
RESOLUÇÃO CRCRJ N.º 600, DE 12 DE SETEMBRO DE 2022.

Institui a Política de Segurança da Informação para Aquisição, Desenvolvimento e Manutenção de Sistemas da Informação.

O CONSELHO REGIONAL DE CONTABILIDADE DO RIO DE JANEIRO, no uso de suas atribuições legais e regimentais, resolve:

CAPÍTULO I
DA INSTITUIÇÃO, OBJETIVO E APLICAÇÃO

Art. 1º Fica instituída a Política de Segurança da Informação para Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação no âmbito do Conselho Regional de Contabilidade do Rio de Janeiro.

Art. 2º Esta política de segurança norteia o processo de aquisição, desenvolvimento e manutenção de sistemas de informação para assegurar a disponibilidade, continuidade, confidencialidade e integridade dos serviços prestados por estes sistemas, visando reduzir os riscos institucionais.

Art. 3º A política deve ser observada na contratação ou implementação de soluções de TI que envolvam o desenvolvimento, a manutenção ou a aquisição de sistemas, independentemente de quem os tenha desenvolvido ou adaptado e são aplicáveis, no que couber, àqueles disponíveis no mercado para aquisição e aos sistemas em produção pelo CRCRJ.

Art. 4º Esta norma se aplica a todos os conselheiros, empregados, assessores, estagiários e aprendizes do CRCRJ ou indivíduos que, direta ou indiretamente, utilizam ou suportam os sistemas, infraestrutura ou informações do CRCRJ e, especialmente, destina-se aos responsáveis da área de TI envolvidos pelo processo de aquisição, desenvolvimento e manutenção dos sistemas de informação.

Art. 5º A elaboração e atualização deste documento é de responsabilidade do Comitê de Segurança da Informação.

CAPÍTULO II
DOS TERMOS E DEFINIÇÕES

Art. 6º Para os efeitos desta política, são estabelecidos os seguintes conceitos e definições:

I - ambiente de desenvolvimento: espaço com acesso controlado contendo os itens de configuração em desenvolvimento, operação, processamento, geração e armazenamento de dados, onde os usuários desenvolvedores farão as publicações e testes no decorrer do processo de construção dos softwares;

II - ambiente de homologação: espaço com acesso controlado contendo os itens de configuração em homologação, operação, processamento, geração e armazenamento de dados, onde os usuários e gestores donos do produto farão as homologações e aceites antes da publicação dos softwares em produção;

III - ambiente de produção: espaço com acesso controlado contendo os itens de configuração em produção, operação, processamento, geração e armazenamento de dados, onde os usuários finais acessarão o software;

IV - ambiente de versão: sistemas de controle de fontes que possibilitam rastrear e gerenciar as alterações em códigos e em documentação de software. Espaço com acesso controlado, contendo os códigos fontes e as documentações dos artefatos de softwares entregues ao CRCRJ ou desenvolvidos pelas equipes internas;

V - ameaça: qualquer circunstância ou evento com o potencial de causar impacto negativo sobre a confidencialidade, integridade, autenticidade e disponibilidade da informação;

VI - análise de risco: uso sistemático de informações de identificação de fontes para estimar o risco;

VII - análise dinâmica: tipo de teste que verifica o comportamento externo do software em busca de anomalias ou vulnerabilidades. A análise dinâmica ocorre por meio de interações com o software em execução. Um exemplo é o chamado teste de penetração;

VIII - análise estática: tipo de teste de software que verifica sua lógica interna em busca de falhas ou vulnerabilidades. A análise estática ocorre por meio da verificação do código-fonte ou dos binários;

IX - ativos de informação: qualquer dispositivo de software ou hardware que agrega valor ao negócio e compõe a infraestrutura de rede de dados do CRCRJ, assim como também os locais onde se encontram estes dispositivos, gestão do pessoal que a eles possuem acesso, além dos processos envolvidos na gestão e operacionalização dos ativos de informação;

X - avaliação de conformidade em segurança da informação: exame sistemático do grau de atendimento dos requisitos relativos à segurança da informação com as legislações específicas;

XI - avaliação de riscos: processo para comparar o risco estimado com critérios predefinidos para determinar a importância do risco;

XII - base de dados: conjunto de dados interrelacionados, organizados de forma a permitir a recuperação da informação. Tem como objetivo fornecer a informação atualizada, precisa e confiável;

XIII - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;

XIV - controles de segurança: medidas adotadas para evitar ou diminuir a probabilidade de exploração de uma vulnerabilidade. Exemplos de controles de segurança são: a criptografia, as funções de **hash**, a validação de entrada, o balanceamento de carga, as trilhas de auditoria, o controle de acesso, a expiração de sessão, os **backups** e etc;

XV - criptografia: arte e ciência de esconder o significado de uma informação de receptores não desejados;

XVI - criticidade: é o nível de dependência da instituição em relação ao ativo, caso ela precise dele durante uma crise. A criticidade está diretamente relacionada ao tempo máximo aceitável da paralisação de um serviço ou processo associado às atividades finalísticas do CRCRJ e pontua o quanto essa paralisação será crítica para a instituição;

XVII - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por um usuário autorizado;

XVIII - integridade: propriedade de que a informação não foi modificada ou destruída, de maneira não autorizada ou acidental, por indivíduos, entidades ou processos;

XIX - modelo positivo de segurança: modelo no qual se define o que é permitido explicitamente, rejeitando o restante;

XX - recuperação segura em caso de falha: modelo no qual a falha no processamento de um controle de segurança resulte no mesmo caminho que seria executado no caso de uma vedação emitida por tal controle;

XXI - requisitos de segurança: conjunto de necessidades de segurança que o sistema deve atender, sendo tais necessidades influenciadas fortemente pela política de segurança do CRCRJ, compreendendo aspectos funcionais, não funcionais e legais. Os aspectos funcionais descrevem comportamentos que viabilizam a criação ou a manutenção da segurança e, geralmente, podem ser testados diretamente. Na maioria dos casos, remetem a mecanismos de segurança como, por exemplo, controle de acesso baseado em papéis de usuários como administradores ou usuários comuns; autenticação com o uso de credenciais como usuário e senha ou certificados digitais. Os aspectos não funcionais descrevem procedimentos necessários para que o sistema permaneça executando as funções adequadamente mesmo quando sob uso indevido. São exemplos de requisitos não funcionais, dentre outros, a validação das entradas de dados e o registro de *logs* de auditoria com informações suficientes para análise forense;

XXII - riscos de segurança da informação: possibilidade potencial de uma ameaça comprometer a informação ou o sistema de informação pela exploração da vulnerabilidade;

XXIII - segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XXIV - sistema de informação: aplicação da tecnologia da informação que dá apoio às atividades de determinada área de conhecimento, visando otimizar as operações, o gerenciamento e a decisão, trabalhando os dados e transformando-os em informação;

XXV - trilhas de auditoria: são rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria. São entendidas como o conjunto cronológico de registros – *logs* – que proporcionam evidências do funcionamento do sistema. Esses registros podem ser utilizados para reconstruir, revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para avaliar e rastrear o uso do sistema, detectando e identificando usuários não autorizados;

XXVI - vulnerabilidade: fragilidade de um ativo ou grupo de ativos de informação que pode ser explorada negativamente por uma ou mais ameaças; e

XXVII - ACL: Lista de Controle de Acesso, é uma técnica de controle de acesso que permite definir para cada usuário, uma lista de recursos que o mesmo tem acesso.

CAPÍTULO III

DAS DIRETRIZES E PROCEDIMENTOS

Art. 8º Para o desenvolvimento, a manutenção, a aquisição ou o funcionamento de sistemas de informação no Conselho Regional de Contabilidade do Rio de Janeiro, independentemente das metodologias ou das tecnologias utilizadas, devem-se observar as seguintes diretrizes e procedimentos.

I - toda aquisição, desenvolvimento e manutenção de sistemas de informação deve ser submetido a um processo de gestão de configuração e mudança de forma a garantir o controle efetivo de modificações realizadas em ambientes diversos, com o objetivo de registrar, avaliar e autorizar qualquer modificação em sistemas de informação;

II - identificar, definir, validar e documentar, na fase inicial de qualquer demanda, os requisitos de segurança e a disponibilidade a que os sistemas deverão atender;

III - usar modelo positivo de segurança definido no contexto da aplicação e dos ativos envolvidos, baseado na classificação da informação e conhecimentos dos processos institucionais;

IV - implementar controle de acesso baseado em papéis ou perfis de usuários, ou controle via Lista de Controle de Acesso (ACL), preferencialmente por meio de componentes isolados;

V - implementar controles de segurança necessários para proteger os ativos e informações digitais, de acordo com a sua criticidade;

VI - sempre que possível, usar controles de segurança como componentes, de forma que sejam catalogados e reutilizados em outros sistemas. É recomendado que esses componentes sejam baseados nos controles definidos nas NBR ISO/IEC 27001 e 27002;

VII - implementar os controles de segurança em múltiplas camadas da arquitetura do sistema, de acordo com a criticidade das informações tratadas;

VIII - implementar a obrigatoriedade de realização de testes para minimizar os erros e, possivelmente a automatização de entrega de publicação de sistemas desenvolvidos;

IX - o backup relacionado aos sistemas de informações, bem como sua frequência e retenção, deve ser definido, conforme o nível de confiabilidade em que foram classificados na Política de Backup;

X - desenvolver ou adquirir sistemas de forma que suas mensagens de erro não revelem detalhes de sua estrutura interna ou a configuração do ambiente;

XI - verificar o atendimento dos requisitos de segurança do **software**, por meio de análise estática e/ou análise dinâmica, preferencialmente na fase de construção;

XII - identificar e corrigir as vulnerabilidades encontradas anteriormente à entrada de qualquer sistema em produção, segundo o critério de prioridade e de aceitação do risco;

XIII - investigar e tratar de forma contínua as vulnerabilidades técnicas dos sistemas de informações em uso;

XIV - a base de dados do ambiente de testes deve ser especificamente para testes, assim como o ambiente de homologação deve ser utilizado especificamente para homologação do sistema e/ou requisitos com o usuário requisitante/final;

XV - remover arquivos desnecessários para o funcionamento do sistema e contas criadas para testes, quando da passagem para o ambiente de produção;

XVI - evitar a implementação de parâmetros de configuração dentro do código-fonte;

XVII - usar arquivos externos de configuração, adequadamente protegidos contra acesso e alteração indevidos;

XVIII - utilizar o princípio do mínimo privilégio, que consiste na estratégia de segurança baseada na ideia de conceder autorizações apenas quando realmente for necessária para o desempenho de uma atividade específica, observada a legislação pertinente;

XIX - recuperar de modo seguro em caso de falha;

XX - registrar em *logs* todos os eventos relevantes para a instituição e para a segurança da informação, com o armazenamento de informações suficientes para investigação e análise forense:

a) os **logs** que permitam a construção de uma trilha de auditoria deverão ser protegidos de forma consistente com o contexto da aplicação e dos processos institucionais envolvidos.

XXI - utilizar controles de segurança da informação específicos para os sistemas, independentemente de quaisquer proteções utilizadas na infraestrutura subjacente;

XXII - as bases e massas de dados utilizadas para teste e validação de sistemas devem ser anonimizadas caso contenham dados classificados como sigilosos, conforme a legislação;

XXIII - não permitir acesso ao ambiente de produção por pessoal estranho às Unidades Organizacionais envolvidas na manutenção de infraestrutura, salvo em situações devidamente justificadas e documentadas e com acompanhamento contínuo e presencial;

XXIV - observar que, em caso de contratação de serviço para desenvolvimento ou manutenção de **software**, o código-fonte deve ser custodiado de modo seguro pela empresa contratada e o CRCRJ;

XXV - para que um sistema de informação seja utilizado no CRCRJ, quando não produzido pelo próprio Conselho, os requisitos e contratos de licenciamento devem ser controlados, indicando o proprietário da aplicação e a forma adequada de uso, em concordância com a lei de direitos autorais, bem como o tempo de vigência do contrato;

XXVI - definir as regras para transferência do conhecimento sobre o **software** desenvolvido de modo a permitir a sua manutenção, de forma independente, por parte dos demais Conselhos;

XXVII - estabelecer acordos de licenciamento, propriedade dos códigos e direitos de propriedade intelectual condizentes com o interesse do CRCRJ, de forma a adquirir a titularidade do **software** ou para apenas exercer o direito de uso;

XXVIII - instaurar meios que visem o controle da qualidade e precisão do trabalho efetuado de forma a garantir que os requisitos de segurança sejam atendidos;

XXIX - sistemas que possuam a necessidade de controle de acesso ou lidem com dados sigilosos devem utilizar criptografia para a transmissão de dados e armazenamento em bancos de dados;

XXX - definir a execução de testes pela contratada e homologação pelo CRCRJ, antes da instalação do **software** obtido no ambiente de produção:

XXXI - realizar a análise estática e a análise dinâmica do **software** desenvolvido por terceiros.

XXXII - definir regras, estabelecer responsabilidades e procedimentos operacionais quanto à liberação de acesso aos recursos tecnológicos e ao ambiente físico ou lógico do CRCRJ;

XXXIII - o suporte dos sistemas somente deve ser realizado após abertura de chamado pelo usuário;

XXXIV - na fase do ciclo de vida do sistema, em que são levantados os requisitos, as necessidades, o estabelecimento de relação com as atividades institucionais ou o levantamento de custos, devem ser desenvolvidas as seguintes ações de segurança:

a) avaliar, preliminarmente, os impactos e categorização do sistema conforme a tabela do inciso XXXVIII; e

b) definir os requisitos de segurança.

XXXV - na fase do ciclo de vida do sistema, em que são especificados e analisados os requisitos, o custo/benefício ou elaborado o plano de gerenciamento de riscos, devem ser desenvolvidas as seguintes ações de segurança:

a) analisar os riscos; e

b) definir os controles de segurança da informação que serão implementados.

XXXVI - na fase do ciclo de vida, em que o sistema é construído, devem ser desenvolvidas as seguintes ações de segurança:

- a) desenvolver e testar os controles de segurança da informação;
- b) implementar controles de versão para garantir a gestão dos código-fonte;
- c) realizar procedimentos de verificação de funcionamento na infraestrutura de desenvolvimento após atualizações ou substituições de sistemas.

XXXVII - na fase do ciclo de vida, em que o sistema é implantado, deve ser desenvolvida a seguinte ação de segurança:

- a) monitorar e avaliar a segurança da informação, podendo utilizar a norma ISO/IEC 15408-3:2008 como referência.

XXXVIII - na fase de manutenção do sistema, deve ser desenvolvida a seguinte ação de segurança:

- a) Gerenciar e revalidar os controles de segurança da informação.

XXXIX - a avaliação de impacto potencial pode ser realizada com base na tabela do FIPS 199 (NIST):

| OBJETIVO DA SEGURANÇA | IMPACTO POTENCIAL | | |
|---|---|--|--|
| | BAIXO | MÉDIO | ALTO |
| Confidencialidade Restrições quanto ao acesso e à divulgação das informações, incluindo meios de proteger informações de privacidade e direitos de propriedade pessoais. | A divulgação não autorizada da informação <u>pode causar efeitos prejudiciais limitados</u> nas operações e nos ativos institucionais ou individuais. | A divulgação não autorizada da informação <u>pode causar sérios efeitos</u> prejudiciais nas operações e nos ativos institucionais ou individuais. | A divulgação não autorizada da informação <u>pode causar efeitos prejudiciais severos ou catastróficos</u> nas operações e nos ativos institucionais ou individuais. |
| Integridade Proteção contra modificação ou destruição indevida das informações. | A modificação ou a destruição não autorizada da informação <u>pode causar efeitos prejudiciais limitados</u> nas operações e nos ativos institucionais ou individuais. | A modificação ou a destruição não autorizada da informação <u>pode causar sérios efeitos</u> prejudiciais nas operações e nos ativos institucionais ou individuais. | A modificação ou a destruição não autorizada da informação <u>pode causar efeitos prejudiciais severos ou catastróficos</u> nas operações e nos ativos institucionais ou individuais. |
| Disponibilidade Garantia de uso e de acesso confiável e em tempo à informação. | A interrupção do uso ou acesso à informação ou a um sistema <u>pode causar efeitos prejudiciais limitados</u> nas operações e nos ativos institucionais ou individuais. | A interrupção do uso ou acesso à informação ou a um sistema <u>pode causar sérios efeitos</u> prejudiciais nas operações e nos ativos institucionais ou individuais. | A interrupção do uso ou acesso à informação ou a um sistema <u>pode causar efeitos prejudiciais severos ou catastróficos</u> nas operações e nos ativos institucionais ou individuais. |

CAPÍTULO IV DAS RESPONSABILIDADES

Art. 9º Os envolvidos no processo de desenvolvimento, manutenção e aquisição de sistemas no CRCRJ devem receber treinamento em segurança de *software*.

Parágrafo único: Todos os usuários, ao utilizar um novo sistema ou nova versão, devem ser treinados e capacitados para a sua efetiva utilização.

Art. 10. O cumprimento desta política deve ser observado quando da elaboração dos processos de contratações de desenvolvimento, manutenção ou aquisição de sistemas, devendo a obrigação estar inserida nos respectivos Estudos Técnicos Preliminares, Termos de Referência ou Projetos Básicos e contratos.

Art. 11. O Departamento de Tecnologia da Informação (DEPTI) deve supervisionar o processo desde o seu planejamento de aquisição, desenvolvimento, manutenção ou implementação, no caso de desenvolvimento de sistemas/softwarewares por terceiros.

Art. 12. O DEPTI ou a Comitê de Tecnologia da Informação do CRCRJ pode estabelecer outros procedimentos com o objetivo de complementar o definido nesta política.

Art. 13. Os usuários da rede interna do CRCRJ devem reportar ao DEPTI as ocorrências de incidentes que afetem os ativos de informação ou descumprimento dessa norma tão logo tomem ciência do ocorrido, preferencialmente por meio de chamado na intranet (Requisição de Suporte DEPTI).

Art. 14. Na ocorrência de quebra de segurança por meio de recursos computacionais, o DEPTI deve ser imediatamente informado para adotar as providências necessárias, limitando o acesso às informações e/ou recursos computacionais do CRCRJ, se necessário.

CONTADOR SAMIR FERREIRA BARBOSA NEHME
Presidente

Aprovada na 1.156ª Reunião Plenária de 2022, realizada em 12 de setembro de 2022.

Publicada no DOERJ em 15 de setembro de 2022