Conselho Federal de Química

Plenário
Presidência
Gabinete

PORTARIA Nº 92, DE 6 DE SETEMBRO DE 2024

Aprova a Política de recuperação de dados e estabelece diretrizes para cópia e armazenamento de dados, no âmbito do Conselho Federal de Química.

O PRESIDENTE DO CONSELHO FEDERAL DE QUÍMICA (CFQ), no uso das atribuições que lhe foram conferidas pelos incisos II e XXVI do art. 74 da Resolução Normativa CFQ Nº 307, de 22 de março de 2023;

Considerando a Instrução Normativa GSI/PR N° 01, de 27 de maio de 2020 que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

Considerando a ABNT NBR ISO/IEC 27002: 2013, que contém o código de Prática para controles de Segurança da Informação;

Considerando a ABNT NBR ISO/IEC 27002:2013, que contém o código de Prática para controles de Segurança da Informação;

Considerando a Lei n° 13.709/2018, que dispõe sobre a Lei Geral de Proteção de Dados;

Considerando o Modelo de Política de Backup do Programa de Privacidade e Segurança da Informação da Secretaria de Governo Digital;

Considerando a Portaria CFQ nº 182, de 6 de outubro de 2022, que dispõe sobre a institucionalização da Política de Segurança da Informação (POSIN) no âmbito do Conselho Federal de Química (CFQ) e dá outras providências;

Resolve:

Art. 1º Aprovar, no âmbito do Conselho Federal de Química, a Política de recuperação de dados, que tem como objetivo estabelecer diretrizes para a cópia e armazenamento de dados, em complemento às diretrizes estabelecidas no Capítulo II, na Seção V, Subseção II, da Política de Segurança da Informação, institucionalizada na Portaria CFQ nº 182, de 6 de outubro de 2022.

CAPÍTULO I

DISPOSIÇÕES GERAIS

Seção I

Conceitos e definições

Art. 2º Para os fins desta Política, considera-se:

I. administrador de backup: pessoa ou equipe responsável pelos procedimentos de elaboração de planos de backup, configuração, execução, monitoramento, elaboração de padrões, atendimentos avançados, resolução de incidentes e testes dos procedimentos de backup e restauração, devendo ser designado entre os empregados públicos do CFQ, com formação ou capacitação técnica compatível a tais atribuições;

II. área técnica: unidade responsável pela operação técnica dos ativos e serviços de Tecnologia da Informação e Comunicações - TIC;

III. ativo: qualquer coisa que tenha valor para a organização;

IV. backup (ou cópia de segurança): conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação, tendo fidelidade ao original assegurada; este termo também é utilizado para identificar a mídia em que a cópia é realizada;

V. backup full (ou completo): modalidade de backup em que todos os dados a serem salvaguardados são copiados integralmente - cópia de segurança completa - para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último backup;

VI. backup diferencial: modalidade de backup em que são salvaguardados apenas dados novos ou modificados desde o último backup completo efetuado;

VII. backup incremental: modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup, seja ele completo, diferencial ou incremental, são salvaguardados;

VIII. base de dados (ou banco de dados): base de dados ou coleção de dados inter-relacionados, armazenando informações sobre um domínio específico; são conjuntos de registros organizados que se relacionam de forma a criar algum sentido - informação, e dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;

IX. código fonte: é o conjunto de palavras ou símbolos escritos de forma ordenada, contendo instruções em uma das linguagens de programação existentes, de maneira lógica;

X. computação em nuvem: modelo computacional que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou de interação com o provedor de serviços;

XI. confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados ou credenciados;

XII. criticidade: grau de importância da informação para a continuidade das atividades e serviços;

XIII. custódia: consiste na responsabilidade de se guardar um ativo para terceiros; a custódia não permite automaticamente o acesso ao ativo e nem o direito de conceder acesso a outros;

XIV. dado: informação preparada para ser processada, operada e transmitida por um sistema ou programa de computador;

XV. descarte: eliminação correta dos dados, unidades de armazenamento e acervos digitais;

XVI. disponibilidade: garantia de que o dado esteja acessível e utilizável sob demanda de pessoa ou entidade devidamente autorizada;

XVII. escopo: informações dos dados digitais a serem salvaguardados, com apontamento do local;

XVIII. gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem, fornecendo uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;

XIX. gestor da informação: agente público formalmente responsável pela administração do serviço de TIC/sistema e pelas informações produzidas em seu processo de trabalho, devendo ser um gestor da área negocial;

XX. janela de backup: intervalo de tempo durante o qual as cópias de segurança sob execução agendada ou manual poderão ser executadas;

XXI. log ou registro de auditoria: registro de eventos relevantes em um dispositivo ou sistema computacional, para posterior análise, podendo ser gerado por sistemas operacionais, aplicações, entre outros;

XXII. operador de backup: pessoa responsável por procedimentos de atendimento de primeiro nível, acompanhamento de execução de rotinas de backup e realização de restaurações de arquivos de usuários, devendo ser designado entre os empregados públicos ou terceirizados

do CFQ com formação ou capacitação técnica compatível às suas atribuições;

XXIII. plano de backup: documento formal onde são definidos os dados que serão armazenados, periodicidade de execução da cópia e tempo de retenção, de acordo com as orientações da Política de recuperação de dados;

XXIV. repositório de arquivo: conjunto de documentos ou lugar onde os documentos são guardados;

XXV. retenção: período em que o dado copiado no backup ficará retido e disponível para uso numa eventual recuperação antes de ser substituído por uma versão mais nova; e

XXVI. zero fill (preenchimento com zeros): técnica utilizada para apagar os dados de um dispositivo de armazenamento antes do descarte ou aproveitamento, garantindo que nenhum dado pessoal ou confidencial possa ser recuperado por terceiros.

Seção II

Escopo

Art.3º Sistemas, bases de dados e repositórios de arquivos digitais institucionais do CFQ serão obrigatoriamente submetidos a processo de *backup*.

§1° A impossibilidade de submissão ao processo de backup de qualquer sistema, base de dados ou repositório de arquivos deverá ser comunicada ao Comitê de Governança Digital - CGD pelo administrador de backup.

§2° 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 pela Gerência de Tecnologia da Informação e Comunicação - GETIC, salvo se integrantes de um plano de *backup* formalmente definido.

Art. 4º Sistemas, bases de dados e repositórios de arquivos institucionais devem possuir um plano de backup específico, devidamente assinado pelo gestor da informação, gestor da GETIC e administrador de *backup*.

Art.5º O *backup*, teste e salvaguarda dos dados em formato digital pertencentes a do CFQ, mas custodiados por outras entidades, públicas ou privadas, devem estar garantidos nos acordos ou contratos que formalizam a relação entre os envolvidos.

Seção III

Regras Gerais

Art.6º A Política de recuperação de dados deve ser compatível com a gestão de continuidade de negócios em nível organizacional, devidamente amparados nas estratégias de governança de TIC do CFQ.

Art.7º As rotinas de *backup* devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando um incidente ocasionar indisponibilidade de serviços de TIC.

Art.8º As rotinas de *backup* devem possuir requisitos mínimos específicos de acordo com o tipo de serviço de TIC ou dado salvaguardado, dando prioridade aos serviços de TIC críticos da organização.

Parágrafo único. A mensuração da criticidade de um serviço será realizada pela elaboração de matriz de risco que considerará a probabilidade versus o impacto.

Art.9º O CGD deverá aprovar lista de sistemas com a designação do respectivo gestor da informação e sua classificação quanto à criticidade, críticos e não críticos.

Art.10. Os backups devem estar em conformidade com a legislação vigente, em especial à Lei Geral de Proteção de Dados - LGPD.

Art.11. Recomenda-se que os backups sejam armazenados de forma criptografada, considerando as melhores práticas de mercado e normas vigentes.

Seção IV

Das Ferramentas de Backup

Art. 12. As rotinas de *backup* devem utilizar soluções especializadas para este fim, de forma automatizada, e deve ser documentada em artefatos que comprovem sua execução.

Art. 13. Os *backups* dos serviços de TIC devem ser realizados utilizando-se as seguintes frequências temporais:

I. diária;

II. semanal;

III. mensal; e

IV. anual.

Art. 14. Especificidades dos serviços de TIC críticos e não críticos podem demandar frequência e tempo de retenção diferenciados, que devem estar devidamente registrados no plano de backup do sistema, base de dados e repositório de arquivos.

Art. 15. A solicitação de salvaguarda dos dados referentes aos serviços de TIC críticos e aos serviços não críticos deve ser realizada pelos responsáveis técnicos dos serviços de TIC, com a anuência prévia e formal dos gestores das informações, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

I. escopo:

a) código fonte;

b) banco de dados;

c) repositório de arquivos;

d) arquivos de configuração de servidores e ativos de rede; e

e) máquinas virtuais.

II. tipo de backup: completo, incremental, diferencial, podendo ser uma associação destes;

III. frequência temporal de realização do backup: diária, semanal, mensal, anual, podendo ser uma associação destes;

IV. retenção: deverá ser definida com base na criticidade, frequência da atualização dos dados e características específicas de cada sistema;

V. RPO - *recovery point objective*: indicador que limita o período de volta no tempo, e define a quantidade máxima tolerada de dados perdidos de uma ocorrência de falha para o último *backup* válido; e

VI. RTO - *recovery time objective*: indicador que mensura o tempo máximo em que um sistema ou uma informação pode ficar indisponível após um incidente.

Art. 16. Os backups podem ser classificados como on-line ou *off-site*, a depender da forma de acesso ao *backup* realizado, da seguinte forma:

I. *On-line*: uma vez realizado, o backup é acessível dentro da rede do CFQ;

II. *Off-site*: uma vez realizado, o backup é armazenado em outro data center, geograficamente separado, ou em serviço de backup em nuvem, desconectado da rede do CFQ.

Art. 17. Os *backups* dos sistemas, base de dados ou repositório de arquivos, que sejam críticos, devem possuir, ao menos, duas cópias, sendo um *on-line* e outro *off-site* ou em arquiteturas diferentes de armazenamento.

Art. 18. A recuperação de dados não será viabilizada em caso de perdas anteriores à conclusão da cópia de segurança.

Parágrafo único. Dados criados ou modificados entre execuções de cópias de segurança subsequentes não serão protegidos por soluções de backup.

Art. 19. Legislações e normas vigentes sobre o período de armazenamento de dados deverão ser observadas em razão de especificidades que podem exigir o armazenamento de backups por longos períodos ou até mesmo de forma vitalícia.

Seção V

Uso da rede

Art. 20. O administrador de *backup* deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados do CFQ, garantindo que o tráfego necessário às suas atividades não ocasione problemas aos demais serviços de TIC.

Art. 21. A execução do *backup* deve concentrar-se, preferencialmente, no período de janela de backup, definido pelo administrador de backup.

Seção VI

Das unidades de armazenamento de backups.

Art. 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*; e

VI. a vida útil da unidade de armazenamento de *backup*.

Art. 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.

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

Art. 25. Todos os ativos relacionados ao armazenamento dos *backups* devem ser acondicionados em locais apropriados com controle de fatores ambientais sensíveis, como umidade e temperatura, e com acesso restrito a pessoas autorizadas pelo administrador de *backup*.

Parágrafo único. *Backups* armazenados com pelo menos duas redundâncias poderão ter contingência em local a ser definido, sem controle de fatores ambientais sensíveis, desde que o acesso seja restrito a pessoas autorizadas pelo administrador de backup.

Art. 26. Quando da necessidade de descarte de unidades de armazenamento de backups, quando e se aplicável, tais recursos devem ser inutilizados por meio de destruição física ou submetidos a um procedimento duplo de "zero filling" para sobrescrever todos os dados no disco com zeros, atentando-se ao descarte sustentável e ambientalmente correto.

Seção VII

Dos testes de Backup

Art. 27. A realização regular do processo de teste de dados é obrigatória, com um intervalo máximo de 30 (trinta) dias, e deverá ser documentada em artefatos que comprovem sua execução, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados a fim de detectar eventuais falhas lógicas e físicas.

Art. 28. Os testes de restauração dos *backups*, se possível, devem ser realizados em servidores diferentes dos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis.

Art. 29. A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de *backup* devem ser devidamente registradas no plano de backup.

CAPÍTULO II

DAS RESPONSABILIDADES

Art. 30. O administrador de *backup* e o operador de *backup* devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de armazenamento e *backup*.

Art. 31. O administrador de *backup* e operador de *backup* deverão ser designados pelo Gerente da GETIC, por meio de despacho processual.

Art. 32. São atribuições do administrador de *backup*:

I. propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pelo CFQ;

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. verificar os eventos gerados pela solução de *backup*, tomando as providências necessárias para remediação de eventuais falhas;

VI. tomar medidas preventivas para evitar falhas;

VII. reportar imediatamente ao CGD incidentes ou erros que causem indisponibilidade ou impossibilitem a execução ou restauração de *backups*;

VIII. gerenciar mensagens e registros de auditoria e *logs* de execução dos *backups*;

IX. disponibilizar informações que subsidiem as decisões referentes à gestão de capacidade relacionada aos *backups*;

X. propor modificações ao CGD visando ao aperfeiçoamento da política de recuperação de dados;

XI. coordenar a execução dos testes de restauração e analisar os relatórios de execução; e

XII. criar e modificar planos de *backup*.

Art. 33. São atribuições do operador de *backup*:

I. aplicar o plano de backup na estrutura de *backup* existente;

II. restaurar ou recuperar os backups em caso de necessidade;

III. operar e manusear as unidades de armazenamento de *backups*;

IV. informar ao administrador de *backup* qualquer problema que impossibilite a criação ou restauração de um backup; e

V. executar os testes de restauração de *backup*.

Art. 34. São atribuições do gerente da GETIC:

I. solicitar restaurações de dados, com anuência do gestor da informação;

II. sanar dúvidas técnicas do administrador de *backup* acerca das informações salvaguardadas;

III. validar, tecnicamente, o resultado das restaurações eventualmente solicitadas;

IV. validar, tecnicamente, o resultado dos testes de restauração dos backups; e

V. verificar periodicamente se as definições do plano de backup estão devidamente configuradas na estrutura de backup vigente.

VI. Aprovar planos de *backups*.

Art. 35. São atribuições dos gestores da informação:

I. Formalizar o backup e restauração das informações geridas; e

II. validar, negocialmente, o resultado das restaurações eventualmente solicitadas.

Art. 36. A solicitação de *backup* ou restauração de dados que tenham sido salvaguardados deve ser realizada por meio da abertura de chamado técnico.

CAPÍTULO III

DAS METAS

Art.37. A GETIC terá como metas iniciais os seguintes prazos:

I. até 3 (três) meses após a publicação desta Portaria para elaborar lista de sistemas com classificação quanto a criticidade (críticos e não críticos), encaminhando-a para aprovação do CGD;

II. até 6 (seis) meses após a publicação desta Portaria para elaborar 100% dos planos de backup dos serviços críticos de TIC;

III. até 12 (doze) meses após a publicação desta Portaria para providenciar a implementação de todos os planos de *backup* dos serviços críticos de TIC;

IV. até 12 (doze) meses após a publicação desta Portaria, para elaborar 100% dos planos de *backup* dos serviços não críticos de TIC; e

V. até 18 (dezoito) meses após a publicação desta Portaria, para providenciar a implementação de todos os planos de *backup* dos serviços não críticos de TIC.

Art. 38. A lista de sistemas e os planos de backup deverão ser atualizados sempre que necessário e revisados no mínimo a cada 12 (doze) meses.

Art. 39. Os planos de *backup* de novos sistemas, que surgirem após o prazo referente ao inciso V do art. 37, devem ser implementados em até 3 (três) meses após a implantação do sistema.

CAPÍTULO IV

DISPOSIÇÕES FINAIS

Art. 40. O Comitê de Governança Digital realizará a revisão deste ato normativo ordinariamente a cada dois anos.

Parágrafo único. A revisão poderá ocorrer a qualquer tempo, quando houver mudanças significativas nos requisitos de segurança da informação que influenciem a gestão de incidentes de segurança da informação no CFQ.

Art. 41. Os casos omissos serão resolvidos pelo Comitê de Governança Digital.

Art. 42. Esta Portaria entra em vigor nesta data.

Dê-se ciência.

Publique-se.

Brasília, 6 de setembro de 2024.

JOSÉ DE RIBAMAR OLIVEIRA FILHO

Presidente

SCS Quadra 09, Edifício Parque Cidade Corporate, Torre B, 9º andar
Brasília/DF, CEP 70.308-200
Telefone: (61) 2099-3300 - www.cfq.org.br