Data Center

DIRETRIZES E NORMAS

Dispõe sobre as orientações, as regras e as responsabilidades mandatórias associadas à disciplina e a utilização do Data Center do INCA.

MUNDO **VIRTUAL,**
SEGURANÇA **REAL.**

CONTROLE DE DISTRIBUIÇÃO

Quanto ao grau de confidencialidade, este documento é classificado como **PÚBLICO.**

CONTROLE DE REVISÕES

Data	Revisão	Natureza da Alteração	Autor
02/10/2009	Original	Elaboração	Área de Recursos Tecnológicos - STI
31/03/2015	1ª Revisão	Atualização	Área de Recursos Tecnológicos - STI
20/05/2016	2ª Revisão	Atualização	Área de Recursos Tecnológicos - STI
10/07/2017	3ª Revisão	Atualização	Área de Gov. e Inovação em TIC - STI

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES

1.1 Apresentação

Esta NORMA, estabelecida na forma de Anexo, para observância e aplicação, elaborada pelo **COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES,** é considerada parte integrante e inseparável da **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA e, eventualmente, no que couber, dos seus DOCUMENTOS COMPLEMENTARES integrantes, uma vez que os complementa, embora com ênfase em outros aspectos.

Esta NORMA utiliza, na forma de Anexo, no que couber, o disposto no **GLOSSÁRIO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA.

1.2 Convenções deste Documento

Para os fins de uniformidade dos procedimentos contidos nesta NORMA, considera-se o disposto na **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA.

1.3 Objetivo

Esta NORMA objetiva estabelecer diretrizes e normas para a operação, o acesso físico e as eventuais manutenções a serem realizadas nos ambientes (principal e de contingência) do *Data Center* do INCA, sendo mandatório para todo o INCA.

1.4 Público-alvo

Esta NORMA aplica-se a todos os usuários que necessitem de acesso físico aos ambientes (principal e de contingência).

1.5 Conceitos e Definições

Para os fins de uniformidade dos procedimentos contidos nesta NORMA, considera-se os conceitos e definições que constam do **GLOSSÁRIO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA.

1.6 Referências Legais e Normativas

Esta NORMA obedecerá aos princípios constitucionais, administrativos e ao arcabouço legislativo vigente que rege a Administração Pública Federal.

As referências legais e normativas utilizadas como base para a elaboração desta NORMA são, principalmente, as seguintes:

1.6.1 Boas Práticas

NBR/ISO/IEC 27001:2006 - Gestão de Segurança da Informação, que dispõe sobre os requisitos para Sistemas de Gestão de Segurança da Informação.

2 DATA CENTER

São diretrizes gerais que devem ser observadas e respeitadas:

- É de competência da **GERÊNCIA DE RECURSOS TECNOLÓGICOS**, subordinada a DTI:

- O ambiente do *Data Center* como um todo que é de acesso restrito, visto que abriga equipamentos computacionais e guarda dados institucionais do INCA, em funcionamento ininterrupto.
- Deve ser elaborado um Procedimento de Operação do *Data Center*.
- Deve ser elaborado um Procedimento de Controle e Transferência de Equipamentos para o *Data Center*.
- Deve ser definida a abrangência do *Data Center*, incluindo o ambiente principal, o de contingência e as demais áreas (sala de energia, sala de impressoras, sala de equipamentos e etc).
- O *Data Center* deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração da equipe de Serviços Gerais.
- Situações emergenciais que venham a ocorrer no extra-horários, finais de semana e feriados deverão ser encaminhadas pelos operadores de turno a a **GERÊNCIA DE RECURSOS TECNOLÓGICOS**. Todas as tratativas deverão ser registradas pelo operador do turno em questão.

2.1 Áreas Seguras

Para prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização, , devem ser adotadas as seguintes medidas:

2.1.1 Perímetro de Segurança Física

Deve ser estabelecido um perímetro de segurança (barreiras tais como paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas) para proteger as áreas que contenham informações e recursos de processamento da informação no ambiente do *Data Center*.

O *Data Center* deve ser monitorado por sistema de imagem e ter controle de acesso (entradas e saídas) com a utilização de sistema forte de autenticação (por exemplo, biometria, cartão magnético entre outros), devendo ser registrado (usuário, data e hora) mediante *software* próprio.

O *Data Center* deve contar com proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem..

2.1.2 Controles de Entrada Física

As áreas seguras (escritórios, salas e instalações) devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.

- Sistema de monitorado por circuito de TV fechado.
- Sistema de alarmes para detecção de portas abertas.
- Vigilância dos ambientes interno e externo.
- Segurança física contra acessos não autorizados e interferências do ambiente externo.

Todo acesso físico ao ambiente do *Data Center* deve ser registrado, controlado e monitorado.

Os usuários terão seus privilégios de acesso físico excluídos no momento da decisão de seu desligamento ou transferência.

Os funcionários da **GERÊNCIA DE RECURSOS TECNOLÓGICOS** terão livre acesso físico, permanência e circulação no ambiente, desde que o façam, conforme o controle de acesso definido. Os demais funcionários deverão solicitar autorização à **GERÊNCIA DE RECURSOS TECNOLÓGICOS**, que poderá deferir ou não a autorização. Em caso de ferimento, deve ser providenciada a liberação de permissão no sistema, sendo esta(s) classificada(s) como autorização permanente, temporária, horário de expediente e extra-horário.

Somente será permitido acesso de pessoas externas ao INCA ao ambiente do *Data Center* por ocasião de manutenções preventivas ou corretivas (devem ser informadas antecipadamente, especificando o horário, o equipamento e ações planejadas), de *hardware* ou de *software*, desde que acompanhadas por um funcionário da **GERÊNCIA DE RECURSOS TECNOLÓGICOS**.

Deverá ser executada semanalmente uma auditoria nos acessos ao *Data Center* por meio do relatório do sistema de registro.

O usuário "administrador" do sistema de autenticação forte ficará de posse e administração do coordenador de infraestrutura.

A lista de funções com direito de acesso ao *Data Center* deverá ser constantemente atualizada e salva no diretório de rede.

Nas unidades em que não existirem colaboradores da área de tecnologia da informação, pessoas de outros departamentos deverão ser cadastradas no sistema de acesso para que possam exercer as atividades operacionais dentro do *Data Center*, como: troca de fitas de *backup*, suporte em eventuais problemas, e assim por diante.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado, que deverá preencher a solicitação de acesso, bem como assinar o Termo de Responsabilidade.

O acesso ao *Data Center*, por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do *Data Center* for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.

Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer colaborador responsável pela administração de liberação de acesso.

Devem existir duas cópias de chaves da porta do *Data Center*. Uma das cópias ficará de posse do coordenador responsável pelo *Data Center*, a outra, de posse do coordenador de infraestrutura.

No caso de desligamento de empregados ou colaboradores que possuam acesso ao *Data Center*, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de colaboradores autorizados.

2.2 Segurança de Equipamentos

Para impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização, devem ser adotadas as seguintes medidas:

2.2.1 Gestão de Capacidade

A utilização dos recursos deve ser monitorada e sincronizada e as projeções devem ser feitas para necessidades de capacidade futura, para garantir o desempenho requerido dos Sistemas de Informação Corporativa.

2.2.2 Instalação

Os equipamentos devem ser colocados no local protegido para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.

2.2.3 Cabeamento

O cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações deve ser protegido contra interceptação ou danos.

2.2.4 Refrigeração

Refrigeração ambiente a 21 ºC por sistema duplo independente redundante.

Controle digital permanente de temperatura e umidade dos ambientes.

2.2.5 Energia

Os equipamentos devem ser protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades.

Alimentação elétrica estabilizada ininterrupta monitorada por circuito inteligente.

No-breaks senoidais digitais com modulo de autonomia extendida, com autonomia energética de 8 horas.

2.2.6 Equipamento Fora do Datacenter

Devem ser tomadas medidas de segurança para equipamentos que operem fora do *Data Center*, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências do *Data Center*.

2.2.7 Manutenções

Manutenções em equipamentos em período de garantia somente poderão ser realizadas pela assistência técnica autorizada;

O rompimento do lacre do equipamento hospedado no *Data Center* somente poderá ser realizado por técnico da **GERÊNCIA DE RECURSOS TECNOLÓGICOS**, preferencialmente na presença do responsável pelo equipamento;

Todo evento produzido nas manutenções deverá ser transcrito no sistema que controla os equipamentos hospedados no *Data Center*.

Não é permitida a entrada e ou saída de peças, equipamentos e acessórios da sala do *Data Center* sem o prévio conhecimento e autorização.

A entrada ou retirada de quaisquer equipamentos do *Data Center* somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pelo responsável do *Data Center*, de acordo com os termos do Procedimento de Controle e Transferência de Equipamentos.

2.2.8 Reutilização e Alienação Segura

Todos os equipamentos que contenham mídias de armazenamento de dados devem ser examinados antes do descarte, para assegurar que todos os dados sensíveis e *softwares* licenciados tenham sido removidos ou sobregravados com segurança.

2.2.9 Remoção de Propriedade

Equipamentos, informações ou *software* não devem ser retirados do local sem autorização prévia.

2.2.10 Segurança Lógica

Monitoração do tráfego de rede em tempo real.

Resposta à atividade não autorizada em tempo real.

Gerenciamento centralizado de sensores remotos.

Integração com roteadores, *firewalls*, aplicações de e-mail e SMS.

Integração com o sistema de gerenciamento.

Storage remoto para armazenamento de *backup*.

2.3 Segurança de Sistemas de Informação Corporativa

2.3.1 Aceitação de Sistemas

Devem ser seguidos os critérios de aceitação para novos sistemas, atualizações e novas versões e que sejam efetuados testes apropriados do(s) sistema(s) durante seu desenvolvimento e antes da sua aceitação.

2.4 Operação

2.4.1 Documentação dos Procedimentos de Operação

Os procedimentos de operação devem ser documentados, mantidos atualizados e disponíveis a todos os que deles necessitem.

2.4.2 Gestão de Mudanças

Modificações nos recursos de processamento da informação e sistemas devem ser controladas.

2.4.3 Segregação de Funções

Funções e áreas de responsabilidade devem ser segregadas para reduzir as oportunidades de modificação ou uso indevido não autorizado ou não intencional dos ativos da organização.

2.4.4 Trilha de Produção

Recursos de desenvolvimento, teste e produção devem ser separados para reduzir o risco de acessos ou modificações não autorizadas aos sistemas operacionais.

2.4.5 Cópias de Segurança

Cópias de segurança das informações e dos *softwares* devem ser efetuadas e testadas regularmente, conforme a **NSIC 07 – Gestão de Cópias de Segurança**.

2.4.6 Servidores

Os computadores servidores destinos aos SERVIÇOS CORPORATIVOS devem:

- Operar em conformidade com o acordo de nível de serviço.
- Operar em local com certificado de infraestrutura segura contra ameaças naturais.
- Dispor de mecanismo de redundância, em caso falha em um dos discos, controlado via *hardware*, visando garantir que, em casos específicos de falha de disco, a quebra da disponibilidade do dispositivo de armazenamento não viole o acordo de nível de serviço.
- Dispor de sistema de paridade controlado via *hardware*.

A disponibilidade dos SERVIÇOS CORPORATIVOS, assim como a disponibilidade do *link* de comunicação entre o usuário e o computador servidor, devem estar em conformidade com o acordo de nível de serviço.

- Os administradores dos SERVIÇOS CORPORATIVOS e dos computadores servidores obedecerão aos procedimentos e acordo de nível de serviço.

O espaço em disco disponível para SERVIÇOS CORPORATIVOS deve ser suficiente para a necessidade do INCA.

- Periodicamente a necessidade de espaço deve ser avaliada com todas as áreas de negócio e deve ser apresentado um relatório de avaliação de capacidade.
- O intervalo de avaliação deve ser definido pela Gerencia de Recursos Tecnológicos, não podendo o intervalo ser maior do que 2 anos e menor do que 6 meses.
- Se for avaliado que há necessidade maior de espaço, sendo ocasionada pelo mau uso desse ou não, deve ser apresentado um plano de ação com o fim de otimizar o espaço ou disponibilizar maior espaço para atender à necessidade.

A comunicação entre o usuário e o computador servidor deve ser criptografada pelo protocolo SSL.

Caso o HD desse computador servidor ou HD do *storage* que comporta arquivos desse serviço:

- For substituído sem apresentar falhas, deve ser realizada uma formatação em nível baixo antes de utilizar em outro computador servidor ou ceder a terceiros.
- Apresentar falhas e precisar ser substituído e descartado, o disco do HD deve ser destruído fisicamente antes do descarte.

2.5 Proibições

Não é permitida a entrada com qualquer tipo de bebida e/ou comida, produto fumígeno ou inflamável.

Não são permitidos jogos, servidores de jogos ou aplicações Desktop, tampouco SPAM.

Não são permitidos programas não licenciados ou que infrinjam as leis nacionais ou que coloquem em risco a integridade da rede pela introdução de vírus passiva ou ativa ou incursões destrutivas de *hackers* e demais invasores, bem como façam valer a propagação de pirataria ou quaisquer técnicas consideradas ilegais.

3 DISPOSIÇÕES FINAIS

Devem ser observadas as penalidades dispostas na **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA.

Deve observado disposto na **POLÍTICA DE RESPONSABILIDADES EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES**.

Devem ser observadas as competências e as responsabilidades do **COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** com relação aos DOCUMENTOS COMPLEMENTARES, conforme o disposto no **DOCUMENTO DE CONSTITUIÇÃO DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES**.

Os casos omissos e as dúvidas com relação a esta POLÍTICA devem ser submetidos ao **COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES** do INCA.