Gestão de Cópias de Segurança

DIRETRIZES E NORMAS

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

Dispõe sobre as orientações, as regras e as responsabilidades mandatórias associadas à disciplina para a salva guarda dos dados corporativos do INCA, visando manter a integridade e a disponibilidade da informação e dos recursos de processamento de informação.

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 Campo de Aplicação

Esta NORMA aplica-se, de forma mandatória e em sentido lato, exclusivamente no âmbito do INCA, incluindo todas as suas Unidades Administrativas e Hospitalares, para todo o PÚBLICO-ALVO desta NORMA.

1.4 Objetivo

Este DOCUMENTO objetiva estabelecer diretrizes e normas que se aplicam de forma mandatória a realização e recuperação de cópias de segurança dos dados corporativos do INCA, incluindo as responsabilidades dos membros da TI.

1.5 Público-alvo

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

1.6 Vigência

Esta NORMA tem prazo de validade indeterminado, portanto, sua vigência se estenderá desde sua publicação, gerando efeitos imediatos, até a edição de outro marco normativo que motive sua atualização ou a revogação.

1.7 Publicação

Esta NORMA encontra-se publicada e disponibilizada, pelo **COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES**, para acesso ou *download*, a qualquer tempo, a todos os usuários, de forma permanente nos canais de comunicação internos do INCA (inclusive na Intranet do INCA), disposta de maneira que seu conteúdo possa ser consultado a qualquer momento, sem prejuízo dos pertinentes meios oficiais de publicação aplicáveis, e no D.O.U.

1.8 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.

2 PROPRIEDADE DOS DADOS E DAS INFORMAÇÕES

Todo e qualquer dado ou informação (em formato físico ou lógico) gerada, adquirida, utilizada, armazenada ou que trafegue pela REDE INTERNA DE COMUNICAÇÃO DE DADOS é considerada propriedade exclusiva e patrimônio do INCA, não podendo ser interpretados como de uso pessoal, devendo ser protegida conforme estabelecido nesta POLÍTICA. Como também, todos os documentos e *softwares* produzidos por intermédio de seus colaboradores, durante o exercício de suas atividades profissionais, são de propriedade do INCA.

Toda e qualquer informação produzidas por USUÁRIOS INETRNOS e USUÁRIOS COLABORADORES, no exercício de suas funções, são patrimônio intelectual do INCA e não cabe a seus criadores qualquer forma de direito autoral.

Quando as informações forem produzidas por terceiros para uso exclusivo do INCA, um instrumento próprio obrigará os criadores ao sigilo permanente do conteúdo dos produtos.

É vedada a utilização das informações a que se refere o parágrafo anterior em quaisquer outros projetos ou atividades de uso diverso ao estabelecido pelo INCA, salvo com autorização formal específica emitida pelo responsável pela DTI.

As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelo INCA devem observar, no que couber, o contido nos parágrafos anteriores e nos demais dispositivos integrantes desta POLÍTICA.

3 GESTÃO DE CÓPIAS DE SEGURANÇA

É de competência da **GERÊNCIA DE RECURSOS TECNOLÓGICOS** realizar, disponibilizar, manter e gerenciar cópias de segurança (*backups*) dos SERVIDORES DE DADOS do INCA.

Todos os *backups* devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de *backup*" – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os colaboradores responsáveis pela gestão dos sistemas de *backup* deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o *software* não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do data center.

As fitas de *backup* devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

O tempo de vida e uso das mídias de *backup* deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

As mídias de backups históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de sala-cofre, em local diferente do *Datacenter*.

Os *backups* imprescindíveis, críticos, para o bom funcionamento dos serviços do INCA, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

Na situação de erro de *backup* e/ou *restore* é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse *backup*, eles deverão ser autorizados apenas mediante justificativa de necessidade nos termos do Procedimento de Controle de *Backup* e *Restore*.

Quaisquer atrasos na execução de backup ou *restore* deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Mídias de *Backup*.

Testes de restauração (*restore*) de *backup* devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do *backup*.

Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de *backups* e *restores*, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo coordenador de infraestrutura, nos termos do Procedimento de Controle de *Backup* e *Restore*.

Os colaboradores responsáveis descritos nos devidos procedimentos e na planilha de responsabilidade poderão delegar a um custodiante a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.

4 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.