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

ATOS DO INSTITUTO BRASILEIRO DE INFORMAÇÃO E CIÊNCIA E TECNOLOGIA

PORTARIA Nº 25, DE 10 DE ABRIL DE 2017

A diretora do Instituto Brasileiro de Informação em Ciência e Tecnologia - IBICT, nomeada pela Portaria nº. 845, da Casa Civil da Presidência da República, publicada no D.O.U. nº 217 de 07 de novembro de 2013, no uso de suas atribuições conferidas pela Portaria MCTIC nº. 5147, de 14 de novembro de 2016, publicada no D.O.U. de 16 de novembro de 2016, resolve:

Art. 1º - Instituir o Grupo de Trabalho para Desenvolvimento da Política de Segurança da Informação (GTDPSI) do Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT).

Art. 2º - Designar os seguintes servidores para compor o Grupo de Trabalho dentro da estrutura do Comitê de Segurança da Informação e Comunicação (CSIC):

I. Tiago Emmanuel Nunes Braga (Presidente)
II. Benício Mendes Teixeira Júnior;
III. Virginia Ferreira da Silva Castro;
IV. Washington Luis Ribeiro de Carvalho Segundo;
V. Ricardo Medeiros Pimenta;
VI. Marcos Pereira Novais e;
VII. Henrique Denes Hildenberg Fernandes

Art. 3º - Finalizar o mandato dos membros do Grupo de Trabalho em maio de 2017.

Art. 4º - Esta Portaria entra em vigor na data de sua publicação.

CECÍLIA LEITE OLIVEIRA
Diretora

PORTARIA Nº 26, DE 10 DE ABRIL DE 2017

A DIRETORA DO INSTITUTO BRASILEIRO DE INFORMAÇÃO EM CIÊNCIA E TECNOLOGIA DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES, nomeada pela Portaria nº. 845 da Casa Civil da Presidência da República, publicada no DOU nº 217 de 07 de novembro de 2013, no uso de suas atribuições conferidas pela Portaria MCTIC nº. 5147, de 14 de novembro de 2016, publicada no DOU de 16 de novembro de 2016, resolve:

Modelo de Política de Gestão de Ativos

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Versão 1.1
Brasília, maio de 2022

MODELO DE POLÍTICA DE GESTÃO DE ATIVOS

MINISTÉRIO DA ECONOMIA

Paulo Roberto Nunes Guedes

Ministro

SECRETARIA ESPECIAL DE DESBUROCRATIZAÇÃO, GESTÃO E GOVERNO DIGITAL

Caio Mario Paes de Andrade

Secretário Especial de Desburocratização, Gestão e Governo Digital

SECRETARIA DE GOVERNO DIGITAL

Fernando André Coelho Mitkiewicz

Secretário de Governo Digital

DEPARTAMENTO DE GOVERNANÇA DE DADOS E INFORMAÇÕES

Leonardo Rodrigo Ferreira

Diretor do Departamento de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Proteção de Dados

Equipe Técnica de Elaboração

Amaury C. da Silveira Junior

Eder Ferreira de Andrade

Francisco Magno Felix Nobre

Heráclito Ricardo Ferreira Gomes

Ivaldo Jeferson de Santana Castro

Yuri Arcanjo de Carvalho

Ramon Caldas

Guilherme Rufino Junior

Guilherme Mendonça Medeiros

Equipe Revisora

Marcus Paulo Barbosa Vasconcelos

Samuel Barichello Conceição

Sumaid Andrade de Albuquerque

Histórico de Versões

Data	Versão	Descrição	Autor
31/03/2022	1.0	Modelo de Política de Gestão de Ativos	Equipe Técnica de Elaboração
05/05/2022	1.1	Modelo de Política de Gestão de Ativos	Equipe Técnica de Elaboração

Sumário

Esclarecimentos

O objetivo deste Modelo é fornecer aos responsáveis pela Proteção de Dados e Gestão da Segurança da Informação no âmbito dos órgãos integrantes do Sistema Integrado de Recursos de Tecnologia da Informação (SISP), orientações para mitigação de possíveis riscos ligados às temáticas de privacidade e segurança da informação relativos aos seus sistemas informacionais, contratos administrativos e processos de trabalho da instituição.

O Modelo foi construído a partir de análises de pontos relevantes dos sistemas informacionais críticos dos órgãos integrantes do Sistema Integrado de Recursos de Tecnologia da Informação (SISP), realizado pela Secretaria de Governo Digital (SGD) da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia.

Introdução

No contexto da transformação digital do Estado brasileiro, o Governo Federal publicou em 29 de abril de 2020, através do Decreto nº 10.332, a Estratégia de Governo Digital, iniciativa que se encontra em plena execução. Ela norteia as ações de todos os órgãos federais, com o objetivo de transformar o governo pelo Digital, oferecendo políticas públicas e serviços de melhor qualidade, mais simples, acessíveis de qualquer lugar e a um custo menor para o cidadão.

Hoje, mais do que em qualquer outro momento da história, o Governo utiliza a tecnologia para melhorar e expandir a oferta de serviços públicos para o cidadão apoiado em sistemas informatizados.

Nesse contexto, os órgãos federais, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais (por exemplo, fornecimento de serviços financeiros; fornecimento de serviços de emissões guias, certificados e carteiras; processamento de autorizações de segurança ou dados de saúde; fornecimento de serviços em nuvem; desenvolvendo comunicações via cabo, wireless e/ou satélites; sistemas militares de defesa). As informações federais são frequentemente fornecidas ou compartilhadas, obedecidos os requisitos legais, com entidades como governos estaduais e municipais, empresas públicas e privadas, faculdades e universidades, organizações de pesquisa independentes ou públicas e organizações do terceiro setor.

A proteção dessas informações pelo Governo enquanto agente de tratamento está designada no **Art.46. da Lei Geral de Proteção de Dados**, sancionada em 14 de agosto de 2018 – “Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.”

A sua não observância pode impactar diretamente a capacidade do governo federal de cumprir suas missões precípuas de promover uma gestão pública eficiente, ampliar o acesso à cidadania, estimular uma economia brasileira crescentemente digitalizada, dinâmica, produtiva e competitiva, e em última instancia, impedir a geração de valor público para o cidadão.

O presente Modelo de Política de Gestão de Ativos para o Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict) servirá como subsídio para a elaboração de norma complementar à Política de Segurança da Informação e Comunicação do órgão, visando a segurança de ativos informacionais.

Política de Gestão de Ativos

Para ter validade jurídica, este modelo de Política de Gestão e Ativos deverá ser discutido no âmbito do Comitê de Segurança da Informação e Comunicação (CSIC) do Ibict e devidamente aprovado como norma complementar à Portaria 02/2018 do Ibict, publicada no Boletim de Serviço do MCTI no. 01, de 29 de janeiro de 2018.

Responsável	Nome da pessoa ou área responsável pela gestão desta política.
Aprovado por:	Nome da pessoa ou área responsável pela aprovação e autorização da implementação desta política.

Políticas Relacionadas	Política de Segurança da Informação e Comunicação do Ibict, e normas complementares, a saber: i) Estrutura física, rede elétrica, nobreak, grupo gerador, sistema contra incêndio e climatização; ii) Link e redes cabeada e wireless; iii) Controle de acesso e circulação; iv) Correio eletrônico; v) Recursos computacionais; vi) Utilização de telefones celulares, fixos e outros dispositivos comunicacionais e vii) Utilização de internet e intranet.
Localização de armazenamento	Descreva a localização física ou digital das cópias desta política.
Data da Aprovação	Liste a data em que essa política entrou em vigor.
Data de revisão	Liste a data em que esta política deve passar por revisão e atualização.
Versão	Indique a versão atual desta política

Propósito

O objetivo desta política é garantir que os ativos de informação sejam identificados adequadamente e que os controles de proteção recomendados para estes ativos de informação estejam em vigor.

Para manter a segurança e continuidade do negócio do Ibict, em sua missão, é fundamental mapear e monitorar os ativos tecnológicos, para maior controle da organização, auxiliando na aplicação de atualizações, implementação de controles de segurança e gestão de risco da organização. Auxiliando também na recuperação de incidentes.

Os ativos de informação do Ibict devem ser classificados a fim de permitir a definição de níveis de segurança para eles. Cada ativo de informação deverá ter um responsável, o qual realizará a classificação do ativo e deverá ser registrado em uma base de dados gerenciada de forma centralizada.

Escopo

Esta Política de Gestão de Ativos se aplica a todos os processos de negócios e dados, sistemas de informação e componentes, pessoal e a todas as coordenações do Ibict.

- Aplica-se a todos os ativos de informação do órgão, incluindo ativos armazenados fora da sede da entidade armazenados em serviços de nuvem. Ativos de informação neste contexto, incluem bibliotecas e acervos digitais, coleções, documentos, bases de dados, contratos, documentação de sistemas, procedimentos, manuais, logs de sistemas, planos, guias, programas de computador, servidores, computadores, e-mail, arquivos pessoais e compartilhados, bancos de dados e conteúdo da web específicos.
- A classificação dos ativos de informação e o escopo desta política serão revisados a cada dois anos.

Termos e Definições

ATIVOS DE INFORMAÇÃO - meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

INCIDENTE - interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida

de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

Referência legal e de boas práticas

Orientação	Secção
Acórdão 1.889/2020-TCU-Plenário	Relatório de Levantamento de Auditoria Páginas 30-32
Decreto Nº 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo Art.3, Inciso I, II e V
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso III, IV, VIII XI CAPÍTULO VI - Seção IV – Art.15
Framework de segurança cibernética do CIS 8	Salvaguarda 1,2 e 3
Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI;	Gestão da Segurança da Informação
Guias Operacionais SGD	Todos
Instrução Normativa Nº 01/GSI/PR	Art.12, Inciso IV, alínea d
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021	Capítulo II
Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI)	Em sua íntegra
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50
NIST SP 800-53 v4	AC-3, AC-4, AC-16, AC-20, CM-8, CM-9, MP-2, MP-3, PL-4, PM-5, PS-6, RA-2, SC-16
Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos;	A.8 (A.8.1., A.8.2., A.8.3.)
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra
Portaria Ibict nº 02, de 25 de janeiro de 2018	Em sua íntegra

Declarações da política

Dos princípios gerais

i. A Política de Gestão de Ativos de informação está alinhada à Política de Segurança da Informação e Comunicações do Ibict.

ii. A Política de Gestão de Ativos de informação deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

iii. O processo de mapeamento de ativos de informação deve estruturar e manter um registro de ativos de informação, destinados a subsidiar os processos de gestão de risco, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação.

iv. As rotinas de inventário e mapeamento de ativos de informação devem ser orientadas para a identificação dos ativos de informação da organização, a fim de manter o escopo da organização mapeado e documentado.

v. O processo de mapeamento de ativos de informação deve considerar, preliminarmente os objetivos estratégicos da organização, seus processos internos, os requisitos legais e sua estrutura organizacional.

vi. O registro de ativos de informação resultante do processo de mapeamento de ativos de informação deverá conter: os responsáveis (proprietários e custodiantes) de cada ativo de informação; as informações básicas sobre os requisitos de segurança da informação de cada ativo de informação; os contêineres de cada ativo de informação; as interfaces de cada ativo de informação e as interdependências entre eles.

Os seguintes ativos de informação devem ser considerados no processo de mapeamento de ativos de informação:

I. Ativos físicos;
II. Bases e bancos de dados;
III. Dispositivos móveis;
IV. Hardwares;
V. Mídias removíveis;
VI. Serviços;
VII. Softwares;
VIII. Bibliotecas digitais;
IX. Acervos digitais;
X. Coleções.

Diretrizes:

1. Informações ou ativos de informação de instalações de processamento de informações devem ser inventariados e documentados e esse registro deve ser mantido atualizado.

   - A categorização do inventário deve ser aprovada pelas partes apropriadas ou autoridade de autorização.
   - A organização empregará o uso de mecanismos automatizados para identificar sistemas autorizados e não autorizados, incluindo hardware ou software.
   - O inventário também deverá incluir atualizações ou remoções do sistema de informação.

2. Das responsabilidades do proprietário do processo (recomenda-se a leitura ao Art. 9º da IN GSI/PR nº 3/2021)

   - Identificar potenciais ameaças aos ativos de informação;
   - Identificar vulnerabilidades dos ativos de informação;
   - Consolidar informações resultantes da análise do nível de segurança da informação de cada ativo de informação ou de grupos de ativos de informação em um relatório;
   - Avaliar os riscos dos ativos de informação ou do grupo de ativos de informação.
   - Indivíduos que requerem acesso aos sistemas de informação devem seguir o procedimento adequado para receber tal acesso, como descritos na política de controle de acesso e catalogadas no sistema de gestão de ativos.
   - Os processos em torno do gerenciamento de mudança e de configuração também serão estabelecidos e monitorados.

- Todos os ativos de informação devem ser devolvidos após a rescisão do contrato de trabalho ou contrato.

3. Criticidade do ativo de informação:
    - A criticidade dos ativos de informação da organização é determinada pelo:
        i. Requisitos legais;
        ii. Pelo valor econômico;
        iii. Pelo seu potencial de agregar valor ao negócio; e
        iv. Por sua vida útil.

4. Classificação das informações:
    - Todos os ativos de informação devem ser classificados de acordo com sua criticidade.
    - As informações armazenadas, transmitidas, processadas ou que se encontram sob a guarda dos ativos de informação do Ibict devem ser classificados de acordo com a legislação pertinente (recomenda-se leitura da LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011), podendo ser classificado em uma das seguintes categorias:
        i. **Ultrassecreta:** São passíveis de classificação como ultrassecretos, dentre outros, dados, informações ou documentos referentes à soberania e à integridade territorial nacionais, a planos e operações, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade ou do Estado.
        ii. **Secreta:** São passíveis de classificação como secretos, dentre outros, dados, informações ou documentos referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicas, cujo conhecimento não autorizado possa acarretar dano grave à segurança do órgão, da sociedade ou do Estado.
        iii. **Reservada:** São passíveis de classificação como confidenciais, dentre outros, dados, informações ou documentos que, no interesse do Ibict, devam ser de conhecimento restrito e cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança do órgão, da sociedade ou do Estado.
    - Os ativos de informação serão rotulados e manuseados com base nos procedimentos apropriados de classificação de informações usados pela organização.

5. Manipulação de mídia:
    - A mídia removível também deve ser gerenciada pelo mesmo procedimento de classificação de ativos de informação usado pela organização.
    - A mídia removível deve ser protegida contra acesso não autorizado e uso indevido durante o uso e em trânsito, e deve ser descartada com segurança, usando os procedimentos apropriados.
    - A mídia contendo informações confidenciais e internas do Ibict devem ser protegidas contra acesso não autorizado, uso indevido, corrupção durante o transporte e, preferencialmente, com o uso de criptografia.

6. Uso aceitável:
    - Padrões ou diretrizes para o uso aceitável de ativos devem ser documentados para indicar o que os usuários dos ativos de informação podem ou não fazer.
    - Os seguintes itens devem ser cobertos, quanto ao uso aceitável, nas normas complementares à Política de Segurança da Informação e Comunicação do Ibict (Portaria 02/2018-IBICT):
        i. Uso do computador e dos sistemas de informação (Anexo V da Portaria);
        ii. Uso de softwares e dados (Anexo V);
        iii. Uso da Internet e e-mail (Anexo IV);
        iv. Uso do telefone (Anexo VI);
        v. Uso de equipamentos e materiais de escritório (Anexo V).
    - Como requisito de acesso ao ativo de informação e como componente do treinamento de conscientização de segurança, todos os usuários dos ativos de informação, sejam funcionários ou terceiros, serão obrigados a fornecer aceitação assinada das diretrizes de uso aceitáveis

Procedimentos Relevantes

Procedimentos formais serão criados no sentido de promover, reforçar e apoiar as determinações dessa política. Os procedimentos, sempre em consonância com essa política, serão editados pelo Comitê de Segurança da Informação e Comunicações (CSIC) do Ibict e publicados na intranet, com ampla divulgação.

Não conformidade

Nos termos dos artigos 33 a 35 da Portaria 02/2018-IBICT, o descumprimento dessas disposições caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo da responsabilização penal e civil, e sujeito à aplicação das penalidades previstas na Lei 8.112/90 e na legislação pertinente.

Concordância

Eu li e entendi a Política de Controle de Ativos do Instituto Brasileiro de Informação para Ciência e Tecnologia - Ibict. Entendo que se eu violar as diretrizes estabelecidas nesta Política, posso enfrentar ações legais ou disciplinares de acordo com as leis aplicáveis ou normas internas do órgão.

Nome do Servidor/Empregado

Assinatura do funcionário Data

Histórico de Revisão

ID da versão	Data da Mudança	Autor
Ibict	09/05/2022	Henrique

Modelo de Política de Backup

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Versão 1.1
Brasília, maio de 2022

MODELO DE POLÍTICA DE CONTROLE DE BACKUP

MINISTÉRIO DA ECONOMIA

Paulo Roberto Nunes Guedes

Ministro

SECRETARIA ESPECIAL DE DESBUROCRATIZAÇÃO, GESTÃO E GOVERNO DIGITAL

Caio Mario Paes de Andrade

Secretário Especial de Desburocratização, Gestão e Governo Digital

SECRETARIA DE GOVERNO DIGITAL

Fernando André Coelho Mitkiewicz

Secretário de Governo Digital

DEPARTAMENTO DE GOVERNANÇA DE DADOS E INFORMAÇÕES

Leonardo Rodrigo Ferreira

Diretor do Departamento de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Proteção de Dados

Equipe Técnica de Elaboração

Amaury C. da Silveira Junior

Eder Ferreira de Andrade

Francisco Magno Felix Nobre

Heráclito Ricardo Ferreira Gomes

Ivaldo Jeferson de Santana Castro

Yuri Arcanjo de Carvalho

Ramon Caldas

Guilherme Rufino Junior

Guilherme Mendonça Medeiros

Equipe Revisora

Marcus Paulo Barbosa Vasconcelos

Samuel Barichello Conceição

Sumaid Andrade de Albuquerque

Histórico de Versões

Data	Versão	Descrição	Autor
30/03/2022	1.0	Modelo de Política de Backup	Equipe Técnica de Elaboração
05/05/2022	1.1	Modelo de Política de Backup	Equipe Técnica de Elaboração

Sumário

Esclarecimentos

O objetivo deste Modelo é fornecer aos responsáveis pela Proteção de Dados e Gestão da Segurança da Informação no âmbito dos órgãos integrantes do Sistema Integrado de Recursos de Tecnologia da Informação (SISP), orientações para mitigação de possíveis riscos ligados às temáticas de privacidade e segurança da informação relativos aos seus sistemas informacionais, contratos administrativos e processos de trabalho da instituição.

O Modelo foi construído a partir de análises de pontos relevantes dos sistemas informacionais críticos dos órgãos integrantes do Sistema Integrado de Recursos de Tecnologia da Informação (SISP), realizado pela Secretaria de Governo Digital (SGD) da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia.

Introdução

No contexto da transformação digital do Estado brasileiro, o Governo Federal publicou em 29 de abril de 2020, por meio do Decreto nº 10.332, a Estratégia de Governo Digital, iniciativa que se encontra em plena execução. Ela norteia as ações de todos os órgãos federais, com o objetivo de transformar o governo pelo Digital, oferecendo políticas públicas e serviços de melhor qualidade, mais simples, acessíveis de qualquer lugar e a um custo menor para o cidadão.

Hoje, mais do que em qualquer outro momento da história, o Governo utiliza a tecnologia para melhorar e expandir a oferta de serviços públicos para o cidadão apoiado em sistemas informatizados

Nesse contexto, os órgãos federais, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais (por exemplo, fornecimento de serviços financeiros; fornecimento de serviços de emissões guias, certificados e carteiras; processamento de autorizações de segurança ou dados de saúde; fornecimento de serviços em nuvem; desenvolvendo comunicações via cabo, wireless e/ou satélites; sistemas militares de defesa). As informações federais são frequentemente fornecidas ou compartilhadas, obedecidos os requisitos legais, com entidades como governos estaduais e municipais, empresas públicas e privadas, faculdades e universidades, organizações de pesquisa independentes ou públicas e organizações do terceiro setor.

A proteção dessas informações pelo Governo enquanto agente de tratamento está designada no **Art.46. da Lei Geral de Proteção de Dados**, sancionada em 14 de agosto de 2018 – “Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.”

A sua não observância pode impactar diretamente a capacidade do governo federal de cumprir suas missões precípuas de promover uma gestão pública eficiente, ampliar o acesso à cidadania, estimular uma economia brasileira crescentemente digitalizada, dinâmica, produtiva e competitiva, e em última instancia, impedir a geração de valor público para o cidadão.

O presente Modelo de Política de Backup e Restauração de Dados Digitais para o Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict) servirá como subsídio para a elaboração de norma complementar à Política de Segurança da Informação e Comunicação do órgão, visando a segurança de ativos informacionais.

Política de Backup e Restauração de Dados Digitais

Para ter validade jurídica, este modelo de Política de Backup e Restauração de Dados Digitais deverá ser discutido no âmbito do Comitê de Segurança da Informação e Comunicação (CSIC) do Ibict e devidamente aprovado como norma complementar à Portaria 02/2018 do Ibict, publicada no Boletim de Serviço do MCTI no. 01, de 29 de janeiro de 2018.

Responsável	Nome da pessoa ou área responsável pela gestão desta política.
Aprovado por:	Nome da pessoa ou área responsável pela aprovação e autorização da implementação desta política.
Políticas Relacionadas	Política de Segurança da Informação e Comunicação do Ibict, e normas complementares, a saber: i) Estrutura física, rede elétrica, nobreak, grupo gerador, sistema contra incêndio e climatização; ii) Link e redes cabeada e wireless; iii) Controle de acesso e circulação; iv) Correio eletrônico; v) Recursos computacionais;

	vi) Utilização de telefones celulares, fixos e outros dispositivos comunicacionais e vii) Utilização de internet e intranet.
Localização de armazenamento	Descreva a localização física ou digital das cópias desta política.
Data da Aprovação	Liste a data em que essa política entrou em vigor.
Data de revisão	Liste a data em que esta política deve passar por revisão e atualização.

Propósito

A Política de Backup e Restauração de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pela(s) Divisão de Produção e Redes (Dired) e formalmente definidos como de necessária salvaguarda na instituto, para se manter a continuidade do negócio. No sentido de assegurar sua missão é fundamental estabelecer mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de indisponibilidades ou perdas por erro humano, ataques, catástrofes naturais ou outras ameaças. O presente documento apresenta a Política de Backup e Restauração de Dados Digitais, onde se estabelece o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais.

Escopo

- Esta política se aplica a todos os dados no âmbito do Ibict, incluindo dados fora do órgão armazenados em um serviço de nuvem Pública ou Privada. “Dados críticos”, neste contexto, incluem bases de dados, repositórios, bibliotecas, acervos e coleções digitais, e-mail, arquivos pessoais e compartilhados, bancos de dados e conteúdo web específico. A definição de dados críticos e o escopo desta política de backup serão revisados a cada dois anos.
- Os serviços de TI críticos do Ibict devem ser formalmente elencados pelo Comitê de Segurança da Informação e Comunicação (CSIC).
- Esta política se aplica aos administradores, criadores e usuários de tais dados. A política também se aplica a terceiros que acessam e usam sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade do órgão.
- Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas unidades de TI, ficando sobre a responsabilidade do indivíduo que usa o(s) dispositivo(s).
- A salvaguarda dos dados em formato digital pertencentes a serviços de TI da organização mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve estar garantida nos acordos ou contratos que formalizam a relação entre os envolvidos.

Termos e Definições

BACKUP OU CÓPIA DE SEGURANÇA - Conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

CUSTODIANTE DA INFORMAÇÃO - Qualquer indivíduo ou estrutura de órgão ou entidade da Administração Pública Federal, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de Segurança da Informação comunicadas pelo proprietário da informação;

ELIMINAÇÃO - Exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

MÍDIA - Mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação - inclui discos ópticos, magnéticos, CDs, fitas e papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos;

INFRAESTRUTURA CRÍTICA – instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança;

Recovery Point Objective (RPO): ponto no tempo em que os dados dos serviços de TI devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente;

Recovery Time Objective (RTO): tempo estimado para restaurar os dados e tornar os serviços de TI novamente operacionais, correspondendo ao prazo máximo em que se admite manter os serviços de TI inoperantes até a restauração de seus dados, após um incidente;

Referência legal e de boas práticas

Orientação	Secção
Acórdão 1.889/2020-TCU-Plenário	Relatório de Levantamento de Auditoria Páginas 30-32
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo Art.3, Inciso I, II e V
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso III, IV, VIII XI CAPÍTULO VI - Seção IV – Art.15
Framework Control Objectives for Information and Related Technology – Cobit, conjunto de boas práticas a serem aplicadas à governança da TI;	v4.1: DS11: Gerenciar Dados v5: DSS01.01, DSS04.08; DSS06.04, DSS04.08, DSS05.06; DSS06.05-06, DSS04.08, DSS001.01; DSS05.02-05; DSS06.03; DSS06.06
Framework de segurança cibernética do CIS 8	Salvaguardas do controle 11 (Data Recovery Capabilities)
Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI;	Gestão da Segurança da Informação

Guias Operacionais SGD	Todos
Instrução Normativa 01/GSI/PR	Art.12, Inciso IV, alínea g, h
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021	Capítulo IV
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50
Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI)	Em sua íntegra
Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemasde gestão de segurança da informação - Requisitos;	A.12.3 Cópias de segurança
Norma ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;	12.3 Cópias de segurança
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra
Portaria Ibict nº 02, de 25 de janeiro de 2018	Em sua íntegra

Declarações da política

Dos princípios gerais

1. A Política de Backup e Restauração de Dados deve estar alinhada com à Política de Segurança da Informação e Comunicação (POSIC) do Ibict.
2. A Política de Backup e Restauração de Dados deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.
3. As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.
4. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.
5. As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização.
6. O armazenamento de backup, se possível, deve ser realizado em um local distinto da infraestrutura crítica. É desejável que se tenha um sítio de backup em um local remoto ao da sede da organização para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos.
7. A infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.
8. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.
9. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de criptografia.

Da frequência e retenção dos dados

10. Os backups dos serviços de TI devem ser realizados utilizando-se as seguintes frequências temporais:

    I – Diária;

II – Semanal;

III – Mensal.

11. Os serviços de TI devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

I – Diária: 7 dias;

II – Semanal: 3 semanas;

III – Mensal: 1 ano;

12. Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.
13. Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.
14. A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pelo responsável pelo serviço, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

I – Escopo (dados digitais a serem salvaguardados);

II – Tipo de *backup* (completo, incremental, diferencial);

III – Frequência temporal de realização do backup (diária, semanal, mensal, anual);

IV – Retenção;

V – POR.

15. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao Divisão de Produção e Redes (Dired).
16. Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de backup deverão zelar pelo cumprimento das diretrizes estabelecidas.

Tipo de backup

I – Completo (*full*);

II – Incremental;

III – Diferencial.

Salvo indicação em contrário, o backup dos dados do sistema será feito de acordo com a seguinte programação padrão:

17. Backup incremental diário (segunda a quinta), armazenado no local.
18. Backup completo semanal (toda sexta-feira). Sempre que possível, os backups devem ser iniciados às 0 h da manhã de sexta para permitir que haja tempo suficiente para lidar com quaisquer problemas que possam surgir durante o processo de backup.

Do uso da rede

19. O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI.
20. A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.
21. O período de janela de backup deve ser determinado pelo administrador de backup em conjunto com a área técnica responsável pela administração da rede de dados.

Do transporte e armazenamento

22. As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar as seguintes características dos dados resguardados:

    I – A criticidade do dado salvaguardado;

    II – O tempo de retenção do dado;

    III – A probabilidade de necessidade de restauração;

    IV – O tempo esperado para restauração;

    V – O custo de aquisição da unidade de armazenamento de backup;

    VI – A vida útil da unidade de armazenamento de backup.

23. O administrador de backup deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

24. Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de restauração dos dados seja considerado aceitável pelos gestores das informações.

25. A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

26. No caso de desligamento do usuário (de forma permanente ou temporária), o backup de seus arquivos em nuvem deverá ser mantido por, no mínimo, 60 (sessenta) dias. Após esse período os arquivos poderão ser excluídos a qualquer tempo.

27. As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade, temperatura, poeira e pressão, e com acesso restrito a pessoas autorizadas pelo administrador de backup. Além disso, as condições de temperatura, umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento.

28. Quando da necessidade de descarte de unidades de armazenamento de backups, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.

As fitas de backup serão transportadas e armazenadas conforme descrito neste documento:

- A mídia será claramente identificada e armazenada em uma área segura acessível apenas para pessoa(s) autorizada(s).
- Backups completos semanais serão mantidos por um período de 3 (três) semanas. Após esse período, as mídias serão reutilizadas ou destruídas.
- Backups completos mensais dos dados arquivados serão mantidos por um ano. Depois deste período, as fitas serão reutilizadas ou destruídas.

Dos testes de backup

29. Os backups serão verificados periodicamente:

- Diariamente, os logs de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup.
- Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha.
- A TI manterá registros de backups e testes de restauração para demonstrar conformidade com esta política.

- Os testes devem ser realizados em todos os backups produzidos independente do ambiente.

30. Os testes de restauração dos backups devem ser realizados, por amostragem, uma vez por semana, em equipamentos servidores diferentes dos equipamentos que atendem aos ambientes de produção, observados os recursos humanos de TI e tecnologias disponíveis, a fim de verificar backups bem-sucedidos.
31. Verificar se foram atendidos os níveis de serviço pactuados, tais como os Recovery Point Objectives – RPOs.
32. Os registros deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu reestabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do backup e se o procedimento foi concluído com sucesso
33. Quaisquer exceções a esta política serão totalmente documentadas e aprovadas pelo Comitê de Segurança da Informação e Comunicação (CSIC).

Procedimento de restauração de backup

34. O atendimento de solicitações de restauração de arquivos, e-mails e demais formas de dados deverá obedecer às seguintes orientações:

    a. A solicitação de restauração de objetos deverá sempre partir do responsável pelo recurso, através da abertura de chamado técnico.

    b. A restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de backup.

    c. A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações.

    d. O operador de backup terá a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestor da unidade do demandante.

Do Descarte da Mídia

35. A mídia de backup será retirada e descartada conforme descrito neste documento:
    a. A TI garantirá que a mídia não contenha mais imagens de backup ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados.
    b. A TI garantirá a destruição física da mídia antes do descarte.

Das Responsabilidades

36. O administrador de backup e o operador de backup devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de backup.
37. A administração do backup é de responsabilidade de Dired.

São atribuições do administrador de backup:

I – Propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela organização;
II – Providenciar a criação e manutenção dos backups;
III – Configurar as soluções de backup;
IV – Manter as unidades de armazenamento de backups preservadas, funcionais e seguras;
V – Definir os procedimentos de restauração e neles auxiliar;

Procedimentos Relevantes

Os procedimentos de backup serão devidamente documentados e ficarão disponíveis por meio de ferramenta tecnológica.

Não conformidade

Nos termos dos artigos 33 a 35 da Portaria 02/2018-IBICT, o descumprimento dessas disposições caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo da responsabilização penal e civil, e sujeito à aplicação das penalidades previstas na Lei 8.112/90 e na legislação pertinente.

Concordância

Eu li e entendi a Política de Backup e Restauração de Dados Digitais do Ibict. Entendo que se eu violar as diretrizes estabelecidas nesta Política, posso enfrentar ações legais e/ou disciplinares de acordo com as leis aplicáveis e as normas internas do órgão.

_____
Nome do Servidor/Empregado

_____
Assinatura do funcionário Data

Histórico de Revisão

ID da versão	Data da Mudança	Autor
Ibict	13/05/2022	Henrique

_____

Modelo de Política de Controle de Acesso

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Versão 1.1

Brasília, maio de 2022

MINISTÉRIO DA ECONOMIA

Paulo Roberto Nunes Guedes

Ministro

SECRETARIA ESPECIAL DE DESBUROCRATIZAÇÃO, GESTÃO E GOVERNO DIGITAL

Caio Mario Paes de Andrade

Secretário Especial de Desburocratização, Gestão e Governo Digital

SECRETARIA DE GOVERNO DIGITAL

Fernando André Coelho Mitkiewicz

Secretário de Governo Digital

DEPARTAMENTO DE GOVERNANÇA DE DADOS E INFORMAÇÕES

Leonardo Rodrigo Ferreira

Diretor do Departamento de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Proteção de Dados

Equipe Técnica de Elaboração

Amaury C. da Silveira Junior

Eder Ferreira de Andrade

Francisco Magno Felix Nobre

Heráclito Ricardo Ferreira Gomes

Ivaldo Jeferson de Santana Castro

Yuri Arcanjo de Carvalho

Ramon Caldas

Guilherme Rufino Junior

Guilherme Mendonça Medeiros

Equipe Revisora

Marcelo de Lima

Marcus Paulo Barbosa Vasconcelos

Sumaid Andrade de Albuquerque

Histórico de Versões

Data	Versão	Descrição	Autor
01/04/2022	1.0	Modelo de Política de Controle de Acesso	Equipe Técnica de Elaboração
05/05/2022	1.1	Modelo de Política de Controle de Acesso	Equipe Técnica de Elaboração

SUMÁRIO

Esclarecimentos

O objetivo deste Modelo é fornecer aos responsáveis pela Proteção de Dados e Gestão da Segurança da Informação no âmbito dos órgãos integrantes do Sistema Integrado de Recursos de Tecnologia da Informação (SISP), orientações para mitigação de possíveis riscos ligados às temáticas de privacidade e segurança da informação relativos aos seus sistemas informacionais, contratos administrativos e processos de trabalho da instituição.

O Modelo foi construído a partir de análises de pontos relevantes dos sistemas informacionais críticos dos Órgãos e entidades integrantes do Sistema Integrado de Recursos de Tecnologia da Informação (SISP), realizadas pela Secretaria de Governo Digital (SGD) da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia.

Introdução

No contexto da transformação digital do Estado brasileiro, o Governo Federal publicou em 29 de abril de 2020, através do Decreto nº10.332, a Estratégia de Governo Digital, iniciativa que se encontra em plena execução. Ela norteia as ações de todos os órgãos federais, com o objetivo de transformar o governo pelo Digital, oferecendo políticas públicas e serviços de melhor qualidade, mais simples, acessíveis de qualquer lugar e a um custo menor para o cidadão.

Hoje, mais do que em qualquer outro momento da história, o Governo utiliza a tecnologia para melhorar e expandir a oferta de serviços públicos para o cidadão apoiado em sistemas informatizados.

Nesse contexto, os órgãos federais, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais (por exemplo, fornecimento de serviços financeiros; fornecimento de serviços de emissões guias, certificados e carteiras; processamento de autorizações de segurança ou dados de saúde; fornecimento de serviços em nuvem; desenvolvendo comunicações via cabo, wireless e/ou satélites; sistemas militares de defesa). As informações federais são frequentemente fornecidas ou compartilhadas, obedecidos os requisitos legais, com entes como governos estaduais e municipais, empresas públicas e privadas, faculdades e universidades, organizações de pesquisa independentes ou públicas e organizações do terceiro setor.

A proteção dessas informações pelo Governo enquanto agente de tratamento está designada no **Art.46. da Lei Geral de Proteção de Dados**, sancionada em 14 de agosto de 2018 – “Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.”

A sua não observância pode impactar diretamente a capacidade do governo federal de cumprir suas missões precípuas de promover uma gestão pública eficiente, ampliar o acesso à cidadania, estimular uma economia brasileira crescentemente digitalizada, dinâmica, produtiva e competitiva, e em última instância, impedir a geração de valor público para o cidadão.

O presente Modelo de Política de Controle de Acesso para o Instituto Brasileiro de Informação em Ciência e Tecnologia (Ibict) servirá como subsídio para a elaboração de norma complementar à Política de Segurança da Informação e Comunicação do órgão, visando a segurança de ativos informacionais.

Política de Controle de Acesso

Para ter validade jurídica, este modelo de Política de Controle de Acesso deverá ser discutido no âmbito do Comitê de Segurança da Informação e Comunicação (CSIC) do Ibict e devidamente aprovado como norma complementar à Portaria 02/2018 do Ibict, publicada no Boletim de Serviço do MCTI no. 01, de 29 de janeiro de 2018.

Este modelo tem por foco prover diretrizes para o controle de acesso, a fim de atender a necessidade de implementar os controles emergenciais previstos no anexo 5 do Programa de Privacidade e Segurança da Informação (PPSI), contudo, recomenda-se que o órgão considere, no mínimo as diretrizes gerais estabelecidas para implementação da Política de Segurança da Informação, conforme prevê o Art.12, Inciso IV, da Instrução Normativa 01/GSI/PR, em especial as diretrizes para controle de acesso (lógico e físico), referenciado na alínea f do referido inciso. Ainda, recomenda-se que considere o item 7 da Norma Complementar nº 7/IN01/DSIC/GSIPR, a qual estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação, nos órgãos e entidades da Administração Pública Federal.

Responsável	Nome da pessoa ou área responsável pela gestão desta política.
Aprovado por:	Nome da pessoa ou área responsável pela aprovação e autorização da implementação desta política.
Políticas Relacionadas	Política de Segurança da Informação e Comunicação do Ibict, e normas complementares, a saber: i) Estrutura física, rede elétrica, nobreak, grupo gerador, sistema contra incêndio e climatização; ii) Link e redes cabeada e wireless; iii) Controle de acesso e circulação; iv) Correio eletrônico; v) Recursos computacionais; vi) Utilização de telefones celulares, fixos e outros dispositivos comunicacionais e vii) Utilização de internet e intranet.
Localização de armazenamento	Descreva a localização física ou digital das cópias desta política.
Data da Aprovação	Data em que essa política entrou em vigor.
Data de revisão	Data em que esta política passou por revisão e atualização.
Versão	Indique a versão atual desta política

Propósito

A Política de Controle de Acesso objetiva estabelecer controles de identificação, autenticação e autorização para salvaguardar as informações do Ibict, estejam elas em qualquer meio, seja digital ou físico, a fim de evitar a quebra da segurança da informação e quaisquer acessos não autorizados que impliquem em risco de destruição, alteração, perda, roubo ou divulgação indevida.

Sem controles de autorização, identificação e autenticação, existe o risco potencial de que os sistemas de informação possam ser acessados ilicitamente e que a segurança desses sistemas de informação seja comprometida.

Considera-se, portanto, que as credenciais: crachá de identificação funcional e logins de acesso dos sistemas de informações, são pessoais e intransferíveis e são o único método legítimo pelo qual o direito de acesso físico e/ou lógico podem ser exercidos.

Os controles de autorização, identificação e autenticação garantem que apenas usuários autorizados tenham acesso físico ou façam uso dos sistemas de informação do Ibict.

Escopo

Esta Política se aplica a todas as informações, onde o Ibict seja o agente de tratamento, ao meio utilizado para este tratamento, seja digital ou físico, e as dependências físicas desta organização, bem como a qualquer pessoa que circule nas dependências ou que interaja exercendo controle administrativo, técnico ou operacional, mesmo que eventual, desses meios de tratamento.

Especificamente, inclui todos os funcionários, sejam servidores efetivos ou temporários, colaboradores contratados e terceiros que trabalham para o órgão, além de funcionários de parceiros que acessam fisicamente as dependências ou que acessam a rede e sistemas de informação do Ibict.

Termos e Definições

ACESSO - ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

CONTROLE DE ACESSO - conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

Referência legal e de boas práticas

Orientação	Secção
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo Art.3, Inciso I
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso XI CAPÍTULO VI - Seção IV – Art.15
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Instrução Normativa 01/GSI/PR	Art.12, Inciso IV, alínea f
Norma Complementar nº 7/IN01/DSIC/GSIPR	Item 7
Acórdão 1.889/2020-TCU-Plenário	Relatório de Levantamento de Auditoria Páginas 30-32
ABNT NBR ISO/IEC 27002: 2013. Código de Prática para controles de Segurança da Informação	Itens 9 – 11.2.9 (Páginas 23 - 47)
CIS V8	CAPÍTULO 6
Guia do Framework de Segurança – LGPD	Páginas 24 - 26
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra
Portaria Ibict nº 02, de 25 de janeiro de 2018	Em sua íntegra

Declarações da política

A DIRETORA DO INSTITUTO BRASILEIRO DE INFORMAÇÃO EM CIÊNCIA E TECNOLOGIA (IBICT), DO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO, no uso de suas atribuições e tendo em vista o disposto no Portaria MCTIC nº 5.147 de 14 de novembro de 2016, publicado no DOU de 16 novembro de 2016,

R E S O L V E:

Art. 1º Fica aprovada, no âmbito do Ibict, a Norma para Criação e Administração de contas de acesso, em complemento às diretrizes estabelecidas pelo Artigo 32, da Política de Segurança da Informação e Comunicação - POSIC do Ibict.

CAPÍTULO I

ACESSO LÓGICO

Art. 2º O acesso lógico aos recursos da Rede Local deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pela Divisão de Suporte Técnico (Disup), através de chamado aberto à prestadora de serviços de sustentação da infraestrutura tecnológica, baseado nas responsabilidades e tarefas de cada usuário.

I. Terão direito a acesso lógico aos recursos da Rede Local os usuários de recursos de tecnologia da informação.

II. Para fins desta Resolução, consideram-se usuários de recursos de tecnologia da informação servidores ocupantes de cargo efetivo ou cargo em comissão, ocupantes de emprego público em exercício, assim como funcionários de empresas prestadoras de serviços, estagiários e demais usuários temporários em atividade no Ibict.

III. O acesso remoto deve ser realizado por meio de VPN – Rede Virtual Privada, após as devidas autorizações.

CAPÍTULO II

CONTA DE ACESSO LÓGICO E SENHA

Art. 3º Para utilização das estações de trabalho do Ibict, será obrigatório o uso de uma única identificação (*login*) e de senha de acesso, fornecidos pela Disup, mediante solicitação formal pelo titular da unidade do requisitante.

I. O formulário de solicitação de acesso se encontra disponível para preenchimento na Intranet do instituto.

II. Os privilégios de acesso dos usuários à Rede Local devem ser definidos pela unidade requisitante ao qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas.

III. Na necessidade de utilização de perfil diferente do disponibilizado, o titular da unidade do usuário deverá encaminhar solicitação para a Disup, através de chamado aberto à prestadora de serviços de sustentação da infraestrutura tecnológica, que a examinará, podendo negá-la nos casos em que a entender desnecessária.

Art. 4º O *login* e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pela Disup quando constatada qualquer irregularidade.

Parágrafo único. Para retomar o acesso à rede, deverá ser formalizada nova requisição pelo titular da unidade do requisitante.

Art. 5º O padrão adotado para o formato da conta de acesso do usuário é a sequência primeiro nome + último nome do usuário, como por exemplo, joaosilva.

Parágrafo único. Nos casos de já existência de conta de acesso para outro usuário, a prestadora de serviços de sustentação da infraestrutura tecnológica realizará outra combinação utilizando o nome completo do usuário para o qual a conta está sendo criada.

Art. 6º O padrão adotado para o formato da senha é o definido pela Divisão de Produção e Redes (Dired), que considera o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores.

I. A formação da senha da identificação (*login*) de acesso à Rede Local deve seguir as regras de:

a) Possuir tamanho mínimo de oito caracteres, sendo obrigatório o uso de letras e números.

b) Recomenda-se a utilização de letras maiúsculas, minúsculas e caracteres especiais ($, %, &,...);

c) Não ser formada por sequência numérica (123...), alfabética (abc...), nomes próprios, palavras de fácil dedução, datas, placa de carro, número de telefone, a própria conta de acesso, apelidos ou abreviações;

d) Não utilizar termos óbvios, tais como: Brasil, senha, usuário, *password* ou *system*.

e) Não reutilizar as últimas 3 (três) senhas.

II. A prestadora de serviços de sustentação da infraestrutura tecnológica fornecerá uma senha temporária para cada conta de acesso criada no momento da liberação dessa conta e a mesma deverá ser alterada pelo usuário quando do primeiro acesso à Rede Local.

Art. 7º As senhas de acesso serão renovadas a cada 180 (cento e oitenta) dias, devendo o usuário ser informado antecipadamente a fim de que ele próprio efetue a mudança.

Parágrafo único. Caso não efetue a troca no prazo estabelecido, será bloqueado seu acesso à Rede Local até que a nova senha seja configurada.

CAPÍTULO III

BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO

Art. 8º A conta de acesso será bloqueada nos seguintes casos:

I. Solicitação do superior imediato do usuário com a devida justificativa;

II. Quando da suspeita de mau uso dos serviços disponibilizados pelo órgão ou descumprimento da Política de Segurança da Informação e Comunicação – POSIC e normas correlatas em vigência.

III. Após 180 (cento e oitenta) dias consecutivos sem movimentação pelo usuário.

Art. 9º O desbloqueio da conta de acesso à Rede Local será realizado apenas após solicitação formal do superior imediato do usuário à Disup através de chamado aberto à prestadora de serviços de sustentação da infraestrutura tecnológica.

Art. 10º Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido do superior imediato.

Art. 11º A conta de acesso não utilizada há mais de 180 (cento e oitenta) dias poderá ser cancelada.

CAPÍTULO IV

MOVIMENTAÇÃO INTERNA

Art. 12º Quando houver mudança do usuário para outro setor, os direitos de acesso à Rede Local devem ser readequados, conforme solicitação do novo superior imediato.

Parágrafo único. Os direitos de acesso antigos devem ser imediatamente cancelados conforme solicitação do antigo superior imediato.

CAPÍTULO V

CONTA DE ACESSO BIOMÉTRICO

Art. 13º A conta de acesso biométrico, quando implementada, deve ser vinculada a uma conta de acesso lógico e ambas devem ser utilizadas para se obter um acesso, a fim de atender os conceitos da autenticação de multifatores.

Parágrafo único. O Ibict deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

CAPÍTULO VI

ADMINISTRADORES

Art. 14º A utilização de identificação (*login*) com acesso no perfil de administrador é permitida somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

I. Usuários com perfil técnico poderão solicitar senha com privilégio de administrador nos equipamentos locais.

II. Na necessidade de utilização de *login* com privilégio de administrador do equipamento local, o usuário deverá encaminhar solicitação através de chamado aberto à prestadora de serviços de sustentação da infraestrutura tecnológica.

III. A Disup poderá indeferir o uso de senha com privilégio de administrador dos equipamentos locais nos casos em que entender desnecessária a sua utilização.

IV. Se concedida a permissão ao usuário como administrador local na estação de trabalho, esse será responsável por manter a integridade da máquina, não podendo instalar, desinstalar ou remover qualquer programa sem autorização formal da Disup.

V. Caso constatada a irregularidade, o usuário perderá o acesso como administrador, não mais podendo requerer outra permissão.

VI. Salvo para atividades específicas da área responsável pela gestão da tecnologia da informação do órgão, não será concedida, para um mesmo usuário, identificação (login) com privilégio de administrador para mais de uma estação de trabalho.

VII. Poderão ser concedidas identificações (*login*) de acesso à rede de comunicação de dados a visitante em caráter temporário por meio de chamado aberto à prestadora de serviços de sustentação da infraestrutura tecnológica.

CAPÍTULO VII

RESPONSABILIDADES

Art. 15º É de responsabilidade do superior imediato do usuário comunicar formalmente à Disup o desligamento ou saída do usuário do órgão para que as permissões de acesso à Rede Local sejam canceladas.

Art. 16º Os serviços serão filtrados por programas de *antivírus*, *anti-phishing* e *anti-spam* e, caso algum artefato viole alguma regra de configuração, este será bloqueado ou excluído automaticamente.

Art. 17º É de responsabilidade da Disup o monitoramento da utilização de serviços de rede e de acesso à Internet, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos, bem como bloquear, temporariamente, sem aviso prévio, a estação de trabalho que esteja realizando atividade que coloque em risco a segurança da rede, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica do órgão.

Art. 18º O usuário é responsável por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados à Rede Local e a recursos de tecnologia custodiados ou de propriedade do Ibict.

I. O usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, no caso de sua ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou desconectar-se da estação, para coibir acessos indevidos.

II. A utilização simultânea da conta de acesso à Rede Local em mais de uma estação de trabalho ou notebook deve ser evitada, sendo responsabilidade do usuário titular da conta de acesso os riscos que a utilização paralela implica.

III.O usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha à Rede Local.

Art. 19º O usuário deve informar à Disup qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

Art. 20º É dever de o usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para a Instituição, a saber:

I. Não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;

II. Evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros, para não gerar indisponibilidade de informações internas e externas;

III. Interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo;

IV. Não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso;

V. Não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;

VI. Utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas;

VII. Não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo-as como pessoais e intransferíveis;

VIII. Assinar o Termo de Responsabilidade (Modelo - Anexo A) quanto a utilização da respectiva conta de acesso.

CAPÍTULO VIII

DISPOSIÇÕES GERAIS

Art. 21º Os incidentes que afetem a Segurança das Informações, assim como o descumprimento da Política de Segurança da Informação e Normas de Segurança devem ser obrigatoriamente comunicados pelos usuários à Disup e à Dired.

Art. 22º Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, a prestadora de serviços de sustentação da infraestrutura tecnológica fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

I. Nos casos em que o ator da quebra de segurança for um usuário, a Disup comunicará os resultados ao superior imediato do mesmo para adoção de medidas cabíveis.

II. Ações que violem a POSIC ou que quebrem os controles de Segurança da Informação serão passíveis de sansões civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente.

III. Processo administrativo disciplinar específico deverá ser instaurado para apurar as ações que constituem em quebra das diretrizes impostas por esta Norma e pela POSIC.

IV. A resolução de casos de violação/transgressões omissos nas legislações correlatas será resolvida pelo Comitê de Segurança da Informação - CSI do Ibict.

Art. 23º Esta Resolução entra em vigor na data de sua publicação.

ANEXO A – Modelo de Termo de Responsabilidade

SERVIÇO PÚBLICO FEDERAL

INSTITUTO BRASILEIRO DE INFORMAÇÃO PARA CIÊNCIA E TECNOLOGIA

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF _____, identidade _____, expedida pelo _____, em _____, e lotado no(a)_____deste instituto, DECLARO , sob pena das sanções cabíveis nos termos da legislação vigente que assumo a responsabilidade por:

I. Tratar o(s) ativo(s) de informação como patrimônio do Ibict;

II. Utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do órgão;

III. Contribuir para assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 27 de maio de 2020, que Dispõe sobre Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal;

IV. Utilizar as credenciais, as contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do Ibict;

V. Responder, perante o órgão, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

VI. Acessar a rede corporativa, computadores, Internet e/ou utilização de e-mail, somente com autorização (usuário/senha), por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições contidas na Resolução Normativa que rege o acesso à rede corporativa, computadores, Internet e/ou utilização de e-mail;

VII. Utilizar o correio eletrônico (*e-mail*) colocado a minha disposição somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações, em estrita observância aos procedimentos, normas e disposições contidas na Resolução Normativa que rege o acesso à rede corporativa, computadores, Internet e/ou utilização de e-mail;

VIII. Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

IX. Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

X. Não me ausentar da estação de trabalho sem encerrar a sessão de uso do navegador (*browser*), bloquear estação de trabalho, bem como encerrar a seção do cliente de correio, garantindo assim a impossibilidade de acesso indevido por terceiros;

XI. Não revelar minha senha de acesso à rede corporativa, computadores, Internet e/ou do correio eletrônico (e-mail) a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento;

XII. Responder, em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso.

Local, UF, _____de _____de _____.

_____
Assinatura
Nome do usuário e seu setor organizacional

_____
Nome da autoridade responsável pela autorização do acesso

Histórico de Revisão

ID da versão	Data da Mudança	Autor
Ibict	13/05/2022	Henrique

INSTITUTO BRASILEIRO DE INFORMAÇÃO EM CIÊNCIA E TECNOLOGIA
Diretoria do Instituto Brasileiro de Informação em Ciência e Tecnologia
Coordenação-Geral de Tecnologias de Informação e Informática

DESPACHO

Processo nº: 01302.000407/2022-19
Referência:

Interessados:
Benício Mendes Teixeira Júnior (DIRED)
Virginia Ferreira da Silva Castro (COPAV)
Washington Luis Ribeiro de Carvalho Segundo (CODIC)
Ricardo Medeiros Pimenta (COEPE)
Marcos Pereira de Novais (CGTI)
Henrique Denes Hilgenberg Fernandes (CGTI)

Assunto: Avaliação das propostas para a política de backup, política de gestão de ativos e política de controle de acesso.

Solicito aos membros do Comitê de Segurança da Informação (CSIC) do IBICT a avaliação das propostas de:

- **Políticas de Backup** (10448771)
- **Política de Gestão de ativos** (10448745)
- **Política de Controle de acesso** (10448780)

As contribuições deverão ser submetidas por meio de memorando até o dia **07/10/2022**. Uma reunião futura será agendada para validá-las.

Tiago Emmanuel Nunes Braga
Presidente do CSIC do IBICT
(assinado digitalmente)

Brasília, 22 de setembro de 2022.

Documento assinado eletronicamente por **Tiago Emmanuel Nunes Braga**, **Coordenador-Geral de Tecnologias de Informação e Informática**, em 22/09/2022, às 16:28 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.mcti.gov.br/verifica.html, informando o código verificador **10448860** e o código CRC **DF38E0E3**.

INSTITUTO BRASILEIRO DE INFORMAÇÃO EM CIÊNCIA E TECNOLOGIA
Diretoria do Instituto Brasileiro de Informação em Ciência e Tecnologia
Coordenação-Geral de Pesquisa e Manutenção de Produtos Consolidados
Coordenação de Tratamento, Análise e Disseminação da Informação Científica

Memorando nº 437/2022/IBICT

Brasília, 23 de setembro de 2022

Ao Senhor Presidente do CSIC do IBICT,
Tiago Emanuel Nunes Braga

Assunto: **Reposta ao Despacho IBICT_CGTI (10448860).**

1. Informo ao Senhor Presidente do CSIC do IBICT que aprovo as propostas apresentadas por meio dos documentos SEI No. 10448617, 10448745, 10448771 e 10448780.

Sem mais,

Subscrevo eletronicamente,

Washington Luís R. de Carvalho Segundo
Coordenador da CODIC

Documento assinado eletronicamente por **Washington Luiz Segundo**, **Coordenador de Tratamento, Análise e Disseminação da Informação Científica**, em 23/09/2022, às 08:50 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.mcti.gov.br/verifica.html, informando o código verificador **10450401** e o código CRC **03AC8E5B**.

Anexos

Não Possui.

Referência: Processo nº 01302.000407/2022-19 SEI-IBICT nº 10450401

INSTITUTO BRASILEIRO DE INFORMAÇÃO EM CIÊNCIA E TECNOLOGIA
Diretoria do Instituto Brasileiro de Informação em Ciência e Tecnologia
Coordenação de Ensino e Pesquisa, Ciência e Tecnologia da Informação

Memorando nº 439/2022/IBICT

Rio de Janeiro, 23 de setembro de 2022

Presidente do CSIC do IBICT,

Tiago Emanuel Nunes Braga

Assunto: **Reposta ao Despacho IBICT_CGTI (10448860).**

Informo ao Senhor Presidente do CSIC do IBICT que, após análise, julgo aprovadas as propostas No. 10448617, 10448745, 10448771 e 10448780, elencadas no SEI e a mim atribuídas para emitir respectivo parecer.

Cordialmente,

Documento assinado eletronicamente por **Ricardo Pimenta**, **Pesquisador Titular**, em 23/09/2022, às 09:58 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.mcti.gov.br/verifica.html, informando o código verificador **10450895** e o código CRC **7534D084**.

Anexos

Não Possui.

Referência: Processo nº 01302.000407/2022-19 SEI-IBICT nº 10450895

Correspondência Eletrônica - 10944599

Data de Envio:
24/03/2023 10:10:48

De:
IBICT/Coordenação-Geral de Tecnologias de Informação e Informática do IBICT <cgti@ibict.br>

Para:
marcosnovais@ibict.br
virginiacastro@ibict.br
benicio@ibict.br
denes@ibict.br
tiagobraga@ibict.br

Assunto:
Políticas relacionadas à segurança da informação

Mensagem:
Prezados,

Solicito atenção ao Despacho 10448860, que possuía prazo estabelecido de 07/10/2022. Se faz necessário retorno o mais breve possível com relação à demanda expressa.

Cordialmente,

Tiago Emmanuel Nunes Braga

Coordenador-geral de Tecnologias da Informação e Informática

(assinado digitalmente)

Anexos:
Despacho_10448860.html

INSTITUTO BRASILEIRO DE INFORMAÇÃO EM CIÊNCIA E TECNOLOGIA
Diretoria do Instituto Brasileiro de Informação em Ciência e Tecnologia
Coordenação de Ensino e Pesquisa, Ciência e Tecnologia da Informação

Memorando nº 128/2023/IBICT

Brasília, 09 de maio de 2023.

Ao Senhor Presidente do CSIC do IBICT,

Dr. Tiago Emanuel Nunes Braga

Assunto: **Reposta ao Despacho IBICT_CGTI (10448860).**

Senhor Presidente,

Registro como aprovadas as propostas
Nº 10448617, 10448745, 10448771 e 10448780, elencadas no SEI e a mim atribuídas para emissão de parecer.

Permaneço à disposição.

Respeitosamente,

Documento assinado eletronicamente por **Benicio Mendes Teixeira Junior**, **Chefe da Divisão de Produção e Redes**, em 09/05/2023, às 14:48 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.mcti.gov.br/verifica.html, informando o código verificador **11049665** e o código CRC **D69968C1**.

Anexos

Não Possui.

Referência: Processo nº 01302.000407/2022-19 SEI-IBICT nº 11049665

INSTITUTO BRASILEIRO DE INFORMAÇÃO EM CIÊNCIA E TECNOLOGIA
Diretoria do Instituto Brasileiro de Informação em Ciência e Tecnologia
Coordenação-Geral de Tecnologias de Informação e Informática

Memorando nº 136/2023/IBICT

Brasília, 11 de maio de 2023

Ao Senhor Tiago Emmanuel Nunes Braga
Presidente do CSIC do IBICT

Assunto: **Resposta ao despacho IBICT_CGTI (10448860)**

1. Informo a Vossa Senhoria que, após análise, considero aprovadas a Política de Controle de Acesso (10448780), a Política de Backup (10448771) e a Política de Gestão de Ativos (10448745) deste instituto.

2. Sem mais, coloco-me à disposição.

Atenciosamente,

Documento assinado eletronicamente por **Henrique Denes Hildenberg Fernandes**, **Tecnologista**, em 11/05/2023, às 13:17 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.mcti.gov.br/verifica.html, informando o código verificador **11056215** e o código CRC **2814A8D0**.

Anexos

Não Possui.

Referência: Processo nº 01302.000407/2022-19 SEI-IBICT nº 11056215