INSTITUTO FEDERAL
NORTE DE MINAS GERAIS

Número da Norma	Revisão - Data	Emissão	Folha
05/IN05/CSIC/IFNMG	00 - 15/07/2013	15/07/2013	1/7

GESTÃO DE DADOS CORPORATIVOS

ORIGEM

Esta é uma norma complementar à Política de Segurança de Informação e Comunicações (POSIC) e foi elaborada pelo Comitê de Segurança da Informação e Comunicações (CSIC) do Instituto Federal de Educação, Ciência e Tecnologia do Norte de Minas Gerais (IFNMG) instituído pela Portaria nº 304 de 08 de agosto de 2012.

REFERÊNCIA NORMATIVA

Conforme disposto no Regimento do Comitê de Segurança da Informação e Comunicação do IFNMG compete ao CSIC determinar e orientar acerca do uso legal de recursos computacionais dentro de seu domínio.

CAMPO DE APLICAÇÃO

Esta norma se aplica a todo o IFNMG.

OBJETIVOS GERAIS

Estabelecer critérios para a gestão de dados corporativos

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esta norma observa a estrutura proposta pela Norma 01/IN01/CSIC/IFNMG.

APROVAÇÃO

Presidente do CSIC

GESTÃO DE DADOS CORPORATIVOS

1 OBJETIVO

Dar ciência e estabelecer critérios gerais para o uso de software proprietário dentro do IFNMG.

2 FUNDAMENTAÇÃO LEGAL E NORMATIVA.

Conforme disposto na POSIC compete ao CSIC do IFNMG determinar critérios para uso seguro e direcionado dos recursos computacionais e de comunicação dentro e fora do domínio de rede do IFNMG.

3 DEFINIÇÕES

3.1 Para efeito desta norma considera-se:

3.1.1 Dado: Qualquer elemento identificado em sua forma bruta e que, por si só, não conduz a uma compreensão de uma fato ou situação.

3.1.2 Acesso: permissão, privilégio ou capacidade de ler, registrar, atualizar, gerenciar ou administrar a consulta e/ou a manipulação do acervo de dados e informações do IFNMG.

3.1.3 Dado de uso corporativo ou institucional: todos os dados capturados e utilizados nas operações de serviço e administrativas do IFNMG.

3.1.4 Agente: qualquer pessoa ou conjunto de pessoas autorizadas pelo IFNMG para o acesso e/ou tratamento dos dados corporativos: docentes, funcionários, discentes e terceirizados.

3.1.5 Informação: dados contextualizados.

3.1.6 Responsável pela custódia do dado: agente do IFNMG a quem é delegada responsabilidade por uma parte dos dados com o objetivo de garantir a sua integridade e precisão.

3.1.7 Responsável pelo gerenciamento dos dados: é o agente do IFNMG que fornece serviços de processamento de dados como suporte aos usuários dos dados.

3.1.8 Administrador de Sistemas e Rede: responsável pela segurança, disponibilidade e integridade dos dados e serviços disponíveis no ambiente computacional sob seu controle e responsável por manter o sigilo das senhas de acesso a esse ambiente.

3.1.9 Usuário de dados: agente autorizado a ler, registrar, e/ou atualizar dados;

4 GESTÃO DE DADOS CORPORATIVOS

4.1 O IFNMG é proprietário de todos os seus dados corporativos e detém os direitos autorais de

todas as políticas, manuais e compilações destes dados.

4.2 Aos responsáveis pela custódia dos dados cabe:

4.2.1 identificar os itens de dados corporativos e a sua fonte primária;

4.2.2 identificar e documentar a quem é permitido o acesso ao dado e o nível de acesso;

4.2.3 autorizar acesso aos dados;

4.2.4 especificar os requisitos de segurança de acesso;

4.2.5 estabelecer procedimentos para a obtenção de autorização para acesso aos dados;

4.2.6 implementar processos que mantenham a integridade, precisão, temporalidade, consistência, padronização e o valor do dado;

4.2.7 garantir através de procedimentos que o dado seja captado e utilizado de forma adequada;

4.2.8 monitorar as atividades de acesso aos dados e notificar as exceções ao Diretor de TI.

4.3 Aos responsáveis pela gerência dos dados compete:

4.3.1 implementar a segurança de acesso aos dados como especificado pelo Responsável pela Custódia do Dado, assim como de acordo com os padrões e orientação de acesso aos dados;

4.3.2 prover acesso aos dados pelos usuários como especificado pelo Responsável pela Custódia do Dado;

4.3.3 garantir que os mecanismos de proteção física dos dados estejam instalados e operando de forma satisfatória;

4.3.4 monitorar a efetividade dos controles implantados contra tentativas de acesso não autorizado;

4.3.5 acessar os dados, da forma autorizada pelo Responsável pela Custódia do Dado, para a execução das tarefas necessárias para garantir a disponibilidade e acessibilidade;

4.3.6 garantir que todos os dados possuem um responsável pela sua custódia;

4.3.7 prover e dar suporte aos sistemas e aplicações necessárias para atender às especificações dos Responsáveis pela Custódia do Dado para a manutenção e disseminação dos dados;

4.3.8 proteger os dados contra destruição, modificações ou acessos durante as transferências

eletrônicas ou físicas de um local para outro;

4.3.9 documentar e promover o valor do dado para os objetivos do IFNMG e facilitar o compartilhamento e a integração dos dados;

4.3.10 gerenciar o uso de padrões comuns de definição de dados em toda o IFNMG.

4.4 Aos usuários de dados compete:

4.4.1 acessar os dados conforme a autorização dada pelo Responsável pela Custódia do Dado;

4.4.2 garantir que os mecanismos de proteção física dos dados estejam instalados e operando de forma satisfatória.

4.5 É vetado aos usuários de dados divulgar qualquer dado sem a permissão do responsável pela custódia.

4.6 É política do IFNMG manter os dados corporativos integrados e íntegros através de todas as suas instâncias, permitindo que os seus administradores acessem as informações que necessitam, dentro de um ambiente controlado.

4.7 Novos sistemas desenvolvidos ou adquiridos de terceiros devem se integrar dos sistemas corporativos existentes, atendendo requisitos técnicos para esta integração

4.8 Ao responsável pela custódia dos dados cabe:

4.8.1 identificar os itens de dados corporativos e a sua fonte primária;

4.8.2 identificar e documentar a quem é permitido o acesso ao dado e o nível de acesso;

4.8.3 autorizar acesso aos dados;

4.8.4 especificar os requisitos de segurança de acesso;

4.8.5 estabelecer procedimentos para a obtenção de autorização para acesso aos dados;

4.8.6 implementar processos que mantenham a integridade, precisão, temporalidade, consistência, padronização e o valor do dado;

4.8.7 garantir através de procedimentos que o dado seja captado e utilizado de forma adequada;

4.8.8 monitorar as atividades de acesso aos dados e notificar as exceções ao Diretor de Gestão de TI.

4.9 Aos responsáveis pela gerência dos dados compete:

4.9.1 implementar a segurança de acesso aos dados como especificado pelo Responsável pela Custódia do Dado, assim como de acordo com os padrões e orientação de acesso aos dados;

4.9.2 prover acesso aos dados pelos usuários como especificado pelo Responsável pela Custódia do Dado;

4.9.3 garantir que os mecanismos de proteção física dos dados estejam instalados e operando de forma satisfatória;

4.9.4 monitorar a efetividade dos controles implantados contra tentativas de acesso não autorizado;

4.9.5 acessar os dados, da forma autorizada pelo Responsável pela Custódia do Dado, para a execução das tarefas necessárias para garantir a disponibilidade e acessibilidade;

4.9.6 garantir que todos os dados possuem um responsável pela sua custódia;

4.9.7 prover e dar suporte aos sistemas e aplicações necessárias para atender às especificações dos Responsáveis pela Custódia do Dado para a manutenção e disseminação dos dados;

4.9.8 proteger os dados contra destruição, modificações ou acessos durante as transferências eletrônicas ou físicas de um local para outro;

4.9.9 documentar e promover o valor do dado para os objetivos do IFNMG e facilitar o compartilhamento e a integração dos dados;

4.9.10 gerenciar o uso de padrões comuns de definição de dados em toda o IFNMG.

4.10 Aos usuários de dados compete:

4.10.1 acessar os dados conforme a autorização dada pelo Responsável pela Custódia do Dado;

4.10.2 garantir que os mecanismos de proteção física dos dados estejam instalados e operando de forma satisfatória.

4.10.3 É vetado aos usuários de dados divulgar qualquer dado sem a permissão do responsável pela custódia.

4.10.4 O IFNMG é proprietário de todos os seus dados corporativos e detém os direitos autorais de todas as políticas, manuais e compilações destes dados.

4.10.5 É política do IFNMG manter os dados corporativos integrados e íntegros através de todas as suas instâncias, permitindo que os seus administradores acessem as informações que

necessitam, dentro de um ambiente controlado.

4.10.6 Os novos sistemas desenvolvidos ou adquiridos de terceiros devem se integrar dos sistemas corporativos existentes, atendendo requisitos técnicos para esta integração.

4.11 Os prestadores de serviços ao IFNMG que, por força de contrato, tenham acesso a qualquer de seus dados corporativos deverão ser signatários de um ACORDO DE CONFIDENCIALIDADE que será firmado no ato da contratação dos serviços. O Anexo desta norma traz um modelo de referência para um acordo de confidencialidade.

5 GESTÃO DE CÓPIAS DE SEGURANÇA – BACKUP

5.1.1 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.

5.1.2 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.

5.1.3 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.

5.1.4 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.

5.1.5 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.

5.1.6 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.

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

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

5.1.9 Os backups imprescindíveis, críticos, para o bom funcionamento dos serviços do IFNMG, 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.

5.1.10 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.

5.1.11 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.

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

5.1.13 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.

5.1.14 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.

5.1.15 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.

5.1.16 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.

6 DISPOSIÇÕES GERAIS

6.1 Os casos omissos e as dúvidas com relação a esta Norma serão submetidos ao Presidente do CSIC que, se considerar necessário fará convocação de reunião do Comitê.

7 VIGÊNCIA

7.1 Esta Norma entra em vigor a partir da data de sua publicação.