Política de Segurança da Informação e Comunicações – PoSIC

DTIC – Diretoria de Tecnologia da Informação e Comunicação

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

TÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Este documento estabelece a Política de Segurança da Informação e Comunicações (PoSIC), que é um conjunto das diretrizes necessárias à preservação e à segurança dos bens de informação produzidos e utilizados na Universidade Federal do Estado do Rio de Janeiro (UNIRIO).

Art. 2º Integram a PoSIC normas gerais e específicas de Segurança da Informação bem como procedimentos complementares, destinados à proteção da informação e à disciplina de sua utilização, emanados no âmbito da UNIRIO.

Art. 3º A PoSIC alinha-se, igualmente, às estratégias – Plano de Desenvolvimento Institucional (PDI) e Plano Diretor de Governança de Tecnologia da Informação e Comunicação (PGDTIC) – da UNIRIO e tem por objetivo garantir a confidencialidade, a disponibilidade e a integridade das informações produzidas ou custodiadas pela Universidade.

TÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 4º Para efeito e significância da PoSIC, consideram-se os termos e expressões conforme as seguintes definições:

I. Política de Segurança da Informação: documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da Segurança da Informação;

II. Segurança da Informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

III. Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda de uma pessoa física ou determinado sistema, órgão ou entidade;

IV. Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

V. Confidencialidade: propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizada e credenciada;

VI. Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

VII. Gestão de Segurança da Informação e Comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

VIII. Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

IX. Informação: qualquer forma de representação dotada de significado em determinado contexto pelo qual seja veiculada;

X. Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

XI. Custodiante: entidade detentora da posse, mesmo que transitória, de informação produzida ou recebida pela UNIRIO;

XII. Ativos: tudo o que tem valor para a Instituição;

XIII. Ativos de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

XIV. Ameaças: eventos que comprometem os objetivos da organização;

XV. Risco: probabilidade de uma ameaça se concretizar;

XVI. Vulnerabilidade: ausência de um mecanismo de proteção ou falha;

XVII. *Data Center*: ambiente projetado para abrigar servidores (equipamentos) e outros componentes como sistemas de armazenamento de dados (*storages*) e ativos de rede (*switches*, roteadores);

XVIII. *Firewall*: dispositivo de rede que tem por função regular o tráfego de rede entre redes distintas e impedir a transmissão de dados nocivos ou não autorizados de uma rede a outra.

XIX.

CAPÍTULO I
DAS INSTÂNCIAS ADMINISTRATIVAS

Art. 5º Para efeito e significância desta PoSIC, entende-se como:

I. Reitoria: órgão executivo superior, responsável pela definição das políticas institucionais;

II. Unidades Administrativas: qualquer instância administrativa da UNIRIO, a exemplo dos *campi*: Unidades ligadas aos *campi*;

III. Conselho Universitário (CONSUNI): órgão máximo de deliberação coletiva da UNIRIO;

IV. Pró-Reitoria de Planejamento (PROPLAN): responsável pela elaboração e pelo acompanhamento dos Planos e documentos regulatórios da Universidade;

V. Diretoria de Tecnologia da Informação e Comunicação (DTIC): subordinada à PROPLAN, é responsável por assessorar a Administração Superior e apoiar os demais órgãos da UNIRIO em assuntos relativos à área de tecnologia de informação e comunicação; promover apoio aos usuários; administrar tecnicamente os dados institucionais; garantir o funcionamento de *softwares* e *hardwares*, entre outros encargos previstos em seu Regimento.

VI. Seção de Segurança e Acesso à Informação (SAI): subordinada à Gerência de Infraestrutura (GI) da DTIC, é responsável que a Política de Segurança da Informação e Comunicações da UNIRIO seja cumprida.

TÍTULO III
DAS DIRETRIZES GERAIS

CAPÍTULO I
DO TRATAMENTO DA INFORMAÇÃO

Art. 6º Os Ativos de Informação, sob a responsabilidade da UNIRIO, devem ser protegidos pela Instituição com o objetivo de diminuir os riscos aos mesmos e aos serviços realizados nesta, seguindo a Instrução Normativa 20/IN01/DSIC/GSIPR.

CAPÍTULO II
DO TRATAMENTO DE INCIDENTES EM SEGURANÇA DA INFORMAÇÃO

Art. 7º Para assegurar que os incidentes de Segurança da Informação sejam tratados de forma efetiva, serão observadas as orientações da Norma Complementar nº 06/IN01/DSIC/GSI/PR e da ABNT NBR-ISO/IEC-27001.

CAPÍTULO III
DA GESTÃO DE RISCOS

Art. 8º Conforme a Instrução Normativa 04/IN01/DSIC/GSI/PR, a UNIRIO deve adotar processo contínuo de Gestão de Riscos de Segurança da Informação e Comunicações.

Parágrafo único. O processo de Gestão de Riscos de Segurança da Informação e Comunicações deverá ser periodicamente revisto pela Seção de Segurança e Acesso à Informação a fim de aperfeiçoar e agir proativamente contra riscos que venham surgir de novas tecnologias e de novas ameaças, objetivando a constante elaboração de planos de ação apropriados para a proteção de seus Ativos de Informação.

CAPÍTULO IV
DA GESTÃO DE CONTINUIDADE

Art. 9º De forma a permitir o cumprimento de seu objetivo, a PoSIC deve monitorar e controlar o risco de interrupção de serviços, causado por desastres ou falhas nos recursos de Tecnologia da Informação e Comunicação da UNIRIO.

Parágrafo único. Os níveis de resiliência dos serviços que se utilizam de Ativos de Informação devem ser planejados e implementados por meio de um Plano de Gestão de Continuidade do Negócio, conforme a Norma Complementar 06/IN01/DSIC/GSI/PR e a NBR ISO/IEC 27002:2005. O Plano de Gestão de Continuidade do Negócio deve ser testado periodicamente e aprimorado conforme a necessidade da UNIRIO.

CAPÍTULO V
DA AUDITORIA E CONFORMIDADE

Art. 10º A Seção de Segurança da Informação deverá propor diretrizes, padrões e processos para manterem o registro e procedimentos – como mecanismos de auditoria – que possibilitem o rastreamento, acompanhamento, controle e verificação de acessos aos serviços, sistemas corporativos e rede interna, quando necessário.

CAPÍTULO VI
DOS CONTROLES DE ACESSO

Art. 11º A política de controle de acesso visa a estabelecer critérios de responsabilidade a fim de garantir a segurança dos usuários e a proteção dos Ativos da Instituição. A UNIRIO aplicará diretrizes – conforme a Instrução Normativa 07/IN01/DSIC/GSIPR – a todos os colaboradores e comunidade acadêmica. A política de controle de acesso lógico a todos os sistemas institucionais, intranet, internet, informações, dados e a política de controle de

acesso físico, às quais não estão previstas nesta Política, deverão ser definidas e regulamentadas por meio de normas internas complementares, com o objetivo de garantir a segurança dos usuários e a proteção dos Ativos da Instituição.

CAPÍTULO VII
DO ACESSO À INTERNET

Art. 12º O acesso à internet dar-se-á, exclusivamente, pelos meios autorizados e configurados pela UNIRIO:

I. Os equipamentos, tecnologia e serviços fornecidos para prover o acesso à internet são de propriedade da UNIRIO, que pode, se necessário, bloquear qualquer arquivo, sítios, correio eletrônico, domínio, serviço ou aplicação armazenados na Rede UNIRIO/internet, visando a assegurar o cumprimento da Política de Segurança e Acesso à Informação;

II. Uso de sistemas e mecanismos na rede interna para garantir a integridade dos dados e programas: toda tentativa de alteração dos parâmetros de segurança, por qualquer usuário, sem o devido credenciamento e autorização para tal, será julgada inadequada, e os riscos relacionados serão informados ao usuário e à autoridade máxima da Unidade;

III. É vedado aos usuários da Rede UNIRIO utilizar os recursos da Instituição para, deliberadamente, propagar qualquer tipo de vírus, *worm*, cavalo de troia, *spam*, assédio, perturbação ou programas de controle de outros computadores; e acessar sítios que representem ameaça de segurança ou que possam comprometer, de alguma forma, a integridade da rede de computadores;

IV. A liberação de acesso a sítios e serviços bloqueados, mas necessários ao desempenho das atividades acadêmicas/administrativas do usuário, dependerá de solicitação, devidamente justificada à DTIC, que a submeterá, quando for o caso, ao Comitê de Segurança e Acesso à Informação, para análise e deliberação;

V. Por critério técnico, poderão ser adotadas medidas visando à manutenção da disponibilidade e da qualidade do acesso à internet, seja em situações normais de funcionamento, seja em situações de contingência, tais como: bloqueios totais ou parciais e/ou priorização de acessos a determinados sítios e serviços; e limitação de banda de tráfego de dados:

a) As medidas identificadas, quando implementadas, serão comunicadas à Seção de Atendimento aos Usuários a fim de possibilitar o repasse de informações aos interessados;

VI. Os usuários da Rede UNIRIO não poderão, em hipótese alguma, utilizar os recursos da Universidade para o uso, a instalação, a cópia ou a distribuição não autorizada de *softwares* que tenham direitos autorais, marca registrada ou patente na internet.

Parágrafo único. A utilização e/ou instalação de qualquer software não autorizado será passível de exclusão, e a atividade poderá ser considerada delituosa.

CAPÍTULO VIII
DOS SÍTIOS E USO DO *E-MAIL*

Art. 13º Os serviços e servidores (equipamentos) que hospedam as páginas de internet da Instituição deverão ser configurados para usar tecnologias de autenticação e criptografia, sendo de responsabilidade da DTIC manter a disponibilidade, integridade, confidencialidade e não repúdio das informações armazenadas.

Parágrafo único. É de responsabilidade de cada Unidade da UNIRIO a manutenção da informação publicada em seus respectivos sítios.

Art. 14º Os usuários da UNIRIO terão direito a uma conta de *e-mail* no serviço de correio eletrônico oficial da Instituição, sendo de titularidade única, intransferível e de responsabilidade do usuário a sua utilização.

Parágrafo único. O serviço de *e-mail* não deverá ser usado para a prática de atos ilegais – definidos pela presente Política e normas complementares que venham a ser editadas –, os quais conflitem com os interesses da UNIRIO ou de terceiros.

CAPÍTULO IX
DA SEGURANÇA FÍSICA E DO AMBIENTE DE TI

Art. 15º A Segurança Física tem como objetivo manter as instalações físicas e as áreas de processamento de informações críticas ou sensíveis protegidas contra acesso indevido, danos e interferências. Seguindo a NBR ISO/IEC 27001:2001 e a 07/IN01/DSIC/GSIPR, a área de Segurança Física na UNIRIO é implementada da seguinte forma:

I. Áreas de Segurança**:** define o perímetro da segurança, baseado no nível de criticidade, com controles de acesso físico, segurança nas salas e instalações de processamento;

II. Segurança dos Equipamentos**:** previne perda, dano ou comprometimento dos Ativos e a interrupção das atividades do negócio; mantém a instalação e proteção de equipamentos, o fornecimento de energia e a difusão de boas práticas no tocante à segurança dos equipamentos de redes, armazenamento e processamento de dados;

III. Controles Gerais**:** evita a exposição ou roubo de informação e de recursos de processamento da informação, por meio da conscientização dos usuários, de cursos, palestras, e eventos sobre a temática de Segurança e Acesso à Informação. Sempre que possível manter a política de mesa limpa e tela limpa, que consiste em não deixar qualquer informação exposta, seja fisicamente na mesa de trabalho, como relatórios, lembretes, entre outros, seja na tela do computador, quando o usuário estiver ausente;

IV. Segurança Externa e de Entrada: proteção da instalação onde os equipamentos estão localizados, *Data Centers*, por meio das seguintes medidas de segurança: controle de acesso de pessoas não autorizadas e monitoramento por meio de câmeras;

V. Segurança das Salas de Armazenamento de Equipamentos: registro de todo o pessoal que acessar o ambiente. A sala deve ser trancada quando da saída das pessoas. O conteúdo da sala não deve ser visível externamente;

VI. Redundância: a UNIRIO deverá dar condições de manter a máxima disponibilidade possível dos serviços e sistemas essenciais, mediante sítios de contingenciamento;

VII. Segurança no Fornecimento de Energia Elétrica: geralmente o fornecimento de energia é de responsabilidade da concessionária, e pode apresentar variação de tensão ou interrupção do fornecimento.

VIII. Para garantir a disponibilidade da informação e serviços, a UNIRIO precisa assegurar o fornecimento estável de energia (dentro da tensão recomendada) para os seus *Data Centers*;

IX. *Backups:* o processo de *backup* envolve segurança física e lógica:

a) *Backup* físico: deve-se manter em lugar adequado e com as mídias físicas usadas para tal propósito protegidas de uso e acesso indevido;

b) *Backup* lógico: deve-se criar políticas de *backup* que garantam que as informações críticas da Universidade sejam preservadas com a utilização de sítios de contingência análogos ao *Data Center* principal.

CAPÍTULO X
DA SEGURANÇA LÓGICA DO AMBIENTE DE TI

Art. 16º A UNIRIO aplicará tecnologias de criptografia e controle de acesso para os dados em trânsito e armazenados, no que couber, observando a Lei de Acesso à Informação para dados pessoais e classificados, a fim de garantir a confidencialidade dos dados, inclusive em incidentes de segurança que resultem em vazamento de dados, diminuindo o impacto do incidente.

Art. 17º Em virtude do surgimento constante de novas ameaças cibernéticas e da busca de vulnerabilidades por agentes externos na Rede UNIRIO, a equipe de Segurança e Acesso à Informação reserva a prerrogativa de realizar varreduras de vulnerabilidades nos Ativos de Informação da Universidade, aplicando o dispositivo do art. 6º desta Política.

Art. 18º A equipe de Segurança e Acesso à Informação é responsável pela gestão das políticas do equipamento de *Firewall*, fazendo refletir as normas desta Política no ambiente lógico da Instituição.

TÍTULO IV
DAS SANÇÕES E PENALIDADES

Art. 19º Atos ou ações que violem o disposto nesta Política ou em quaisquer de suas normas ou diretrizes e que prejudiquem os controles de Segurança e Acesso à Informação no âmbito da UNIRIO serão apurados e encaminhados à Gestão superior para as providências cabíveis.

TÍTULO V
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 20º Ao Comitê de Segurança da Informação e Comunicações compete:

I. Assessorar o CONSUNI e a Reitoria na implementação das ações de segurança da informação e comunicações;

II. Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

III. Propor alterações na Política de Segurança da Informação e Comunicações;

IV. Propor normas relativas à segurança da informação e comunicações.

Art. 21º Ao Gestor de Segurança da Informação e Comunicações, no âmbito de suas atribuições, incumbe:

I. Promover cultura de segurança da informação e comunicações no âmbito da UNIRIO;

II. Informar e acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III. Propor recursos necessários às ações de segurança da informação e comunicações;

IV. Coordenar o Comitê de Segurança da Informação e Comunicações e a equipe de tratamento de incidentes e resposta aos mesmos em redes computacionais;

V. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

VI. Manter contato direto com a gerência de Infraestrutura, suporte aos Usuários e Sistemas de Informação para o trato de assuntos relativos à segurança da informação e comunicações;

VII. Propor normas relativas à segurança da informação e comunicações.

Art. 22º Compete à DTIC, por meio da seção específica, especializada em Segurança e Acesso à Informação (SAI):

I. Implementar, coordenar e acompanhar a PoSIC e as normas complementares;

II. Homologar processos de trabalho e procedimentos operacionais necessários para a implementação da PoSIC;

III. Monitorar, auditar e avaliar periodicamente as práticas de Segurança da

Informação, adotadas pela PoSIC;

IV. Constituir e coordenar a Equipe de Tratamento de Incidentes de Segurança da Informação da UNIRIO;

V. Fomentar a cultura e boas práticas da segurança da informação.

TÍTULO VI
VIGÊNCIA E VALIDADE

Art. 23º Esta Política entrará em vigor a partir da sua publicação no Boletim da UNIRIO, e será revisada e atualizada a cada dois (2) anos, a contar da sua vigência ou quando identificada a necessidade pelo Comitê de Segurança da Informação e Comunicações.

ANEXO I

DAS REFERÊNCIAS LEGAIS E NORMATIVAS

I. Decreto nº 3.505, de 13 de junho de 2000: institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

II. Lei nº 12.965, de 23 de abril de 2014: Marco Civil;

III. Decreto-lei nº 2.848, de 7 de dezembro de 1940: Código Penal;

IV. Lei nº 8.069, de 13 de julho de 1990: Estatuto da Criança e do Adolescente;

V. NBR ISO/IEC 27000: Informações básicas sobre as normas da série;

VI. NBR ISO/IEC 27001:2006: Sistema de Gestão de Segurança da Informação;

VII. NBR ISO/IEC 27002:2005: Código de Práticas para a Gestão da Segurança da Informação;

VIII. NBR ISO/IEC 27003: Diretrizes mais específicas para a implementação do SGSI;

IX. NBR ISO/IEC 27004: Normas sobre as métricas e relatórios do SGSI;

X. NBR ISO/IEC 27005: Diretrizes para o processo de Gestão de Riscos de Segurança da Informação;

XI. Instrução Normativa GSI/PR nº 1: Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

XII. Instrução Normativa 04/IN01/DSIC/GSI/PR: Trata da Gestão de Riscos de Segurança da Informação;

XIII. Instrução Normativa 05/IN01/DSIC/GSIPR: Trata da criação de equipes de tratamento de incidentes de segurança;

XIV. Instrução Normativa 06/IN01/DSIC/GSI/PR: Trata da Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações no âmbito da Administração Pública Federal, direta e indireta;

XV. Instrução Normativa 07/IN01/DSIC/GSIPR: Diretrizes para implementação de controles de acesso;

XVI. Instrução Normativa Complementar 08/IN01/DSIC/GSIPR: Gerenciamento de Incidentes em Redes Computacionais nos Órgãos e Entidades da Administração Pública Federal;

XVII. Instrução Normativa Complementar 20/IN01/DSIC/GSIPR: Instituição do Processo de Tratamento da Informação nos Órgãos e Entidades da Administração Pública Federal, direta e indireta.