PORTARIA Nº 255, DE 14 DE NOVEMBRO DE 2023

Estabelece diretrizes de segurança da informação para o inventário e controle de ativos corporativos (hardware) do Conselho Federal de Química.

O PRESIDENTE DO CONSELHO FEDERAL DE QUÍMICA (CFQ), no uso das atribuições que lhe foram conferidas pelo art. 11, da Lei Federal n.º 2.800, de 18 de junho de 1956;

Considerando o previsto nos incisos II e XXVI do art. 74 da Resolução Normativa CFQ nº 307, de 22 de março de 2023;

Considerando a Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências;

Considerando a Lei nº 13.709 de 14 de agosto de 2018 - Lei Geral de Proteção de Dados;

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 Instrução Normativa GSI/PR N° 03, de 28 de maio de 2021, que dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

Considerando a Norma Brasileira ABNT NBR ISO/IEC 27002 - Código de prática para controles de segurança da informação;

Considerando o *Framework CIS Controls* V8 desenvolvido pelo Center for Internet Security® (CIS) - conjunto prioritário e prescritivo de práticas recomendadas de segurança cibernética e ações defensivas que podem ajudar a prevenir os ataques mais generalizados e perigosos, dando suporte à conformidade em uma era de múltiplas estruturas;

Considerando que a Gestão de Ativos tem um papel crítico no monitoramento de segurança, resposta a incidentes, *backup* e recuperação de sistemas;

Considerando a importância de determinar a amplitude do parque de ativos tecnológicos do Conselho Federal de Química, é necessário existir um inventário atualizado dos ativos de TIC;

Resolve:

Art. 1º Estabelecer diretrizes para realização de gestão ativa, que compreenderá inventário, rastreamento e correção de todos os ativos corporativos (ativos com potencial para armazenar ou processar dados, incluindo se dispositivos de usuários final, dispositivos de rede, dispositivos não computacionais/internet das coisas -IOT e servidores de ambientes virtuais, baseados em nuvem e físicos) do Conselho Federal de Química.

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 2º Para efeitos desta Norma, serão considerados os conceitos e as definições de segurança da informação estabelecidos pela Portaria GSI/PR N° 93, de 18 de outubro de 2021, que aprova o Glossário de Segurança da Informação, destacando-se:

I. ATIVO DE REDE - equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores;

II. ATIVOS DE INFORMAÇÃO - os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso;

III. 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;

IV. CUSTODIANTE - aquele que, de alguma forma, total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema estruturante - ou dos ativos de informação que compõem o sistema de informação - que não lhe pertence, mas que está sob sua custódia; e

V. CUSTODIANTE DA INFORMAÇÃO - qualquer indivíduo ou estrutura de órgão ou entidade da APF, 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 SI comunicadas pelo proprietário da informação.

CAPÍTULO II

DAS DIRETRIZES GERAIS

Art. 3º O processo de inventário de ativos de informação deve considerar, preliminarmente, os objetivos estratégicos do CFQ, seus processos internos, os requisitos legais e sua estrutura organizacional.

Art.4º Todos os ativos de informação e de processamento que utilizem infraestrutura de Tecnologia da Informação, enquanto permanecerem sob responsabilidade ou custódia do CFQ, devem ser identificados.

Parágrafo único. Inventariar ativos requer ações técnicas e processuais que prestam contas e gerenciam o inventário de ativos corporativos e todos os dados associados ao longo de seu ciclo de vida.

Art. 5º O inventário inclui ativos conectados à infraestrutura física, virtual, bem como, aqueles dentro dos ambientes de nuvem.

Parágrafo único. O inventário a que se refere o caput deste artigo abrange os ativos regularmente conectados à infraestrutura de rede corporativa, mesmo que não sejam de propriedade do CFQ.

Art. 6º As informações registradas no inventário de ativos corporativos (*hardware*) devem ser revisadas em periodicidade não superior a 1 (um) ano e as anomalias encontradas devem ser apresentadas ao Comitê de Governança Digital (CGD).

Art. 7º O inventário deve incluir todos os ativos de informação e processamento, que utilizem a infraestrutura tecnológica do CFQ, conectados ou não à rede corporativa, e conter informações indispensáveis às necessidades de recuperação ou de substituição eficiente dos ativos em caso de desastre e fornecer subsídios aos processos de:

I. Segurança das Infraestruturas Críticas de Informação;
II. Gestão da Segurança da Informação;
III. Gestão de Riscos;
IV. Gestão de Continuidade de Negócios;
V. Gerenciamento de Configuração;
VI. Gerenciamento de Liberação;
VII. Gerenciamento de Problemas;
VIII. Central de Serviços;
IX. Gerenciamento de Mudanças;
X. Gerenciamento de Incidentes; e
XI. Gestão da Informação e do Conhecimento.

Art. 8º Informações de ativos na rede deverão ser coletadas de forma ativa e dinâmica, visando o controle de dispositivos dentro da rede, e mantidos em uma plataforma de controle de ativos.

Parágrafo único. Quando não for possível o registro automático, deverá ser realizado o registro manual.

CAPÍTULO III

DAS DIRETRIZES ESPECÍFICAS

Art. 9º O inventário deverá ser preciso, detalhado e atualizado com todos os ativos corporativos com potencial para armazenar ou processar dados, incluindo dispositivos de usuário final, portáteis e móveis, dispositivos de rede, dispositivos não computacionais/IoT e servidores.

Art. 10. O detalhamento dos ativos deve contemplar, no mínimo, e, quando aplicável, o seguinte conjunto de informações:

I - identificação única, tais como matrícula, número patrimonial, nome, QR *Code*, *Radio Frequency Identification* - RFID;

II - tipo de ativo;

III - descrição do ativo;

IV - localização;

V - unidade responsável;

VI - proprietário do ativo de informação;

VII - custodiantes;

VIII -informações complementares sobre software, como versão, fornecedor, formato, data de instalação, licenças de uso, disponibilidade de suporte, cópia de segurança (backup);

IX - aprovação de instalação na rede corporativa; e

X - informações complementares sobre hardware, como endereço de rede, se estático, endereço de hardware (*MAC Address*), nome da máquina, proprietário do ativo de dados, departamento para cada ativo e se o ativo foi aprovado para se conectar à rede.

Art. 11. Recomenda-se que o detalhamento dos ativos contemple, também, sempre que possível:

I - o levantamento das interfaces e das interdependências internas e externas dos ativos de informação considerados críticos, bem como os impactos quando da indisponibilidade ou destruição de tais ativos de informação, seja no caso de incidentes ou de desastres;

II - os requisitos de segurança da informação categorizados, no mínimo, em 5 (cinco) categorias de controle:

a) tratamento da informação;

b) controles de acesso físico e lógico;

c) gestão de risco de segurança da informação;

d) tratamento e respostas a incidentes em redes computacionais; e

e) gestão de continuidade dos negócios nos aspectos relacionados à segurança da informação.

Art. 12. O inventário de ativos de TI deve ser único e assegurar compatibilidade e exatidão de conteúdo com outros inventários em uso no CFQ, a exemplo do controle patrimonial.

Art. 13. Ativos não autorizados deverão ser tratados semanalmente, podendo a Gerência de Tecnologia da Informação - GETIC remover o ativo da rede, negar seu acesso remoto ou colocar o ativo em quarentena.

Art. 14. Cabe ao gestor de segurança da informação coordenar o processo de mapeamento de ativos de informação, bem como designar um agente responsável pela gestão dos ativos de informação, dentre os servidores efetivos do Conselho Federal de Química.

Parágrafo único. O agente responsável pela gestão de ativos de informação será nomeado por portaria.

Art. 15. Cabe ao agente responsável pela gestão dos ativos de informação:

I - identificar e classificar os ativos de informação por nível de criticidade;

II - identificar potenciais ameaças aos ativos de informação;

III - identificar vulnerabilidades dos ativos de informação;

IV - 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;

V - autorizar a atualização do relatório mencionado no inciso IV do caput; e

VI - avaliar os riscos dos ativos de informação ou do grupo de ativos de informação.

CAPÍTULO IV

DAS RESPONSABILIDADES

Art. 16. Cada ativo de informação em uso no CFQ deve ter um proprietário formalmente instituído por sua posição ou cargo, responsável primário do ativo.

Art. 17. À GETIC compete:

I - a descrição do ativo de informação;

II - a comunicação das regras de segurança da informação do ativo, alinhadas à Política de Segurança da Informação do CFQ, a todos os custodiantes e usuários;

III - o monitoramento contínuo do cumprimento das exigências de segurança da informação; e
IV - a indicação dos riscos de segurança da informação que podem afetar os ativos.

Art. 18. O proprietário do ativo de informação deve assumir, no mínimo, as seguintes responsabilidades:

I - reforçar a comunicação das regras de segurança da informação do ativo, padronizadas pela GETIC, alinhadas à Política de Segurança da Informação do CFQ, a todos os custodiantes e usuários;

II - garantia de cumprimento das exigências de segurança da informação;

III - garantia do adequado manuseio dos ativos sob sua responsabilidade, considerando a classificação das informações nele contidas; e

IV - comunicar à GETIC, via chamado aberto no GLPI, quando houver mudança de localização física no ambiente do CFQ ou custódia do ativo.

Art. 19. O proprietário do ativo de informação poderá delegar as tarefas de rotina para um custodiante, providência que não afastará, todavia, a responsabilidade do primeiro.

CAPÍTULO V

DA GESTÃO DO INVENTÁRIO DOS ATIVOS

Seção I

Controle de Redes

Art. 20. Requisitos mínimos de controle devem ser implementados na rede corporativa para assegurar a gestão adequada dos ativos de processamento (hardware) inventariados, entre os quais:

I - utilização de ferramenta de varredura ativa ou passiva para manter automaticamente o inventário atualizado;

II - utilização de ferramentas de gerenciamento de endereço *Internet Protocol* - IP para atualizar o inventário;

III - controle sobre quais ativos podem ser conectados à rede corporativa; e

IV - garantia de remoção da rede corporativa ou de colocação em quarentena de ativos não autorizados ou de atualização do inventário em tempo hábil.

Seção II

Controle de Ativos de Processamento

Art. 21. O processo de gerência de configuração deve assegurar que o inventário dos ativos seja adequadamente gerenciado, atualizado e monitorado em cada fase do ciclo de vida do ativo, quais sejam:

I - aquisição;

II - implementação;

III - manutenção; e

IV - descarte.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 22. 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 o uso seguro de ativos de TIC, de forma a assegurar sua continuidade, sustentabilidade, adequação e efetividade.

Art. 23. O descumprimento desta portaria deve ser imediatamente registrado como incidente de segurança e comunicado ao CGD, para apuração e consequente adoção das providências cabíveis, em conjunto com a Assessoria Jurídica, nos termos da Lei e considerando a Política de Segurança da Informação do CFQ.

Art. 24. Esta Portaria entra em vigor nesta data.

Dê-se ciência.
Publique-se.

Brasília, 14 de novembro de 2023.

JOSÉ DE RIBAMAR OLIVEIRA FILHO
Presidente