RESOLUÇÃO Nº 1.355/2019

(Publicada no D.O.E. de 22-02-2019, p. 21)

Aprova a Política de Segurança da Informação (PSI) da UNEB no âmbito da UNEB, e dá outras providências.

O CONSELHO UNIVERSITÁRIO (CONSU) da Universidade do Estado da Bahia (UNEB), no uso de suas competências legais e regimentais, com fundamento no Artigo 11, inciso IV do Regimento Geral da UNEB, e de acordo com o que consta do Processo nº 0603180069859, em sessão desta data,

RESOLVE:

Art. 1º. Aprovar a Política de Segurança da Informação (PSI) da Universidade do Estado da Bahia (UNEB), com vistas a minimizar os riscos aos ambientes tecnológicos na instituição e, consequentemente, às informações sob sua responsabilidade, conforme Anexo Único desta Resolução.

Art. 2º. Esta Resolução entra em vigor na data de sua publicação.

Sala das Sessões, 14 de fevereiro de 2019.

José Bites de Carvalho
Presidente do CONSU

*OBSERVAÇÃO: *O Anexo Único desta Resolução encontra-se disponível no site da UNEB.*

ANEXO ÚNICO DA RESOLUÇÃO Nº 1.355/2019

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI) DA UNIVERSIDADE DO ESTADO DA BAHIA (UNEB)

CAPÍTULO I
DO OBJETIVO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA UNEB

Art. 1º. Este documento tem por objetivo, orientar os órgãos e setores que compõem a Universidade do Estado da Bahia (UNEB), quanto à utilização e atendimento às Normas e condutas de utilização dos dispositivos eletrônicos da Universidade do Estado da Bahia bem como os serviços de Tecnologia da Informação, no tocante a questões de Segurança da Informação.

§1º. As Normas e condutas que trata o *caput* do artigo têm por objetivo estabelecer as diretrizes de proteção relativas ao uso de equipamentos eletrônicos, da Internet e de outras redes públicas de computadores, reduzindo o risco a que estão expostos os Ativos de Tecnologia da Informação da UNEB.

I. Para fins de especificações técnicas, entende-se como ativos de Tecnologia da Informação, todo e qualquer equipamento eletrônico integrante do patrimônio da Universidade do Estado da Bahia, como telefones móveis, telefones fixos, roteadores, switches, rede de comunicação de dados, computadores, notebooks, servidores, tabletes, impressoras ou qualquer outro equipamento correlato; e,
II. Definem-se como usuários dos ativos de Tecnologia da Informação da Universidade do Estado da Bahia, todos os servidores, estudantes, e convidados que fazem uso dos Ativos de Tecnologia da Informação, de forma permanente ou temporária.

§2º. Este e todos os outros caputs contidos neste documento se aplicam a todos os usuários das instâncias administrativas e acadêmicas da UNEB.

CAPÍTULO II
DA UTILIZAÇÃO DE ATIVOS DE TECNOLOGIA DA INFORMAÇÃO

Art. 2º. Todos os usuários serão devidamente identificados na rede da Universidade, através de autenticação de usuário (login) e senha.

Art. 3º. Os Ativos de Tecnologia da Informação da UNEB, incluindo as conexões com a Internet, hardware e software, devem ser empregados na consecução dos seus objetivos, sendo vedada a sua utilização para outros fins, exceto para os casos explicitamente permitidos por esta norma.

Art. 4º. A UNEB pode examinar, sem aviso prévio, o conteúdo de cache de navegadores Web, favoritos, histórico de sites visitados, configurações dos softwares e outras informações armazenadas ou transmitidas pelos computadores pertencentes e/ou instalados à sua rede de dados.

§1º. As informações referentes a utilização de ativos de tecnologia da informação por usuários será mantida em sigilo absoluto, salvo quando devidamente comprovada a utilização indevida por parte dos usuários.

§2º. A quebra de sigilo das informações deverá ser autorizada previamente pelo Orgão/Setor Competente, quando devidamente justificada pelo mesmo e, ouvido a Procuradoria Jurídica da Universidade.

Art. 5º. A informação obtida pelos usuários, através da Internet de forma livre e gratuita deve ser confirmada por fontes fidedignas antes de ser efetivamente usada, ficando a responsabilidade por danos, imputada ao usuário.

Seção I
Dos Controles de Acesso a Serviços da Internet

Art. 6º. A permissão de acesso à Internet deve ser seletiva em relação aos serviços disponibilizados, tais como sítios Web, VPN, serviços de armazenamento (FTP) e Correio Eletrônico, e ser concedida exclusivamente àqueles usuários que necessitem deste acesso para o seu trabalho, seja ele acadêmico ou administrativo, sendo removida quando não for mais necessária.

Art. 7º. O acesso seletivo à Internet deve ser disponibilizado por meio de listas positivas ou negativas, cabendo à GERINF definir a sua regra.

Art. 8º. A permissão de acesso à Internet deve ser concedida através de uma Conta de Usuário que possibilite identificar, individualmente, seu proprietário, podendo o histórico de acesso, inclusive o conteúdo, ser monitorado, sem necessidade de notificação prévia, devendo ser armazenado por um período mínimo de 45 (quarenta e cinco) dias, ou quando cabível, por período previsto em lei.

Paragrafo Único. As informações referentes ao monitoramento descrito no *caput* do artigo deve seguir a convenção estipulada pelo artigo 4º do presente instrumento.

Art. 9º. Não é permitido suprimir, omitir ou mascarar a identificação da Conta de Usuário a qualquer serviço da Internet, exceto para os serviços que permitem apenas conexão anônima, não sendo permitido também o uso de mecanismos de dissimulação do usuário, como re-mailers (envio de e-mails anônimo), IP Spoofing (ataque que consiste em mascarar pacotes IP utilizando endereços de remetentes falsificados) e tradutores de URL.

Art. 10. A UNEB pode, sem aviso prévio, observando o descumprimento do presente instrumento, restringir o acesso a serviços da Internet, tais como sítios Web, redes de dados ponto-a-ponto e download de arquivos de modo a garantir a segurança e o bom funcionamento da rede da instituição.

Art. 11. A possibilidade de acessar qualquer serviço da Internet não implica em autorização para acessá-lo.

Seção II
Das Conexões de Rede com a Internet

Art. 12. É vedada a conexão entre qualquer rede de dados da UNEB e a Internet através de serviços de telecomunicações não autorizados pela GERINF.

Art. 13º. É vedada a utilização de dispositivos de acesso à internet não autorizados pela GERINF, em equipamentos pertencentes à UNEB.

Art. 14º. Toda comunicação entre computadores remotos e as redes da UNEB, através da Internet ou outra rede pública, deve ser autenticada e criptografada, usando soluções tecnológicas autorizadas pela GERINF, com exceção do acesso aos conteúdos de sítios Web públicos da UNEB.

Art. 15. Toda a comunicação entre as redes da UNEB e a Internet ou qualquer outra rede pública deve, obrigatoriamente, passar por um conjunto de regras de análise de tráfego (firewall), configurado com política restritiva, com monitoramento bidirecional dos fluxos de comunicação e com proteção contra ataques cibernéticos.

Paragrafo Único. A GERINF será responsável por configurar e gerenciar a politica restritiva a qual se refere o caput do artigo de acordo com esta normativa e a legislação em vigor.

Seção III
Do Uso Aceitável da Internet

Art. 16. É permitido o acesso a sites que sejam fontes de informação necessária à execução das atividades da UNEB.

Paragrafo Único. A GERINF será responsável por analisar, autorizar, disponibilizar, gerenciar e configurar a relação de sites permitidos que trata o caput deste artigo.

Art. 17. É permitido o uso de serviços pessoais prestados através da Internet, tais como banco on-line, reservas de passagens, serviços de órgãos públicos, mídias sociais, entre outros, limitados ao estritamente necessário, sem prejuízo das atividades administrativas ou acadêmicas.

Art. 18. Não devem ser usados os recursos de “Salvar Senha” ou “Lembrar Senha”, disponíveis na maioria das aplicações (Chrome, Internet Explorer, etc), devendo ser desmarcada sempre que for apresentada esta opção.

§1º. Senhas não devem ser incluídas em nenhum outro processo de autenticação automática disponível.

§2º. A responsabilidade pela utilização de senhas é única e exclusiva do usuário, ficando ao mesmo, imputada as responsabilidades regimentais e legais sobre o mau uso das mesmas.

Art. 19. Quando estiver usando a Internet e o usuário, ao verificar que o site acessado contém conteúdo impróprio, deve abandonar o site e abrir um incidente de Segurança da Informação através de documento formal junto à GERINF.

Art. 20. Não é permitido o uso de aplicações ponto-a-ponto (peer-to-peer/ P2P), torrents e magnets links (links magnéticos) para distribuição de arquivos, tais como uTorrent,

eMule e correlatos, exceto para fins acadêmicos, mediante solicitação e aprovação da GERINF

Art. 21. Não é permitido o uso de jogos on-line, exceto para fins acadêmicos, mediante solicitação e aprovação da GERINF.

Art. 22. Ressalvados os interesses da UNEB, não é permitido:

I. o acesso a conteúdos impróprios, que são aqueles relativos à pornografia, apologia ao racismo, injúria e difamação, incitação ao ódio, invasão de computadores, entre outros previstos em lei;

II. a sondagem, investigação ou teste de vulnerabilidade em computadores e sistemas da UNEB ou de qualquer outra organização, exceto quando autorizada pela GERINF; e,

III. o uso ou a posse de ferramentas de hardware e software para sondagem, análise de vulnerabilidade, monitoramento de rede, comprometimento de sistemas, ataques e captura de dados, exceto quando autorizado pela GERINF.

Seção IV
Da Criptografia

Art. 23. Recomenda-se que toda a informação classificada como sigilosa, transmitida pela Internet, deve ser criptografada, conforme padrões de criptografia homologados pela GERINF.

Art. 24. Informações que são alvo típico de criminosos, tais como senhas de contas bancárias, números de cartões de crédito, senhas de sistemas, entre outras, não devem ser publicadas na Internet ou transmitidas via Correio Eletrônico sem criptografia.

Paragrafo Único. A responsabilidade pela utilização das informações a que se refere o caput deste artigo é imputada aos seus usuários.

Seção V
Da Legalidade

Art. 25. Sempre que as transações através da Internet ultrapassarem as fronteiras nacionais, devem ser observadas as legislações internacionais pertinentes.

Art. 26. A propriedade intelectual deve ser respeitada em qualquer atividade e sempre que os recursos computacionais da UNEB estiverem sendo usados. A reprodução ou encaminhamento de qualquer conteúdo protegido por direitos de propriedade requer a autorização do proprietário dos direitos autorais.

Art. 27º. Sempre que informações obtidas da Internet forem usadas em documentos internos, a fonte deve ser citada.

Art. 28. A indicação de direitos reservados deve ser presumida para todo conteúdo disponível na Internet, a menos que contenha informação contrária.

Art. 29. Usuários dos serviços de Internet da UNEB não podem obter, instalar, armazenar ou transmitir software não licenciado ou não homologados, conteúdos ilegais, tais como pornografia infantil, senhas de particulares, informações bancárias extraviadas, entre outros.

Seção VI
Do Download de Arquivos

Art. 30. Não é permitido o download de filmes, músicas, vídeo clips ou conteúdos semelhantes relacionados a entretenimento, exceto quando for de interesse da UNEB, mediante solicitação e aprovação da GERINF.

Art. 31. O download de arquivos com grande volume de dados deve considerar as limitações da conexão com a Internet e, sempre que possível, deve ser executado fora do horário normal de expediente.

Art. 32. O download de softwares deve obedecer aos contratos estabelecidos com os fornecedores, quando aplicável.

Art. 33. Todo arquivo obtido em fontes externas à UNEB deve ser submetido à verificação de software antivírus antes de ser utilizado.

Seção VII
Dos Softwares

Art. 34. Os ativos de software de TI devem ter seu uso racional, observando os limites de utilização estabelecidos pela GERINF.

Art. 35. É dever de todos os usuários protegerem os ativos de TI contra qualquer tipo de danos e perdas.

Art. 36. Os usuários dos ativos da TI somente estão autorizados a utilizar os softwares homologados pela GERINF. Os softwares gratuitos poderão ser utilizados apenas quando justificados, autorizados e/ou instalados pela equipe de suporte da GERINF ou coordenadores de TI.

Art. 37. É expressamente proibido instalar qualquer tipo de software, principalmente os que infrinjam quaisquer patentes ou direitos autorais e a utilização de técnicas de engenharia reversa, objetivando decompilar os softwares de propriedade da entidade.

CAPÍTULO III
DO ACESSO AOS ATIVOS DE TECNOLOGIA DA INFORMAÇÃO

Art. 38. Tem como objetivo estabelecer as diretrizes e responsabilidades para o acesso aos recursos de Tecnologia da Informação disponibilizados pela UNEB.

Parágrafo Único. Este *caput* se aplica a todos os usuários dos ativos de Tecnologia da Informação da UNEB.

Seção I
Da Concessão de Acesso

Art. 39. A licença para a utilização dos ativos de Tecnologia da Informação é uma concessão da UNEB aos usuários que necessitem deles para desempenhar suas funções.

Parágrafo Único. A utilização poderá ser monitorada em tempo real e a licença poderá ser suspensa a qualquer momento por decisão do Gestor da área do usuário ou da GERINF, de acordo com os exclusivos critérios estabelecidos pelo presente instrumento, visando evitar perda de produtividade e riscos de segurança da informação.

Art. 40. O acesso à consulta ou utilização dos recursos de Tecnologia da Informação (login) é permitido após a identificação do usuário, somente por meio de suas próprias credenciais de acesso (conta do usuário).

Art. 41. As credencias de acesso aos recursos de Tecnologia da Informação são pessoais, intransferíveis e de responsabilidade exclusiva do usuário, exceto para aqueles recursos que não suportarem a criação de credenciais individuais.

Parágrafo Único. Para os casos em que os recursos não suportem a criação de credenciais individuais, a GERINF deverá ser formalmente consultada e deverá avaliar a possibilidade de fornecer a credencial de acesso.

Art. 42. Toda solicitação, alteração, bloqueio e desbloqueio de acesso aos recursos de Tecnologia da Informação ou aos sistemas deve ser documentada.

Parágrafo Único. Os usuários deverão registar a situação à GERINF, diretamente ou através das coordenações de TI dos departamentos.

Art. 43. O Gestor, responsável institucional pelo usuário, deve informar à GERINF ou ao coordenador de informática do departamento todos os direitos de acesso que o servidor deve possuir.

Art. 44. É expressamente proibida qualquer tentativa de acesso não autorizado aos recursos de Tecnologia da Informação.

Art. 45. A utilização de contas genéricas ou contas institucionais (de colegiado, departamento, de grupos, etc) deve ser limitada ao estritamente necessário.

Art. 46. A composição do endereço eletrônico (e-mail) seguirá as regras de formação de criação de credenciais (nome de usuário e senha) definidas pela GERINF e disponíveis em site próprio.

Art. 47. Sempre que houver suspeita de que a utilização dos serviços de TIC esteja infringindo a PSI ou normas correlatas em vigor, o serviço será temporariamente suspenso pela GERINF até que se complete a apuração dos fatos.

Seção II
Da Conexão de Equipamentos

Art. 48. Somente dispositivos autorizados pela GERINF poderão ter acesso aos recursos de rede da UNEB.

Art. 49. O uso de Access Points (dispositivos que realizam interconexão entre outros dispositivos numa rede) não será permitido na rede da UNEB sem a prévia autorização da GERINF.

Parágrafo Único. Mesmo com a prévia autorização da GERINF, access points domésticos terão acesso limitado tanto de conteúdo quanto de largura de banda.

Seção III
Do Gerenciamento de Senhas

Art. 50. A elaboração de senhas para acesso à rede ou aos sistemas deve ser realizada conforme procedimento estabelecido pela GERINF, o qual deve prever troca periódica de senhas, senhas de difícil dedução e bloqueio automático da sessão por inatividade.

Art. 51. Todas as contas de usuário devem ter suas senhas alteradas no primeiro acesso na rede e nos sistemas de informação, para assegurar sua confidencialidade.

Art. 52. Os critérios para elaboração, manutenção e gerenciamento dos acessos devem levar em consideração a criticidade das informações e as necessidades dos processos de negócio envolvidos.

Seção IV
Da Análise Crítica

Art. 53. Os direitos de acesso dos servidores à rede e aos sistemas devem ser revisados periodicamente.

Art. 54. O servidor em estado de afastamento definitivo da UNEB deve ter seu acesso revogado, quando for o caso, à rede de dados e demais serviços tecnológicos.

Art. 55. Os direitos de acesso dos servidores em afastamento temporário devem ser suspensos no período da ausência, exceto para uso de sua conta de e-mail.

Art. 56. Os direitos de acesso dos servidores em transferência interna, setores e departamentos, devem ser revistos com vistas à adequação aos serviços específicos da área em que passa a atuar.

Seção IV
Das Competências

Art. 57. Cabe à Pró-Reitoria de Gestão de Pessoas (PGDP) informar à GERINF sobre a contratação, o afastamento (definitivo ou temporário) e transferência de setores e ou departamento dos servidores.

Parágrafo Único. É responsabilidade da PGDP dar conhecimento aos servidores públicos (Técnicos/analistas e docentes) da Universidade do Estado da Bahia, bem

como coletar suas assinaturas no Termo de Responsabilidade do Usuário de TI da UNEB.

Art. 58. Cabe a Secretaria Geral de Cursos (SGC) informar à GERINF sobre a matrícula, o afastamento (definitivo ou temporário) dos usuários quando tratar de discentes.

Art. 59. Cabe ao gestor de cada setor da UNEB solicitar à GERINF a liberação e suspensão do acesso à rede de dados da UNEB para os colaboradores terceirizados e estagiários sem vínculo com o estado que prestem serviço sob sua coordenação.

Parágrafo Único. É responsabilidade do gestor de cada setor da UNEB dar conhecimento aos colaboradores terceirizados e estagiários sem vínculo com o estado que prestem serviço sob sua coordenação, bem como coletar suas assinaturas no Termo de Responsabilidade do Usuário de TI da UNEB.

Art. 60. Cabe aos Colegiados, Secretarias de programas de Pós-Graduação e Unidade Acadêmica de Educação a Distância (UNEAD) solicitar à GERINF a liberação e suspensão do acesso à rede de dados da UNEB para os pesquisadores vinculados aos seus Cursos/Programas que não possuem vínculo efetivo com a UNEB.

Parágrafo Único. É responsabilidade dos Colegiados, Secretarias de programas de Pós-Graduação e Unidade Acadêmica de Educação a Distância (UNEAD) dar conhecimento aos pesquisadores vinculados aos seus Cursos/Programas que não possuem vínculo efetivo com a UNEB, bem como coletar suas assinaturas no Termo de Responsabilidade do Usuário de TI da UNEB.

Art. 61. Cabe a GERINF definir, gerenciar e controlar os serviços de Tecnologia da Informação disponibilizados na Universidade.

Parágrafo Único. A GERINF deverá disponibilizar em sitio web as instruções normativas regulamentadoras da utilização de cada serviço de TI ofertado na Universidade.

CAPÍTULO IV
DO ACESSO E UTILIZAÇÃO DO E-MAIL

Art. 62. Tem como objetivo definir as diretrizes de acesso e utilização segura do Correio Eletrônico disponibilizado pela Universidade do Estado da Bahia - UNEB.

Parágrafo Único. Este caput se aplica a todos os usuários que utilizam o serviço de Correio Eletrônico disponibilizado pela Universidade do Estado da Bahia - UNEB.

Art. 63. O serviço de Correio Eletrônico corporativo é uma concessão da UNEB, sendo assim, seu uso é permitido somente para as atividades profissionais e acadêmicas de servidores, colaboradores terceirizados e discentes, não sendo permitido enviar ou arquivar mensagens não relacionadas às finalidades supracitadas, a exemplo de, mas não limitado a:

I- assuntos que provoquem assédio, constrangimento ou que prejudiquem a imagem da organização;

II- temas difamatórios, discriminatórios, material obsceno, ilegal ou antiético;

III- fotos, imagens, sons ou vídeos que não tenham relação com as atividades profissionais da organização; e,

IV- correntes de qualquer temática e/ou pensamentos que não estejam em de acordo com as atividades finalísticas da universidade.

Art. 64. O acesso ao Correio Eletrônico corporativo se dará, minimamente, pelo conjunto "Identificação do Usuário e Senha", que é pessoal e intransferível.

Art. 65. É terminantemente proibido suprimir, modificar ou substituir a identidade do remetente de uma mensagem do Correio Eletrônico.

Art. 66. Havendo indícios de que mensagens veiculadas pelo correio eletrônico possam ocasionar quebra de segurança ou violação de quaisquer das vedações constantes deste ou de outro ato normativo, a GERINF responsável pela administração do Serviço de Correio Eletrônico adotará, imediatamente, medidas para a apuração dessas irregularidades, utilizando-se dos meios e procedimentos legalmente previstos.

Art. 67. A disponibilização do Correio Eletrônico pode ser suspensa a qualquer momento por decisão do Gestor da área do servidor ou da GERINF, amparado pela não observância às condições de uso estabelecidas por esta Norma.

Art. 68. As concessões e revogações de acesso ao serviço de Correio Eletrônico devem ser autorizadas pelo Gestor da área do usuário por meio de uma solicitação de serviço à GERINF.

Art. 69. Os anexos e/ou hiperlinks das mensagens de Correio Eletrônico poderão ser bloqueados quando oferecerem riscos à Segurança da Informação.

Art. 70. A abertura de mensagens de remetentes desconhecidos, externos à UNEB deve ser avaliada pelo servidor, especialmente quando houver dúvidas quanto à natureza do seu conteúdo, como arquivos anexados não esperados ou hiperlinks para endereços externos não relacionados às atividades profissionais em curso.

Art. 71. A quantidade de destinatários deve ser limitada por mensagem, com o objetivo de coibir a prática de Spam. Cabe à GERINF estabelecer tal limite, bem como acordar com as áreas de negócio as eventuais exceções, de acordo com os interesses da UNEB.

Parágrafo Único. Cabe à GERINF divulgar em site próprio o limite estabelecido de destinatários por mensagem.

Art. 72. Todas as mensagens originárias de usuários da UNEB deverão conter a assinatura do remetente em formato padronizado, além de um aviso legal, também padronizado, referenciando a confidencialidade da informação. Esses padrões devem serão definidos pela Assessoria de Comunicação da UNEB (ASCOM).

Art. 73. Limites de armazenamento das caixas de Correio Eletrônico devem ser estabelecidos pela GERINF, considerando as necessidades dos processos de negócio que o serviço de Correio Eletrônico suporta, bem como limitações técnicas aplicáveis.

Parágrafo Único. Cabe à GERINF divulgar em site próprio o limite estabelecido de armazenamento das caixas de correio eletrônico.

Art. 74. Toda e qualquer tramitação de mensagem eletrônica de cunho profissional deve ser feita exclusivamente através do e-mail institucional fornecido pela GERINF.

§1º. As listas de distribuição da universidade conterão, exclusivamente, contas do e-mail institucional da UNEB, conforme o caput desse artigo.

§2º. Somente serão registrados chamados para qualquer serviço de suporte na UNEB, as solicitações que partirem de e-mails institucionais, conforme o caput desse artigo.

Art. 75. Todo servidor da UNEB terá direito a uma conta de e-mail institucional cujas credenciais (nome de usuário e senha) serão as mesmas fornecidas para concessão de acesso aos recursos de TI, conforme CAPÍTULO III desse documento.

CAPÍTULO V
DO GERENCIAMENTO DE INCIDENTES DE S.I.

Art. 76. Tem como objetivo normatizar o registro e o tratamento de incidentes de Segurança da Informação no âmbito da UNEB.

Parágrafo Único. Este caput se aplica a todos os usuários de informações ou recursos de Tecnologia da Informação disponibilizados pela UNEB.

Art. 77. Todo usuário deve reportar incidentes de Segurança da Informação à GERINF.

Art. 78. A GERINF deve registrar um incidente de Segurança da Informação para toda falha de segurança identificada nos recursos de Tecnologia da Informação da UNEB.

Art. 79. A GERINF deve garantir que planos de ação sejam elaborados para tratamento de incidentes, e monitorar sua implementação.

Art. 80. É vedado ao usuário intervir no tratamento dos incidentes sem a devida autorização ou qualificação.

CAPÍTULO VI
DA PROTEÇÃO CONTRA CÓDIGO MALICIOSO

Art. 81. Tem como objetivo estabelecer diretrizes para a proteção dos recursos de Tecnologia da Informação da UNEB contra ação de código malicioso, programas impróprios.

Parágrafo Único. Este *caput* se aplica a todos os usuários e recursos de Tecnologia da Informação da UNEB.

Art. 82. Os recursos de Tecnologia da Informação devem estar providos de sistemas de detecção e bloqueio de códigos maliciosos, tais como programas antivírus, programas de análise de conteúdo de Correio Eletrônico.

§1º. Caberá a GERINF, definir e implantar soluções tecnológicas que atendam ao disposto no caput do artigo.

§2º. Havendo correções ou atualizações para os sistemas de detecção e bloqueio de códigos maliciosos, as mesmas devem ser implementadas, a fim de se evitar que estes sistemas fiquem vulneráveis a códigos maliciosos ou a qualquer tentativa de acesso não autorizado.

§3º. As atualizações e as correções para os sistemas de detecção e bloqueio de programas maliciosos devem ser homologadas pela GERINF antes de aplicadas ao ambiente de produção.

§4º. Arquivos ou mídias que são utilizados nos equipamentos computacionais devem ser verificados automaticamente, quanto à contaminação por código malicioso, antes de sua utilização.

§5º. Os sistemas de detecção e bloqueio de códigos maliciosos devem prover monitoramento, em tempo de execução, dos arquivos e programas, quanto à contaminação por código malicioso.

Art. 83. Os arquivos contaminados por código malicioso devem ser imediatamente descontaminados pelo software antivírus, isolados ou removidos do sistema. Em caso de persistência do problema, o equipamento deve ser isolado até que seja sanado o problema de modo a não afetar o ambiente de produção.

Paragrafo Único. Caberá a GERINF identificar e decidir pela melhor estratégia para atender ao caput do artigo.

Art. 84. Somente mídias magnéticas e produtos de origem confiável devem ser utilizados nos equipamentos computacionais.

CAPÍTULO VII
DOS CONCEITOS E DEFINIÇÕES

Art. 85. Para fins desta Resolução entende-se por:

I- Ativos de Tecnologia da Informação: estações de trabalho, servidores, softwares, mídias e quaisquer equipamentos eletrônicos relacionados à Tecnologia da Informação, bem como processos, pessoas e ambientes;

II- Autenticação: processo de verificação que confirma se uma entidade ou um objeto é quem ou o que afirma ser, incluindo, em alguns exemplos, a confirmação da origem e da integridade das informações, tal como a verificação de uma assinatura digital ou da identidade de um utilizador ou de um computador;

III- Código Malicioso: termo genérico que se refere a todos os tipos de programa especificamente desenvolvidos para executar ações danosas em recursos de Tecnologia da Informação, tais como vírus, cavalo de tróia, spyware, worms, entre outros;

IV- Confidencialidade – propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

V- Conta de Usuário: credencial de acesso à rede ou sistemas, de uso pessoal, intransferível e de responsabilidade de seu usuário designado;

VI- Conta Genérica: credencial de acesso à rede que não identifica o usuário que a utiliza;

VII- Conta Correio Eletrônico - é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação;

VIII- Credencial de Acesso: elemento utilizado para autenticar um usuário perante recursos de Tecnologia da Informação, tais como nome de usuário e senha, certificado digital, informação biométrica ou equivalente;

IX- Criptografia: técnica utilizada para tornar a informação original ilegível, permitindo que somente o destinatário (detentor da chave de criptografia) a decifre;

X- Dado – representação de uma informação, instrução, ou conceito, de modo que possa ser armazenado e processado por um computador;

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

XII- Download - (Baixar) copiar arquivos de um servidor (site) na internet para um computador pessoal;

XIII- E-mail: forma reduzida para Electronic Mail - Correio Eletrônico.

XIV- Estação de Trabalho: todos os computadores e equipamentos correlatos da UNEB, inclusive dispositivos móveis;

XV- Gestão de Continuidade de Negócios: processo de gestão que identifica ameaças em potencial e os possíveis impactos às operações de negócio caso essas ameaças se concretizem. Este processo fornece um framework para que se construa uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar a reputação e a marca do órgão ou entidade e suas atividades de valor agregado;

XVI- Gestão de Riscos: atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos, incluindo, inclusive, análise, avaliação, tratamento, aceitação e comunicação dos riscos;

XVII- Hiperlink: palavras ou endereços em destaque de uma página da Internet ou mensagens de Correio Eletrônico que, ao serem clicadas, efetuam o direcionamento para outra parte do texto da mensagem ou página da Internet;

XVIII- Incidente de Segurança da Informação: representado por um único ou por uma série de eventos indesejados ou inesperados de Segurança da Informação que tenham uma grande probabilidade de comprometer as operações do negócio;

XIX- Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XX- Integridade – propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXI- Internet: consiste de milhares de redes de computadores interconectadas mundialmente e que pela sua abrangência e facilidade de uso, tem sido usada como plataforma para a prestação de um crescente número de serviços;

XXII- Log: arquivo que contém informações sobre eventos de qualquer natureza em um sistema computacional, análise forense para a elucidação de incidentes de segurança, auditoria de processos, cumprimento de exigências legais para a manutenção de registro do histórico de acessos ou eventos e para a resolução de problemas (debugging);

XXIII- Login/Logon: processo de autenticação com o objetivo de permitir o uso de um sistema computacional ou recursos de rede de forma segura;

XXIV- Logoff: processo de encerramento do uso de um sistema computacional ou recursos de rede, removendo as credenciais de acesso;

XXV- Peer-to-peer (P2P) – (Ponto a ponto) permite conectar o computador de um usuário a outro, para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens, entre outros;

XXVI- Programas Impróprios: programas utilitários utilizados para explorar vulnerabilidades ou burlar a segurança dos recursos de Tecnologia da Informação;

XXVII- Recursos de Tecnologia da Informação: estações de trabalho, servidores, redes, sistemas, serviços, banco de dados e dispositivos de interconexão;

XXVIII- Rede: estações de trabalho, servidores e outros dispositivos interligados que compartilham informações ou recursos da UNEB;

XXIX- Segurança da Informação: conjunto de processos articulados, que busca a proteção da informação de vários tipos de ameaças, para garantir a continuidade do negócio, minimizar o risco, maximizar o retorno sobre os investimentos e ampliar as oportunidades de negócio;

XXX- Tratamento de Incidentes de Segurança da Informação: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

XXXI- Termo de Responsabilidade de SI: documento que deve ser assinado pelos usuários de TI da UNEB atestando compromisso e ciência com as normas da PSI;

XXXII- Usuário: qualquer servidor seja ele docente técnico ou analista, estagiário, discente, parceiro, fornecedor, prestador de serviço ou terceiro em geral que acessa informações ou utiliza recursos de Tecnologia da Informação disponibilizados pela UNEB em local ou jornada de trabalho para este último; e,

XXXIII- Webmail: é uma interface da Internet que permite consultar e enviar Correio Eletrônico (E-mail).

CAPÍTULO VIII
DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 86. As ações de Segurança da Informação e Comunicação da UNEB deverão observar os seguintes requisitos e normativos:

I- ABNT NBR ISO/IEC 27002:2013- Tecnologia da Informação - Técnicas de Segurança - Código de prática para Controles de Segurança da Informação;

II- Decreto nº 13.473, de 28 de novembro de 2011, que instituí a política de segurança da informação nos órgãos e entidades da Administração Pública do Poder Executivo Estadual;

III- Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso à informação pública;

IV- Normas de Segurança da Informação v. 3.1. Salvador, SAEB - SGI, abr./2018;

V- Sistema de Gestão de Segurança da Informação do Poder Executivo Estadual – SGSI; e,

VI- Toda e qualquer legislação pertinente à temática em questão.