que o destinatário as repasse a seus conhecidos (pedidos de ajuda, alertas sobre vírus, piadas, apresentações, etc.).

**Art. 73** Fica proibido enviar textos, figuras, desenhos ou mensagens com características ofensivas, racista, discriminatória, difamatória, evitando qualquer tipo de perturbação, seja através da linguagem utilizada, frequência ou tamanho das mensagens que comprometam a reputação ou imagem da Universidade ou de terceiros, tais como:

- I - propaganda político-partidária;
- II - propaganda com finalidades comerciais;
- III - pornografia e de caráter sexual;
- IV - pornografia infantil (pedofilia);
- V - terrorismo;
- VI - drogas;
- VII - crackers ou programas de códigos maliciosos;
- VIII - jogos;
- IX - violência e agressividade (racismo, preconceito, homofobia, etc.);
- X - violação de direito autoral (pirataria, etc.);
- XI - áudio e vídeo, salvo com conteúdo relacionado, diretamente, a UFRB;
- XII - intolerância religiosa ou de qualquer outro tipo.

**Art. 74** O acesso ao correio eletrônico pessoal não hospedado nos servidores da UFRB, é permitido desde que essa ferramenta não seja utilizada de modo indevido, ilegal, antiético e que respeite a POSIC da UFRB.



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

**Art. 75** Todo usuário deverá periodicamente realizar manutenção da caixa de e-mail institucional, evitando acúmulo de e-mails e arquivos inúteis e que venha a sobrecarregar os servidores.

**Art. 76** Não deverão ser executados ou abertos anexos enviados por emittentes desconhecidos ou suspeitos, bem como aqueles com extensões (bat,.exe, .src, .lnk, .bin e .com), se não tiver certeza absoluta de quem enviou este e-mail.

§ 1º Em situações como essas o usuário será responsabilizado pela inobservância desses detalhes.

§ 2º O usuário deverá encaminhar os e-mails suspeitos para mauuso@ufrb.edu.br colocando em anexo o seu respectivo cabeçalho.

## **CAPÍTULO XVIII**

### **PENALIDADES**

**Art. 77** 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 em vigor, em especial o que consta:

I - na Lei nº 8112/1990, que dispõe sobre o regime jurídico dos servidores civis da União, das autarquias e das fundações públicas federais;

II - no Código de Ética do Servidor Público Civil do Poder Executivo Federal, aprovado pelo Decreto nº 1.171/1994;

III - no Código Penal, através do Decreto-Lei nº 2848/1940;

IV - da Lei 8159/1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências;

V - no Decreto nº 7845/2012, 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;



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

**Art. 78** A constatação de descumprimento das determinações da POSIC da UFRB, além de implicar na imediata suspensão ou cancelamento dos direitos de usuário, deverá ser imediatamente comunicado pela COTEC à chefia imediata do usuário, à sua respectiva Pró-Reitoria/Direção do Centro de Ensino e/ou a Administração Central da UFRB dependendo da gravidade.

**Parágrafo único.** Na falta de retorno no prazo máximo de cinco dias úteis por parte da chefia imediata, será feita comunicação à Direção do Centro, Pró-Reitoria ou Reitoria de acordo com a lotação do servidor e gravidade do ato, que decidirá, resguardados seus limites de atuação e de acordo com a legislação, as providências a serem aplicadas considerando-se a gravidade do evento.

## **CAPÍTULO XIX**

### **ATUALIZAÇÃO**

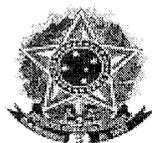
**Art. 79** Todos os instrumentos normativos gerados a partir da POSIC, incluindo a própria POSIC, devem ser revisados pelo CSIC sempre que se fizer necessário, não excedendo o período máximo de um ano.

## **CAPÍTULO XX**

### **DISPOSIÇÕES TRANSITÓRIAS E FINAIS**

**Art. 80** Fica assegurado à COTEC, a qualquer tempo, o poder de suspender temporariamente ou cancelar o acesso dos direitos de usuário a recurso de TIC da UFRB, quando evidenciados riscos à Segurança da Informação e Comunicação ou mau uso.

**Art. 81** As atividades da COTEC devem ser executadas em conformidade com as recomendações publicadas pela Associação Brasileira de Normas Técnicas - ABNT - relativas a sistemas de gestão de segurança da informação, bem como a legislação vigente sobre o assunto.



**Ministério da Educação  
Universidade Federal do Recôncavo da Bahia  
Conselho Universitário**

---

**Parágrafo único.** As normas e procedimentos de que trata o caput desse artigo deverão ser elaboradas tomando-se por base os objetivos de controle estabelecidos na NBR ISO IEC 27001:2006, quais sejam:

- I - organização da segurança da Informação;
- II - gestão de ativos;
- III - segurança em recursos humanos;
- IV - segurança física e do ambiente;
- V - gerenciamento das operações e comunicações;
- VI - controles de acessos;
- VII - aquisição, desenvolvimento e manutenção de sistemas de informação;
- VIII - gestão de incidentes de segurança da informação;
- IX - gestão da continuidade das atividades; e
- X – conformidade.

**Art. 82** Os casos omissos e as dúvidas surgidas na aplicação do disposto na POSIC da UFRB devem ser dirimidos pela COTEC, com a interveniência do CSIC nas situações que requeiram a atuação deste.

**Parágrafo único.** Os casos não resolvidos pelos responsáveis locais, serão analisados e dirimidos pela COTEC, ouvidos os órgãos de assessoria técnica, jurídica e o CSIC.

**Art. 83** Esta Resolução entra em vigor na data de sua publicação, revogadas as disposições em contrário.

Cruz das Almas, 19 de novembro de 2014

**Paulo Gabriel Soledade Nacif  
Reitor  
Presidente do Conselho Universitário**