ATOS DO INSTITUTO BRASILEIRO DE INFORMAÇÃO EM CIÊNCIA E TECNOLOGIA

PORTARIA Nº 2, DE 25 DE JANEIRO DE 2018

A DIRETORA DO INSTITUTO BRASILEIRO DE INFORMAÇÃO EM CIÊNCIA E TECNOLOGIA (IBICT), DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES, no uso da competência que lhe foi delegada pela Portaria MCT nº 407, de 29 de junho de 2006, publicada no DOU de 30 de junho de 2006, e tendo em vista a Portaria MCTIC n° 5.147 de 14 de novembro de 2016, publicada no DOU de 16 de novembro de 2016, resolve:

Art. 1º Aprovar a Política de Segurança da Informação e Comunicação do IBICT, bem como as normas complementares elaboradas pelo Comitê de Segurança da Informação e Comunicação (CSIC), em atendimento ao Art. 1º da Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008.

Art. 2º Fica o CSIC responsável por divulgar, orientar e monitorar internamente o cumprimento das normas relativas à Política de Segurança da Informação e Comunicação do IBICT.

Art. 3º Cabe às coordenações-gerais e coordenações técnicas darem o suporte necessário para que o CSIC atenda ao Art. 2º.

Art. 4º A Política de Segurança da Informação e Comunicação do IBICT e suas normas complementares serão publicadas em página do sítio eletrônico do Instituto, em espaço próprio criado para essa finalidade.

Art. 5º Esta portaria entra em vigor na data de sua publicação.

CECILIA LEITE OLIVEIRA
Diretora

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO DO IBICT COM NORMAS COMPLEMENTARES

DIRETORA
Cecília Leite Oliveira

COORDENAÇÃO-GERAL DE PESQUISA E DESENVOLVIMENTO DE NOVOS PRODUTOS
Arthur Fernando Costa

COORDENAÇÃO-GERAL DE PESQUISA E MANUTENÇÃO DE PRODUTOS CONSOLIDADOS
Lillian Maria Araújo de Rezende Alvares

COORDENAÇÃO-GERAL DE TECNOLOGIAS DE INFORMAÇÃO E INFORMÁTICA
Marcos Pereira de Novais

COORDENAÇÃO DE ENSINO E PESQUISA, CIÊNCIA E TECNOLOGIA DA INFORMAÇÃO
Lena Vania Ribeiro Pinheiro

COMITÊ DE SEGURANÇA DA INFORMAÇÃO CSIC

Membros do CSIC
Tiago Emmanuel Nunes Braga (Presidente)
Benício Mendes Teixeira Júnior
Reginaldo Araújo da Silva
Ricardo Medeiros Pimenta
Virgínia Ferreira da Silva Castro
Washington Luís Ribeiro de Carvalho Segundo

Membro do Grupo de Trabalho
Henrique Denes Hildenberg Fernandes
Marcos Pereira de Novais

O Comitê de Segurança da Informação e Comunicação (CSIC) propôs a Política de Segurança da Informação e Comunicações (Posic) do IBICT em atendimento à Instrução Normativa GSI/PR nº1, de 13 de junho de 2008, que em seu Art. 1º aponta para a necessidade de que os órgãos e entidades da Administração Pública Federal, direta e indireta, implementem orientações para a Gestão de Segurança da Informação e Comunicações (GSIC)[1]. A seguir será traçado um breve histórico de como o Ibict construiu sua Política de Informação e Comunicações a fim de garantir a Segurança da Informação e Comunicações (SIC).

Em 26 de maio de 2015, por meio da Portaria nº 20, foi instituído o Comitê de Segurança da Informação e Comunicação (CSIC). Foram designados os seguintes servidores para compor o CSIC: Ricardo Crisafulli Rodrigues (nomeado Gestor da Segurança da Informação e Presidente do CSIC), Benício Mendes Teixeira Júnior, Virgínia Ferreira da Silva Castro, Washington Luís Ribeiro de Carvalho Segundo e Ricardo Medeiros Pimenta. Houve a preocupação de que todas as

Coordenações do IBICT estivessem representadas[2], uma vez que a Gestão da Segurança da Informação e Comunicações não se restringe à tecnologia da informação, mas abrange também segurança física, segurança lógica, segurança orgânica e segurança organizacional dos processos institucionais estratégicos, operacionais e táticos, entre outros. (Art. 2º, VII, IN GSI/PR nº1, de 13 de junho de 2008).

Uma das principais incumbências do CSIC era a de instituir e aprovar uma Política de Segurança da Informação e Comunicações (Posic) para o Instituto. Esse trabalho teve início já na primeira reunião do Comitê, ocorrida em 8 de julho de 2015 (conforme registrado em Ata). Ficou entendido, desde o início, que o trabalho deveria se apoiar na Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, e na Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal (2015-2018). Sendo assim, diante de uma minuta da POSIC já existente (elaborada pelo Consultor Leandro Pfeifer Macedo, Projeto 914BRA2015, Edital nº 03/2014, Ibict/Unesco), o Comitê passou a realizar uma série de revisões no documento, a fim de adequá-lo à realidade institucional, assim como às orientações mais recentes do Governo Federal.

Com o objetivo de contemplar toda a Segurança da Informação e Comunicações do Instituto, ficou entendido que a Posic deveria conter uma série de normas, as quais seriam chamadas "Normas Complementares", e que elas comporiam a política como anexos. Isso permitiria que o texto principal da Posic ficasse mais claro e direto em seus direcionamentos, e que os anexos contemplassem as questões mais específicas. Essa decisão permitiria também que novos anexos fossem criados ao longo do tempo, sem necessidade de alteração no texto principal. Assim, a primeira composição do CSIC estabeleceu nova versão para o texto da Posic e cinco Normas Complementares: Controles de Acesso e Circulação, Correio Eletrônico, Recursos Computacionais, Utilização da Internet e Intranet e Utilização de Telefones Celulares, Fixos e Outros Recursos Comunicacionais.

Em 9 de dezembro de 2016, por meio da Portaria nº 65, Ricardo Crisafulli Rodrigues, então Gestor da Informação e Presidente do CSIC, foi substituído por Tiago Emmanuel Nunes Braga, que deveria continuar a coordenação, o desenvolvimento e a execução das atividades em voga. Uma das medidas tomadas foi a ampliação do CSIC com a inserção de dois novos membros (Portaria Ibict nº 26 de 10 de abril de 2017): Reginaldo de Araújo Silva (Coordenador de Administração do Ibict) e Henrique Denes Hildenberg Fernandes (servidor da Coordenação-Geral de Tecnologias de Informação e Informática – CGTI). O intuito foi trazer ao comitê necessidades e processos da Administração e mais conhecimento da área de tecnologia da informação.

Diante da premência e urgência de publicação da Posic, foi instituído um Grupo de Trabalho (GT) por meio da Portaria Ibict nº 25 de 10 de abril de 2017. Foram designados os seguintes membros: Tiago Emmanuel Nunes Braga (Presidente), Benício Mandes Teixeira Junior, Virgínia Ferreira da Silva Castro, Washington Luis Ribeiro de Carvalho Segundo, Ricardo Medeiros Pimenta, Marcos Pereira Novaes e Henrique Denes Hildenberg Fernandes. Esse GT deveria trabalhar juntamente com o CSIC na revisão e complementação do documento da política. Nesse processo, foi estabelecido um sistema criterioso de leitura e validação da Posic e de todas as suas Normas Complementares. Ao fim do processo, outras três Normas Complementares foram acrescentadas: Estrutura Física e Rede Elétrica (nobreak, motor gerador, refrigeração e prevenção de incêndio), Rede Cabeada e Wireless, e Acesso Físico e Lógico.

Após esse esforço conjunto que visou contemplar a diversidade de atuação do Ibict, o Comitê de Segurança da Informação e Comunicação apresenta a Política de Segurança da Informação e Comunicações e suas Normas Complementares. Foi um longo percurso de discussão que envolveu servidores das mais diversas áreas de atuação do Ibict e que culmina agora com a apresentação deste conjunto de documentos que almejam fortalecer diretrizes, critérios e suporte suficientes à implementação Segurança da Informação e Comunicações do IBICT.

Boa leitura!

Atenciosamente,
Equipe do Comitê de Segurança da Informação e Comunicação.

[1] A Controladoria Geral da União (CGU) também salientou a necessidade de o Instituto tratar estrategicamente as questões relativas à segurança da informação. Para tanto, seria necessário nomear um Gestor da Segurança da Informação, instituir o Comitê de Segurança da Informação e Comunicação e estabelecer uma Política de Segurança da Informação e Comunicações para o Ibict (Relatório de Auditoria nº 201405620 e Parecer nº 201405620).

[2] Coordenações do Ibict à época: Coordenação Geral de Pesquisa e Desenvolvimento de Novos Produtos (CGPD); Coordenação-Geral de Pesquisa e Manutenção de Produtos Consolidados (CGPM); Coordenação-Geral de Tecnologias de informação e Informática (CGTI), Coordenação de Ensino e Pesquisa, Ciência e Tecnologia da Informação (Coep) e a Coordenação de Planejamento, Acompanhamento e Avaliação (Copa).

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO IBICT

Capítulo I
Objetivo e Abrangência

Art. 1º A Política de Segurança da Informação e Comunicações (Posic) do Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict) tem por objetivo fornecer diretrizes, critérios e suporte para a implementação da segurança da informação e comunicações no Instituto.

Art. 2º A Política de Segurança da Informação é o instrumento que regula a proteção dos dados, informações e conhecimentos da instituição, com vistas à garantia de disponibilidade, integridade, confidencialidade e autenticidade.

Art. 3º A Posic e suas Normas Complementares aplicam-se a servidores, prestadores de serviços, colaboradores, bolsistas, estagiários, consultores externos, visitantes e a quem, de alguma forma, execute atividades vinculadas ao Instituto.

Art. 4º Os contratos, convênios, acordos e outros instrumentos relativos a atividades e parcerias celebrados pelo Ibict – com órgãos e entidades públicas ou privadas – devem atender à Posic.

Capítulo II
Diretrizes

Art. 5º São diretrizes da Posic:

I – a preservação da disponibilidade, integridade, confiabilidade e autenticidade dos dados, informações e conhecimentos que compõem os ativos de informação do Ibict;

II – a garantia de continuidade das atividades institucionais;

III – a economicidade nas ações de proteção dos ativos de informação;

IV – a pessoalidade, utilidade e finalidade do acesso aos ativos de informação;

V – a responsabilização do usuário pelos atos que comprometam a segurança do sistema de informação.

Capítulo III
Orientações Gerais

Art. 6º O planejamento da Segurança da Informação e Comunicações do Ibict e o Planejamento Estratégico Institucional (Plano Diretor da Unidade - PDU), bem como os demais planos institucionais, devem estar alinhados.

Art. 7º Deve-se planejar e investir recursos necessários ao fortalecimento da segurança dos ativos de informação.

Art. 8º Deve ser favorecido o desenvolvimento de habilidades, aperfeiçoamento e atualização profissional adequados à demanda institucional em Segurança da Informação e Comunicações (SIC) e Segurança Cibernética (SegCiber).

Art. 9º Deve-se estimular continuamente a pesquisa, o desenvolvimento e a inovação em SIC.

Art. 10. Deve-se atuar de forma colaborativa para o desenvolvimento e a evolução do sistema de SIC. É indispensável buscar a articulação e o fortalecimento de ações colaborativas e de parcerias com o setor público, privado, academia e terceiro setor, no Brasil e no exterior.

Art. 11. O arcabouço normativo em SIC e SegCiber deve ser implementado de modo abrangente, estimulando o estabelecimento de patamares cada vez mais altos de maturidade institucional nesses temas.

Art. 12. Devem ser contempladas ações para o autodiagnóstico anual, bem como ações para o desenvolvimento de mecanismos internos de acompanhamento e avaliação sistemática do nível de maturidade, objetivando a excelência dessas áreas.

Capítulo IV
Orientações Específicas

Art. 13. Todos os mecanismos de proteção utilizados para a segurança da informação devem ser mantidos e preservados para o regular exercício das funções institucionais.

Art. 14. O gerenciamento dos ativos de informação deverá observar suas normas operacionais e procedimentos específicos, a fim de garantir sua operação segura e contínua.

Art. 15. O cumprimento da Posic e suas normas complementares será monitorado periodicamente pelo Comitê Gestor de Tecnologia de Informação (Cogeti).

Art. 17. As medidas de proteção devem ser planejadas e os gastos na aplicação de controles devem ser compatíveis com o valor do ativo protegido.

Art. 18. O acesso às informações, sistemas e instalações depende da apresentação de identificador único, pessoal, intransferível e com validade estabelecida, que permita de maneira clara e indiscutível o seu reconhecimento.

Art. 19. Para garantir o cumprimento das normas, os responsáveis pela Diretoria, Coordenações-Gerais, Coordenações Técnicas, Divisões e Seções deverão auxiliar no controle da Posic, dentro das suas prerrogativas.

Parágrafo Único. Cabe aos responsáveis citados acima manter a análise de riscos atualizada junto ao Comitê de Segurança da Informação e Comunicação (Csic).

Art. 20. Todos os funcionários do Ibict (servidores, estagiários, bolsistas e terceirizados) e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional e que sejam usuários dos ativos sigilosos, devem assinar Termo de Compromisso quanto ao sigilo dos dados, informações e conhecimentos do Ibict.

Capítulo V
Segurança em Recursos Humanos

Art. 21. A responsabilidade pela segurança da informação em relação aos Recursos Humanos é de cada Chefia imediata, que deverá observar os seguintes itens:

§ 1º Todos os usuários devem ser conscientizados e treinados nos procedimentos de segurança da informação;

§ 2º O controle operacional de uma atividade crítica não pode ser atribuição exclusiva de uma única pessoa;

§ 3º Quando do afastamento, mudança de responsabilidades e de lotação ou atribuições dentro da equipe, faz-se necessária a revisão imediata dos direitos de acesso e uso dos ativos junto à Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (Etir);

§ 4º Quando da efetivação do desligamento de usuário, deverão ser desativados todos os direitos de acesso e uso dos ativos a ele atribuído, o que deverá ser feito junto à Etir;

§ 5º Os ativos produzidos pelo usuário desligado deverão ser avaliados e selecionados para serem mantidos pelo Ibict, garantindo o reconhecimento e o esclarecimento da propriedade do acervo para a instituição.

Capítulo VI
Organização da Segurança da Informação

Art. 22 A estrutura de Gestão de Segurança da Informação e Comunicações (Gsic) do Ibict possui a seguinte composição:

I – Comitê Gestor de Tecnologia da Informação (Cogeti);

II – Comitê de Segurança da Informação e Comunicações (Csic);

III – Gestor de Segurança da Informação e Comunicações;

IV – Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (Etir);

V – Gestor do Ativo de Informação e

VI – Coordenador-Geral de Tecnologia da Informação e Informática (CGTI).

§ 1º A Gsic do IBICT deve auxiliar a Diretoria na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e necessidades operacionais prioritárias do Instituto e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências.

§ 2º A Estrutura de Gsic deve planejar medidas de proteção e balancear os custos na aplicação de controles, de acordo com os danos potenciais de falhas de segurança.

Capítulo VII
Competências e Responsabilidades

Art. 23. Compete à Diretoria:

I – assegurar que a implementação dos controles de segurança da informação tenha uma coordenação e permeie toda a organização; e

II – assegurar os recursos necessários para a implementação e gestão da Posic.

Art. 24. Compete ao Comitê Gestor de Tecnologia de Informação (Cogeti):

I – definir critérios e mecanismos para o acompanhamento periódico destinado a aferir o cumprimento da Posic e suas Normas Complementares;

II – manifestar-se sobre a Posic e Normas Complementares, com posterior encaminhamento à Diretoria, para aprovação;

III – designar o Comitê de Segurança da Informação, o Gestor de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

Art. 25. Compete ao Comitê de Segurança da Informação e Comunicações (Csic):

I – promover a cultura de segurança da informação e comunicações;

II – assessorar na implementação das ações de segurança da informação e comunicações;

III – solicitar apurações quando da suspeita de ocorrências de quebra de SIC;

IV – acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

V – propor recursos necessários às ações de segurança da informação e comunicações;

VI – constituir grupos de trabalho para tratar de temas e propor estudos e soluções específicas sobre segurança da informação e comunicações;

VII – propor alterações na Posic;

VIII – definir estratégias para a implantação da Posic;

IX – propor e editar Normas Complementares relativas à segurança da informação e comunicações;

X – sistematizar a análise de risco, explicitando o estado corrente da organização;

Art. 26. Compete ao Gestor de SIC:

I – presidir o Comitê de Segurança da Informação e Comunicações;

II – coordenar o Comitê de Segurança da Informação e Comunicações; e a equipe de tratamento e resposta a incidentes em redes computacionais;

III – acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

IV – manter contato direto com o Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSI) para o trato de assuntos relativos à segurança da informação e comunicações;

V – coordenar a execução dos programas, planos e projetos relativos à disseminação da Posic.

Art. 27. Compete à Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais (Etir):

I – disponibilizar, de forma imediata e segura, condições para o reestabelecimento dos serviços de infraestrutura de informações e comunicações do Ibict;

II – facilitar as atividades de tratamento e resposta a incidentes de segurança;

III – tratar a SIC enquanto recursos de tecnologia da informação e comunicação, atuando sobre todos os ativos de infraestrutura;

IV – agir proativamente, com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de redes por meio de verificações de conformidade;

V – realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, buscando causas, danos e responsáveis;

VI – analisar ataques, vulnerabilidades e intrusões na rede do Ibict;

VII – executar as ações necessárias para tratar quebras de segurança e obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes.

VIII – supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas e dispositivos de segurança da informação;

IX – identificar controles físicos, administrativos e tecnológicos para mitigação do risco;

X – recepcionar, organizar, armazenar e tratar adequadamente as informações de eventos e incidentes de segurança, determinando aos respectivos gestores as ações corretivas ou de contingência em cada caso;

XI – produzir relatórios síntese de incidentes de segurança da informação para o Cogeti e para o Csic.

Art. 28. Compete ao Gestor do Ativo de Informação:

I – planejar, coordenar, supervisionar e orientar a execução das atividades da Equipe de Tratamento de Incidentes de Rede (Etir);

II – atuar para a garantia da segurança dos ativos de informação;

III – definir e gerir os requisitos de segurança para os ativos de informação em conformidade com esta Posic;

IV – comunicar à Etir a ocorrência de incidentes de SIC;

V – designar custodiante dos ativos de informação, quando aplicável;

VI – proteger e manter as informações, bem como controlar o acesso, conforme requisitos definidos pelo gestor da informação e em conformidade com esta Posic.

Art. 29. Compete ao titular da Diretoria e de cada Coordenação-Geral, Coordenação Técnica, Divisão e Seção:

I – responsabilizar-se pelo acompanhamento das condutas realizadas por aqueles que estão sob sua responsabilidade;

II – conscientizar os usuários sob sua supervisão em relação à Posic, bem como aos conceitos e às práticas de SIC;

III – incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SIC;

IV – tomar as medidas necessárias para que sejam aplicadas ações administrativas nos casos de comprometimento da SIC por parte dos usuários sob sua supervisão;

V – informar à Divisão de Recursos Humanos e à Etir a movimentação de pessoal de sua unidade;

VI – realizar o tratamento e a classificação da informação conforme plano de classificação da informação do Ibict;

VII – autorizar, de acordo com a legislação vigente, a divulgação das informações produzidas na sua unidade administrativa, de acordo com suas prerrogativas;

VIII – comunicar à Etir os casos de quebra de segurança;

IX – manter lista atualizada dos ativos de informação sob sua responsabilidade, com seus respectivos gestores;

X – conceder e revogar acessos aos ativos de informação, dentro de suas prerrogativas.

Art. 30. Cabe aos terceiros e fornecedores, conforme previsto em contrato:

I – observar, no exercício de suas atividades, a íntegra desta Posic e Normas Complementares;

II – tomar conhecimento desta Posic;

III – fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato; e

IV – fornecer toda a documentação dos sistemas, produtos e serviços relacionados às suas atividades.

Art. 31. Cabe aos usuários:

I – observar, no exercício de suas atividades, a íntegra desta Posic e Normas Complementares;

II – obedecer aos requisitos de controle especificados na Posic e Normas Complementares;

III – comunicar os incidentes que afetam a segurança dos ativos de informação e comunicações à Etir.

Capítulo VIII
Normas Complementares

Art. 32. O regimento da Posic no âmbito do Ibict está estruturado em Normas Complementares que devem ser expressamente cumpridas;

§ 1º À medida que forem sendo editadas, as normas complementares deverão ser publicadas por meio de portaria e devem ser divulgadas em boletim interno da instituição.

§ 2º A Posic e suas Normas Complementares devem estar disponíveis na Internet e Intranet.

§ 3º Em nenhuma hipótese será permitido o descumprimento da Posic e suas Normas Complementares pela alegação de desconhecimento das mesmas por parte do usuário.

Capítulo IX
Penalidades

Art. 33. O descumprimento das disposições constantes nesta Política e nas Normas Complementares sobre segurança da informação e comunicação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil;

Art. 34. O usuário que fizer uso de forma indevida ou não autorizada dos recursos de tecnologia da informação, bem como agir em desacordo com os termos desta Política, fica sujeito à aplicação das penalidades previstas na Lei 8.112/90 e na legislação pertinente;

Art. 35. Os casos omissos e as dúvidas com relação a esta Posic serão submetidos ao Comitê de Segurança da Informação e das Comunicações.

Capítulo X
Atualização e Vigência

Art. 36. Esta Posic deve ser revisada anualmente, podendo ser atualizada a qualquer tempo.

Parágrafo único. Recomenda-se a atualização da Posic a cada 3 (três) anos.

Art. 37. Este documento entra em vigor na data de sua publicação.

CECILIA LEITE OLIVEIRA
Diretora

ANEXO I

Norma complementar: Estrutura física, rede elétrica, nobreak, grupo gerador, sistema contra incêndio e climatização

Tipo: Norma complementar de segurança da informação e comunicações
Elaborado por: Comitê Gestor de Segurança da Informação e Comunicações
Aprovado por: Comitê Gestor de Tecnologia de Informação
Área de aplicação: IBICT
Versão: 01/2017
Vigente a partir da data de sua publicação

Objetivo

Estabelecer critérios para manutenção, acesso, prevenção, segurança e utilização do Datacenter e seus ativos.

Resultados esperados

Espera-se que a aplicação da norma garanta a alta disponibilidade no funcionamento da infraestrutura do Datacenter, aumentando a vida útil dos equipamentos e diminuindo interrupções não programadas do serviço.

Diretrizes Gerais

1. Estrutura Física do Datacenter

I. O piso deve ser elevado e o teto falso (forro), facilitando com isso a passagem de cabos de dados e de energia elétrica, a distribuição das linhas de comunicação, a remoção rápida, caso necessário, insuflamento de ar condicionado além de servir como meio para a instalação de diversos dispositivos, como luminárias, sensores e câmeras;

II. Todo o material de alvenaria utilizado deve ser resistente, não inflamável, não desprender partículas e impermeável;

III. As paredes devem ser de concreto ou alvenaria, capazes de suportar impactos ou furações. O ambiente não deve possuir janelas ou outras aberturas, somente uma porta corta-fogo. O conjunto deve garantir no mínimo uma hora de resistência ao fogo a uma temperatura de 1.260º C;

IV. A iluminação deve contribuir com a segurança e a produtividade do ambiente. Possuir índice de iluminação não inferior a 500 lux [9] medidos a 1m do piso. Não pode haver ofuscamento da visão, pontos escuros, bem como reflexo nos monitores.

V. Recomendações específicas de iluminação para equipamentos adquiridos devem ser contempladas, de modo que não interfiram no funcionamento dos demais equipamentos presentes na sala; e

VI. Elementos de PVC e cortinas devem ser evitados, assim como carpetes, devido ao acúmulo de poeira.

2. Sistema de Climatização do Datacenter

I. Devem ser utilizados equipamentos de “ar-condicionado de precisão”;

II. O controle de temperatura do Datacenter deve ser realizado por equipamentos preparados para operar em missão crítica (ininterruptamente);

III. Não pode haver oscilação térmica no Datacenter;

IV. Deve-se utilizar sistemas autocontidos ou confinados com parte superior do corredor fechada e porta de acesso instalada;

V. Devem ser adotadas as metodologias do sistema de corredor quente e corredor frio além do insuflamento sob o piso elevado, a fim de garantir maior controle do fluxo de ar no Datacenter e eliminar pontos de calor;

VI. O Datacenter deve estar configurado para utilizar fileiras de racks de frente para outra fileira;

VII. Deve-se disponibilizar exaustores para retirada do ar quente proveniente dos corredores de ar quente; e

VIII. Deve-se garantir manutenção preventiva e corretiva do sistema de climatização do datacenter.

3. Sistema de Prevenção e Combate de Incêndio do Datacenter

I. A prevenção de incêndios se dará a partir do uso de equipamento certificado e atualizado de detecção e combate de incêndio dentro do ambiente do Datacenter;

II. Compõem o sistema combate e prevenção contra incêndios os seguintes itens: sistema de detecção de fumaça, extintores, gases inibidores e procedimentos de brigadas de incêndio;

III. Deve-se utilizar detectores de fumaça e detectores de câmaras de aspiração;

IV. Os sensores de detecção deverão seguir a norma ABNT NBR 9441.;

V. O sistema de detecção deve possuir preferencialmente conexão automática com o sistema de liberação de gases para a extinção do fogo; conexão manual, com a liberação do gás extintor por um comando ou o uso de extintores de CO2 que devem ser alocados em número e local adequados dentro do recinto.

VI. Extintores de água ou pó químico devem ser evitados, devido aos danos que podem causar a equipamentos eletrônicos;

VII. No combate automático por gás, deve-se utilizar gás FM200;

VIII. As paredes do datacenter devem suportar temperatura de no mínimo 1.260º C por uma hora;

IX. Os materiais utilizados no Datacenter devem ser compostos de materiais antichamas, com ação de retardamento de propagação das chamas e com matérias-primas não combustíveis; e

X. Deve-se garantir manutenção preventiva e corretiva do sistema de prevenção e combate de incêndio.

4. Sistema de Distribuição de Alimentação Elétrica do Datacenter

I. Deve-se utilizar Sistema Ininterrupto de Energia – UPS (Uninterruptible Power Supply);

II. Deve-se projetar sistema de aterramento condizente com as demandas do datacenter e em consonância com as normas ABNT NBR-5419 e NBR-5410;

III. O sistema de aterramento deve ser isolado com destino para-raios e outro sistema de aterramento separado para o Datacenter, eletrocalhas, racks e piso elevado;

IV. Deve-se utilizar sistema de energia de emergência;

V. Os geradores precisam ser dimensionados para suportar todas as cargas necessárias ao funcionamento dos equipamentos do Datacenter durante uma possível falta de energia da concessionária;

VI. Os nobreaks devem assegurar o suprimento contínuo de energia em caso de falha de transformadores ou de fornecimento de energia elétrica pela concessionária por no mínimo 15 minutos, além de conter sistema de monitoramento remoto para alertar quaisquer falhas de funcionamento do sistema de nobreaks e estabilizadores; e

VII. Deve-se garantir manutenção preventiva e corretiva do sistema de alimentação e distribuição de energia elétrica.

ANEXO II

Norma complementar
Link e Redes cabeada e wireless

Tipo: Norma complementar de segurança da informação e comunicações
Elaborado por: Comitê Gestor de Segurança da Informação e Comunicações
Aprovado por: Comitê Gestor de Tecnologia da Informação
Área de Aplicação: IBICT
Versão: 01/17
Vigente a partir da data de sua publicação

Objetivo

Estabelecer critérios para administração e utilização das redes LAN de cabeamento metálico e wireless.

Resultados esperados

Espera-se que a aplicação da norma garanta alta disponibilidade e desempenho no funcionamento da infraestrutura de rede, segurança das informações trafegadas e diminuição nas interrupções não programadas do serviço.

Diretrizes Gerais

1.Rede LAN de cabeamento metálico

I. Esta norma se aplica ao enlace de conexão entre o Ibict e seu provedor, o POP-DF, às conexões do núcleo da rede, de distribuição, de acesso e aquelas internas do Datacenter;

II. Os usuários terão acesso unicamente às conexões (portas RJ-45) que lhes forem atribuídas pela Dired;

III. O uso de mais de uma conexão (porta RJ-45) por um mesmo usuário deverá ser autorizado pela CGTI;

IV. As portas que dão acesso aos compartimentos por onde passam o cabeamento metálico devem permanecer fechadas; as chaves devem ficar sob a guarda da equipe de vigilância e, sempre que for necessária a manutenção nos compartimentos por prestadores de serviço, esta deverá ser acompanhada por colaborador designado pela CGTI;

V. Todos os cabos deverão possuir identificadores visuais nas duas pontas: switch e conector com o usuário;

VI. Usuários em trânsito por outra unidade do Ibict estão autorizados a utilizar conectores disponíveis, devendo solicitar a conexão à Disup;

VII. Fica vedado todo procedimento de manutenção, instalação, desinstalação, configuração e/ou modificação nos cabos e conexões sem o conhecimento e aprovação da Dired;

VIII. As portas dos switches somente devem estar ativas, se estiverem em efetivo uso, havendo controle do ponto de acesso conectado a cada porta; e

IX. A Dired será responsável pelo monitoramento e gerenciamento das conexões da Rede LAN existentes, visando garantir o seu uso de modo seguro e dentro dos padrões exigidos para o seu bom funcionamento.

2.Rede sem fio

I. É permitido o uso e a conexão de smartphones, tablets, notebooks e quaisquer outros dispositivos wireless às redes sem fio do Ibict, desde que previamente autorizado pela Dired;

II. A credencial para acesso à rede sem fio é pessoal e intransferível, sendo proibida a divulgação da mesma pelo usuário que a recebeu;

III. Toda a conexão à rede sem fio deverá ser feita por intermédio do uso do Proxy do Ibict;

IV. Aos acessos feitos a partir da rede sem fio, aplicam-se todas as normas para utilização de Internet e Intranet, a serem estabelecidos na Posic;

V. É proibida a instalação de roteadores/access points (AP's) ou outros dispositivos de compartilhamento de rede, sem a prévio conhecimento e aprovação pela Dired; e

VI. Todos os usuários da rede sem fio do Ibict deverão ser previamente cadastrados pela equipe técnica da Dired.

ANEXO III

Norma complementar
Controle de acesso e circulação

Tipo: Norma complementar de segurança da informação e comunicações
Elaborado por: Comitê Gestor de Segurança da Informação e Comunicações
Aprovado por: Comitê Gestor de Tecnologia de Informação
Área de aplicação: IBICT
Versão: 01/2017
Vigente a partir da data de sua publicação

Objetivo

Regulamentar o acesso às dependências do IBICT.

Resultados esperados

Espera-se que a aplicação da norma garanta o controle de acesso às dependências do Ibict, colaborando para que a segurança da informação e comunicações seja alcançada.

Diretrizes Gerais

1. Do acesso ao edifício

I. O acesso regular às dependências da sede do Ibict, inclusive para visitantes e prestadores, ocorrerá nos dias úteis, das 7h às 20h, e será realizado, prioritariamente, pela entrada leste. A entrada da garagem ficará disponível durante esse horário, e se restringirá à movimentação de carga e descarga de bens e materiais além da movimentação de carros oficiais do Ibict. A entrada oeste será utilizada prioritariamente para acesso alternativo ao edifício, quando a entrada leste estiver bloqueada, ou para evacuação emergencial do edifício.

a. A entrada de visitantes e prestadores de serviços em horário diferente ao definido acima requer a autorização, por escrito, do responsável pela área para a qual o serviço foi solicitado. O documento de autorização será retido na portaria.

b. Excepcionalmente, a autorização referenciada no parágrafo anterior poderá ser concedida por contato telefônico ou comunicação verbal da equipe de segurança da entrada com a pessoa previamente habilitada.

c. Nos casos em que o acesso pela entrada leste ou garagem não for possível por qualquer motivo, será designada outra entrada para o acesso às dependências da sede do Ibict.

II. Será mantido pelo menos um segurança ou uma recepcionista na entrada da garagem do edifício sede do Ibict.

III. Para autorização de entrada de visitantes e prestadores de serviço, cabe à segurança da recepção contatar o funcionário ao qual se destina a visita, utilizando o ramal interno, e instruir o visitante sobre o trajeto a ser feito até o local desejado. Na impossibilidade de obter contato com quem se destina a visita, o setor visitado poderá autorizar a entrada do visitante por telefone. O nome do autorizador ficará registrado na portaria do edifício.

a. Os prestadores de serviços temporários podem ser cadastrados conforme período necessário, estando vinculado seu acesso ao período designado pela chefia de cada área;

IV. A equipe de segurança é responsável pelo cadastro dos visitantes e prestadores de serviços.

V. A entrada e saída de material e equipamentos do edifício somente será permitida com a autorização por escrito, podendo ser por e-mail, da área administrativa a que pertencer o bem, e deve ser acompanhada por funcionário do órgão. Entende-se como funcionário o servidor, bolsista, estagiário ou terceirizado credenciado à recepção do prédio pela chefia para executar esta atividade. A autorização apresentada deverá ser retida por membro da equipe de segurança.

VI. Os visitantes e prestadores de serviço que estiverem portando equipamentos eletrônicos, que não sejam aparelhos celulares, ao adentrarem nas dependências do Ibict, deverão declarar o bem, registrando o tipo de equipamento e o número de série. Ao saírem, deverão apresentar novamente à recepção o equipamento, para conferência. Outra opção é deixar o equipamento em depósito (guarda-volumes) sob a guarda do Serviço de Segurança, para restituição ao saírem, com a apresentação de tíquete comprobatório da propriedade.

a. Em caso de prestação de serviço a médio e longo prazo, é possível o cadastro de equipamentos como notebooks para acesso no período da prestação do serviço;

b. Os equipamentos relacionados na alínea "a" deste item devem ser etiquetados com número interno de cadastro, o nome da área de atuação, o nome do seu dono, seu número de série, período de utilização e código de barras, ou QRCODE, adequado com informações pertinentes; e

c. Cabe ao Serviço de Segurança informar os visitantes acerca da necessidade de cadastro dos equipamentos.

VII. Será mantido na portaria principal Livro de registro de Ocorrências para eventuais anotações relacionadas à movimentação anormal de pessoas e bens patrimoniais.

VIII. É proibido entrar nas dependências do edifício com bermuda, trajes de banho ou equivalente entre as 7h e as 20h.

a. Crianças menores de 12 anos que estejam acompanhando funcionário poderão trajar bermudas e uniformes escolares.

IX. Não é permitido o ingresso, a permanência ou a circulação de animais, inclusive cães, gatos e aves canoras na entrada e no interior do edifício. Ressalva para cão-guia.

2. Do uso de identificação

I. Os servidores, bolsistas, estagiários e terceirizados receberão crachá de identificação a ser fornecido pelo Ibict. Os visitantes e prestadores de serviço receberão adesivo de identificação na recepção, mediante a apresentação de identidade.

II. É obrigatório o uso de crachá ou adesivo de identificação, de forma visível, para circular nas dependências do edifício.

III. O crachá deverá conter o nome, função e fotografia, além de outros elementos de caracterização;

a. O crachá deverá seguir os padrões do governo federal, podendo ser utilizado como identificação pessoal, desde que tenha uma validade associada;

IV. O visitante ou prestador de serviço deverá restituir o adesivo utilizado ao Serviço de Segurança ao sair do edifício.

V. O crachá ou adesivo de identificação é de uso pessoal e intransferível, sendo vedado o seu empréstimo ou cessão a terceiros. A reponsabilidade por problemas causados pelo uso indevido do crachá ou adesivo é exclusivamente do seu portador.

VI. Em caso de extravio ou roubo do crachá, seu portador deverá comunicar o fato por escrito à área administrativa do órgão no prazo máximo de 5 dias úteis.

VII. Em caso de desligamento do órgão, o portador do crachá deverá devolvê-lo ao responsável pela área administrativa do órgão.

VIII. Em nenhuma hipótese será permitida a circulação e a permanência nas dependências do Ibict de pessoa sem identificação visível (crachá ou adesivo).

IX. Tratando-se de servidor do Ibict, será alertado para que coloque o crachá, ou adesivo na falta desse, registrando-se a ocorrência.

X. Na reincidência do fato previsto no item anterior, o Serviço de Segurança remeterá comunicação do evento à Autoridade Superior para a adoção de medidas cabíveis, sujeitando-se o servidor às sanções disciplinares previstas na Política de Segurança da Informação e Comunicações, por descumprimento de norma regulamentar.

ANEXO IV

Norma complementar:
Correio Eletrônico

Tipo: Norma complementar de segurança da informação e comunicações
Elaborado por: Comitê Gestor de Segurança da Informação e Comunicações
Aprovado por: Comitê Gestor de Tecnologia de Informação
Área de aplicação: IBICT
Versão: 01/2017
Vigente a partir da data de sua publicação

Objetivo

Estabelecer critérios para utilização e gerenciamento do serviço de correio eletrônico a ser utilizado pelo Ibict.

Resultados esperados

Com a aplicação da norma espera-se que as informações obtidas e enviadas a partir do serviço de correio eletrônico do Ibict possam ser resguardadas de qualquer acesso indevido, bem como de perdas.

Diretrizes gerais

1. O serviço de correio tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados com as funções do funcionário no Ibict.

I. O serviço de e-mail é um serviço institucional, desta forma está aberto a análises, avaliações e controles que a direção da instituição considerar necessárias;

II. Os e-mails individuais, excepcionalmente, poderão ser acessados por terceiros mediante autorização do Coordenador-Geral ao qual o e-mail está ligado, da Diretoria ou, havendo suspeitas de risco à segurança da informação, do Coordenador-Geral de Tecnologias da Informação e Informática juntamente com o presidente do CSIC.

III. O e-mail institucional poderá se utilizado, também, para fins particulares, estando o usuário ciente de que, sendo institucional, não há nenhuma garantia de privacidade;

IV. Os usuários podem utilizar, dentro do Ibict, e-mail pessoal, para assuntos pessoais, devendo o e-mail institucional ser utilizado, prioritariamente, para fins institucionais; e

V. São usuários do serviço de correio eletrônico corporativo os colaboradores, aqui definidos como membros e servidores do Ibict, os estagiários, bolsistas e os demais agentes públicos ou privados que oficialmente executem atividade vinculada à atuação institucional desta Casa.

2. Será disponibilizada uma única conta de e-mail para cada colaborador do Ibict.

3. O acesso ao serviço de correio eletrônico dar-se-á por meio de senha de uso pessoal e intransferível.

4. É permitida a criação de conta de e-mail para participantes de projetos ou outras atividades temporárias. Nesses casos deve haver pedido fundamentado por parte do responsável pelo respectivo projeto ou atividade a ser encaminhado à CGTI.

I. O acesso às contas de e-mail por participante de projetos ou atividades temporárias poderá ser predeterminado por período certo, desde que solicitado ao responsável pelo projeto ou atividade.

II. O acesso às contas de e-mail será bloqueado a partir do dia em que o participante de projeto ou atividade temporária for desligado do projeto; e

III. O responsável técnico pelo projeto ou atividade poderá solicitar o bloqueio do acesso temporário de participantes do projeto ou atividade a qualquer tempo.

5. Poderão ser criadas contas institucionais, devendo haver o registro da pessoa responsável por essa conta, dos participantes e o período de uso;

6. As mensagens constantes do e-mail institucional serão preservadas por um período de, no mínimo, cinco anos, permanecendo à disposição das autoridades, pesquisadores ou interessados desde que autorizado pela justiça, pelo Coordenador-Geral ao qual o e-mail está ligado, pela Diretoria ou, havendo suspeitas de risco à segurança da informação pelo Coordenador-Geral de Tecnologias da Informação e Informática juntamente com o presidente do CSIC.

7. É vedado ao usuário o uso do serviço de correio eletrônico corporativo com o objetivo de:

I. Praticar crimes e infrações penais de qualquer natureza;

II. Executar ações nocivas contra outros recursos computacionais do Ibict ou de redes externas;

III. Distribuir material obsceno, pornográfico, ofensivo, preconceituoso, discriminatório, ou de qualquer forma contrário à lei e às práticas vigentes;

IV. Disseminar anúncios publicitários, mensagens de entretenimento e mensagens do tipo "corrente", vírus ou qualquer outro tipo de programa de computador que não seja destinado ao desempenho de suas funções;

V. Enviar arquivos de áudio, vídeo ou animações de cunho pessoal;

VI. Executar outras atividades lesivas, tendentes a comprometer a intimidade de usuários, a segurança e a disponibilidade do sistema, ou a imagem institucional.

8. A Dired é responsável por disponibilizar o serviço de correio eletrônico corporativo, diretamente ou mediante contrato, competindo-lhe, ainda, o seguinte:

I. Zelar pelo atendimento aos princípios da segurança, integridade, sigilo e disponibilidade dos serviços e dados transmitidos por meio do sistema de correio eletrônico;

II. Definir os padrões e requisitos para cadastramento, concessão, utilização, suspensão ou exclusão das contas de correio eletrônico e listas de distribuição, definidas por essa Norma Complementar;

III. Manter em local seguro e restrito dados para auditoria acerca da utilização do serviço, no sentido de buscar garantir a recuperação de mensagens em caso de danos ao ambiente de rede;

IV. Suspender, motivadamente, o acesso a conta de correio, quando constatado o uso indevido dos recursos, dando imediata ciência ao respectivo titular, chefia imediata, CSIC e responsável pela apuração formal da ocorrência;

V. Manter sistema de proteção contra vírus e mensagens não solicitadas (spam) nos servidores do correio eletrônico;

VI. Restringir a transmissão de arquivos que possam significar comprometimento do serviço;

VII. Monitorar o uso do ambiente virtual, por meio de ferramentas sistêmicas, a fim de preservar a integridade das informações e identificar possíveis violações ao disposto nessa Norma Complementar;

VIII. Providenciar, sempre que necessária, a capacitação dos usuários no uso da ferramenta de correio eletrônico;

9. Cabe à Divisão de Recursos Humanos e à chefia imediata do colaborador informar à Dired, em até dois dias úteis, as ocorrências de afastamentos ou desligamentos de usuários do serviço, que importem a necessidade de suspensão ou exclusão de contas de correio eletrônico.

10. O CSIC poderá solicitar a qualquer momento log contendo informações de acesso ao correio eletrônico do Ibict com destaque para os acessos realizados por terceiros.

11. Um relatório bimestral composto por justificativas e logs sobre os acessos às caixas de e-mail de e por terceiros será enviado pela CGTI para o CSIC.

ANEXO V

Norma complementar
Recursos Computacionais

Tipo: Norma complementar de segurança da informação e comunicações
Elaborado por: Comitê Gestor de Segurança da Informação e Comunicações
Aprovado por: Comitê Gestor de Tecnologia de Informação
Área de aplicação: IBICT
Versão: 01/2017
Vigente a partir da data de sua publicação

Objetivo

Estabelecer critérios e procedimentos para o uso dos recursos computacionais disponíveis aos usuários da rede do Ibict, assim como o controle, administração e requisitos mínimos desses recursos.

Resultados Esperados

Espera-se que a aplicação da norma garanta o perfeito funcionamento dos recursos computacionais destinados à utilização por parte dos colaboradores do Ibict.

Diretrizes Gerais

1. Recursos Computacionais em Geral

I. Entende-se por recurso computacional qualquer equipamento digital de propriedade do Ibict do qual o colaborador faça uso para o exercício de suas funções.

II. O colaborador deve ter acesso unicamente àqueles recursos computacionais que forem indispensáveis e designados à realização de suas atividades no Ibict;

III. O usuário é responsável pela integridade física dos recursos computacionais a ele disponibilizados durante o uso;

IV. Recursos computacionais de propriedade do Ibict devem ser guardados em local seguro, com controle de acesso e garantia quanto à sua integridade;

V. É vedado aos colaboradores do Ibict utilizar as credenciais de acesso de outro usuário para acessar ou fazer uso de recursos computacionais;

VI. É vedado aos colaboradores do Ibict fazer uso de exploração de falhas de configuração, falhas de segurança ou tentar obter conhecimento de senhas especiais para alterar um recurso computacional;

VII. Os colaboradores que estiverem em trânsito por outra unidade do Ibict poderão utilizar os recursos computacionais da unidade em que estiverem trabalhando;

VIII. Todos os recursos computacionais deverão ser identificados pela Divisão de Material e Patrimônio (Dimpa);

IX. O colaborador que estiver utilizando equipamento de propriedade do Ibict deve assinar termo de responsabilidade sempre que solicitado por sua chefia imediata ou pela Divisão de Material e Patrimônio (Dimpa);

2. Estações de Trabalho

I. O colaborador não deve se alimentar próximo à estação de trabalho;

II. É vedado ao colaborador abrir as estações de trabalho ou modificar a configuração do hardware;

III. Sempre que se ausentar da estação de trabalho, o colaborador deve bloqueá-la para impedir o acesso não autorizado;

IV. O colaborador deve informar imediatamente à sua chefia imediata e à Disup, quando identificada violação da integridade do equipamento por ele utilizado;

V. O colaborador deve ligar/desligar de forma adequada a estação de trabalho;

VI. As atualizações de sistema ocorrerão automaticamente mediante procedimentos realizados pela CGTI/Dired/Disup;

VII. Caso o colaborador identifique a necessidade de alguma atualização, deverá comunicar à CGTI/Dired/Disup;

VIII. Todas as estações de trabalho deverão possuir o programa de antivírus homologado pela Dired e com a autoproteção ativa na estação de trabalho;

IX. O colaborador não deve cancelar o processo de verificação de vírus quando este for iniciado automaticamente na sua estação de trabalho;

X. A conexão de estações de trabalho particulares, portáteis ou não, à rede do Ibict deverá ser autorizada pela chefia imediata do usuário e solicitada junto à Dired, que realizará as verificações de segurança e conformidade cabíveis;

XI. Arquivos salvos na unidade de disco local não terão garantia de recuperação e backup automático;

XII. A concessão de credenciais de administrador será gerenciada pela Dired, que poderá, sob demanda da chefia imediata do usuário, concedê-la ou revogá-la; e

XIII. O compartilhamento de diretórios e arquivos em estações de trabalho somente deve ser realizado quando estritamente necessário para execução das atividades do usuário mediante solicitação formal à CGTI.

3. Equipamentos Portáteis

I. Os equipamentos portáteis devem respeitar as mesmas regras estabelecidas para estações de trabalho;

II. O colaborador, ao solicitar o empréstimo de recurso computacional portátil do Ibict, deve assinar o Termo de Responsabilidade junto à área que detém sua guarda;

III. Somente técnicos autorizados pela Disup devem configurar os equipamentos portáteis para acesso à rede do Ibict; e

IV. O usuário deve evitar armazenar informações confidenciais, sensíveis e/ou pessoais em equipamentos portáteis do Ibict.

4. Servidores

I. As normas complementares relativas a servidores de aplicação, dados ou de recursos de rede serão tratadas em normas complementares específicas para esse fim.

5. Servidores de Arquivo

I. Caberá à Dired configurar estrutura de diretórios no servidor de arquivos que reflitam a mesma estrutura organizacional do Ibict;

II. Tais diretórios deverão ser configurados pela Disup para carregarem na forma de uma unidade de rede nos recursos computacionais aplicáveis utilizados pelos usuários;

III. Caberá à Dired configurar um diretório pessoal para cada usuário ativo na rede do Ibict;

IV. Tal diretório deverá ser configurado pela Disup para carregar como o diretório padrão de documentos na estação de trabalho do usuário;

V. A Dired configurará os diretórios acima mencionados para que os usuários tenham acesso apenas aos arquivos pertinentes às suas atividades, com base na estrutura organizacional do Ibict, definida no regimento interno da instituição; e

VI. O colaborador deverá utilizar os diretórios acima mencionados para armazenar documentos relativos às atividades institucionais, apenas.

6. Impressoras

I. Somente os usuários previamente autorizados poderão ter acesso aos recursos de impressão;

II. A configuração da impressora na estação de trabalho do colaborador deverá ser realizada pelos técnicos autorizados pelo Disup; e

III. Os usuários não devem deixar informações críticas, sigilosas ou sensíveis da instituição em equipamentos de impressão.

7. Utilização de Software

I. No Ibict, só será permitida a utilização de softwares homologados pela CGTI/Dired/Disup;

II. O registro dos softwares homologados, do número de licenças disponíveis e dos softwares instalados nas estações de trabalho deve ser mantido atualizado pela Disup;

III. Perante a necessidade de utilização de software não homologado, a chefia imediata deverá solicitar formalmente à CGTI/Dired/Disup a homologação do mesmo contendo os seguintes itens:

a. Especificações detalhadas do software solicitado;

b. Quantidade de licenças;

c. Suporte ao software (necessidade de suporte);

d. Justificativa.

IV. Caberá à CGTI/Dired/Disup definir os critérios para homologação de software.

V. Compete ao Comitê Gestor de Tecnologia da Informação (Cogeti) deliberar sobre a aquisição de licenças e a distribuição nas unidades do Ibict, de acordo com proposta apresentada pela CGTI/Dired/Disup ou demais coordenações-gerais e diretoria;

VI. A instalação de software de outras categorias, tais como freeware (software gratuito), de domínio público (não protegido por copyright) e/ou cópias de demonstração que não sofram ação de direitos autorais, deve ser previamente requerida à CGTI/Dired/Disup;

VII. A Disup poderá remover programa de computador instalado em estação de trabalho que não se enquadre nos critérios estabelecidos nessa Norma Complementar;

VIII. Os usuários com credenciais de administrador somente poderão instalar softwares necessários ao desempenho de suas atribuições.

8. Manutenção e Configuração

I. Toda solicitação de atendimento para instalação em estações de trabalho, por meio de suporte e configuração dos recursos computacionais, deve ser efetuada mediante formalização à Disup;

II. A equipe de atendimento deve estar devidamente identificada para a execução dos serviços de suporte técnico;

III. Nas dependências físicas do Ibict somente é permitida a execução dos serviços de suporte técnico nos equipamentos de propriedade da instituição ou cedidos formalmente, sendo proibida a assistência técnica em equipamentos particulares;

IV. O colaborador deve acompanhar o técnico durante a manutenção da sua estação de trabalho quando a mesma ocorrer no local e horário de trabalho do colaborador.

V. O colaborador deverá atestar a realização de demandas de suporte quando fiscalizada;

VI. Todo equipamento que tiver a necessidade de ser deslocado para manutenção ou configuração deverá estar devidamente identificado;

VII. O colaborador ou a chefia imediata deve estar ciente da saída do equipamento de seu local de trabalho, caso seja necessária a retirada do mesmo para manutenção;

VIII. Todo recurso computacional que sair das dependências físicas do Ibict por motivo de manutenção deverá ser registrado pelo responsável pela movimentação e deverá ter suas informações institucionais críticas previamente copiadas para unidade de armazenamento, e então excluídas do recurso computacional que será retirado da instituição; e

IX. A saída do equipamento deverá ser autorizada pela Dimpa.

9. Controle e Administração de Recursos Computacionais

I. Todo recurso computacional deve ser identificado e inventariado pela Dimpa;

II. Os recursos computacionais que não são de propriedade do Ibict devem ser devidamente identificados;

III. Novas implementações, alterações e atualizações de recursos computacionais devem ser homologadas antecipadamente pela CGTI/Dired/Disup; e

IV. Os recursos computacionais devem ser monitorados e administrados pela CGTI/Dired/Disup.

ANEXO VI

Norma complementar
Utilização de telefones celulares, fixos e outros dispositivos comunicacionais

Tipo: Norma complementar de segurança da informação e comunicações
Elaborado por: Comitê Gestor de Segurança da Informação e Comunicações
Aprovado por: Comitê Gestor de Tecnologia de Informação
Área de aplicação: IBICT
Versão: 01/2017
Vigente a partir da data de sua publicação

Objetivo

Estabelecer normas, limites, proibições, responsabilidades e controle para o uso dos serviços de telefonia no Ibict.

Resultados Esperados

Espera-se que a aplicação da norma garanta segurança e economia na utilização dos serviços de telefonia do Ibict.

Diretrizes gerais

1. Cabe à Coordenação Geral de Administração controlar a aquisição, locação e utilização dos aparelhos, acessórios e equipamentos de comunicação que integram os serviços de telefonia do Ibict, igualmente, armazenar registro dos dados dos equipamentos de comunicação móvel celular, tais como: número de série do equipamento, número do código Imei de equipamentos de telefonia móvel e número de série do chip.

2. São usuários todas os colaboradores que utilizam linhas telefônicas de propriedade ou de responsabilidade do Ibict.

3. Os colaboradores são responsáveis pelos recursos telefônicos por eles utilizados, devendo preservar a sua integridade e continuidade.

4. Os serviços de comunicação de voz por meio de telefonia móvel e de dados, sua utilização e dispositivos disponibilizados pelo Ibict destinam-se às necessidades do serviço.

5. A concessão de equipamentos e linhas telefônicas deverá ser objeto de controle patrimonial, com responsabilidade pelo uso e pela guarda atribuída no ato da entrega ou instalação, através da assinatura do Termo de Responsabilidade próprio.

6. A devolução de equipamentos e linhas telefônicas, igualmente, será acompanhada de formulário de Requisição de Serviços entregue à Coordenação de Administração, que providenciará o recolhimento e alterações no controle patrimonial, quando aplicável.

7. Da utilização da rede fixa de comunicação

I. São responsáveis pela utilização das linhas fixas e equipamentos telefônicos os coordenadores e chefes de divisão da estrutura organizacional ou pessoas por eles indicados;

II. Cada setor poderá, a critério do Coordenador da área, determinar um único encarregado em controlar e atestar os históricos das contas telefônicas, devendo previamente comunicar à Coordenação de Administração; e

III. As ligações interurbanas e internacionais serão realizadas apenas para transmissão de informações e instruções breves de interesse do Ibict.

8. Da utilização da telefonia móvel

I. Os serviços de comunicação de voz por meio de telefonia móvel e de dados, sua utilização e dispositivos disponibilizados pelo Ibict são destinados aos ocupantes de cargos em comissão do Grupo-Direção e Assessoramento Superiores – DAS de níveis 5, 4 e equivalentes;

II. Em casos excepcionais, devidamente justificados, a outros servidores, no interesse da Administração Pública Federal, desde que autorizado pela autoridade máxima do Ibict.

III. O usuário de dispositivo móvel deverá assinar Termo de Responsabilidade próprio quando de seu recebimento.

IV. Os usuários dos serviços de comunicação de voz por meio de telefonia móvel e de dados, na utilização de seus dispositivos de propriedade do Ibict, deverão prezar pelo bom uso do equipamento, devendo, em caso de perda ou furto do equipamento, comunicar à Coordenação de Administração e realizar os procedimentos relativos à ocorrência.

9. É vedado ao usuário o uso do serviço de correio eletrônico corporativo com o objetivo de:

I. Praticar crimes e infrações penais de qualquer natureza;

II. Executar ações nocivas contra outros recursos computacionais do Ibict ou de redes externas;

III. Distribuir material obsceno, pornográfico, ofensivo, preconceituoso, discriminatório, ou de qualquer forma contrário à lei e às práticas vigentes;

IV. Disseminar anúncios publicitários, mensagens de entretenimento e mensagens do tipo "corrente", vírus ou qualquer outro tipo de programa de computador que não seja destinado ao desempenho de suas funções;

V. Enviar arquivos de áudio, vídeo ou animações de cunho pessoal;

VI. Executar outras atividades lesivas, tendentes a comprometer a intimidade de usuários, a segurança e a disponibilidade do sistema, ou a imagem institucional.

ANEXO VII

Norma complementar
Utilização da Internet e Intranet

Tipo: Norma complementar de segurança da informação e comunicações
Elaborado por: Comitê Gestor de Segurança da Informação e Comunicações
Aprovado por: Comitê Gestor de Tecnologia de Informação
Área de aplicação: IBICT
Versão: 01/2017
Vigente a partir da data de sua publicação

Objetivo

Estabelecer critérios para administração e utilização de acesso aos serviços de Internet e Intranet no âmbito do Ibict.

Resultados esperados

Espera-se que a aplicação da norma garanta segurança no acesso a recursos de informação disponíveis na Internet e Intranet.

Diretrizes Gerais

1. Internet

I. São usuários da Internet do Ibict os colaboradores representados por servidores, estagiários e os demais agentes públicos ou particulares que oficialmente executem atividade vinculada à atuação institucional do Ibict.

II. A internet deverá ser utilizada para fins institucionais;

III. O acesso à Internet deverá ser auditado e seus logs armazenados pela CGTI;

IV. As contas de usuários deverão ter níveis de acesso distintos, conforme a necessidade dos serviços, de acordo com os perfis definidos pela CGTI e aprovados pela COGTI;

V. Cada usuário é responsável pelas ações e acessos realizados por meio da sua Conta de Acesso;

VI. Os usuários devem estar capacitados a utilizar os serviços de modo a garantir a sua utilização adequada;

VII. É vedado o uso de provedores não autorizados no ambiente do Ibict;

VIII. A CGTI deverá prover o serviço de conexão à Internet implementando mecanismos de segurança adequados;

IX. Toda alteração de nível de acesso somente será realizada mediante solicitação formal, pela chefia imediata do usuário, contendo a devida justificativa, que será avaliada pela CGTI, podendo esta solicitação ser negada em caso de risco ou vulnerabilidade à segurança e à integridade da rede do Ibict, caso em que a solicitação deverá ser validada pela CSIC;

X. É vedado acessar páginas de conteúdo considerado ofensivo, ilegal ou impróprio, tais como:

a. pornografia, pedofilia, preconceitos, vandalismo, entre outros;

b. acessar ou obter na Internet arquivos que apresentem vulnerabilidade de segurança ou possam comprometer, de alguma forma, a segurança e a integridade da rede do Ibict;

c. uso de proxy anônimo;

d. acesso a jogos em horário de expediente, exceto aqueles definidos como ferramenta de trabalho;

e. divulgação de informações confidenciais da instituição por meio de correio eletrônico, grupos ou listas de discussão, sistemas de mensageria ou bate-papo, blogs, microblogs, ou ferramentas semelhantes;

f. contorno ou tentativa de contorno às políticas de bloqueios automaticamente aplicadas pelas ferramentas sistêmicas do Ibict;

g. utilização de softwares de compartilhamento de conteúdos na modalidade peer-to-peer (P2P);

h. tráfego de quaisquer outros dados em desacordo com a lei ou capazes de prejudicar o desempenho dos serviços de tecnologia da informação do Ibict, na forma definida pela CGTI.

XI. O usuário poderá solicitar liberação de determinada página, com a devida justificativa, mediante solicitação formal à CGTI; e

XII. A ocorrência de qualquer hipótese de má utilização da internet deverá ser comunicada, de imediato, à CGTI.

2. Intranet

I. São usuários da Intranet do Ibict os colaboradores representados por servidores, estagiários e os demais agentes públicos ou particulares que oficialmente executem atividade vinculada à atuação institucional do Ibict;

II. A Intranet deverá ser utilizada para fins institucionais;

III. O acesso à Intranet deverá ser auditado e seus logs armazenados pela CGTI;

IV. Cada usuário é responsável pelas ações e acessos realizados por meio da sua Conta de Acesso;

V. Os usuários devem estar capacitados a utilizar os serviços de modo a garantir a sua utilização adequada.

3. Navegação e Administração

I. Os navegadores de Internet e Intranet utilizados no âmbito do Ibict deverão ser homologados pela CGTI;

II. As paralisações dos serviços de Internet e Intranet para manutenção preventiva ou corretiva devem ser previamente comunicadas pela CGTI a todos os usuários; e

III. Os problemas técnicos verificados pelos usuários, ocorridos durante o acesso aos serviços de Internet e Intranet, devem ser imediatamente comunicados à CGTI para que sejam solucionados.

PORTARIA Nº 3, DE 25 DE JANEIRO DE 2018

A DIRETORA DO INSTITUTO BRASILEIRO DE INFORMAÇÃO EM CIÊNCIA E TECNOLOGIA (IBICT), DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES, no uso da competência que lhe foi delegada pela Portaria MCT nº 407, de 29 de junho de 2006, publicada no DOU de 30 de junho de 2006, e tendo em vista a Portaria MCTIC n° 5.147 de 14 de novembro de 2016, publicada no DOU de 16 de novembro de 2016, e