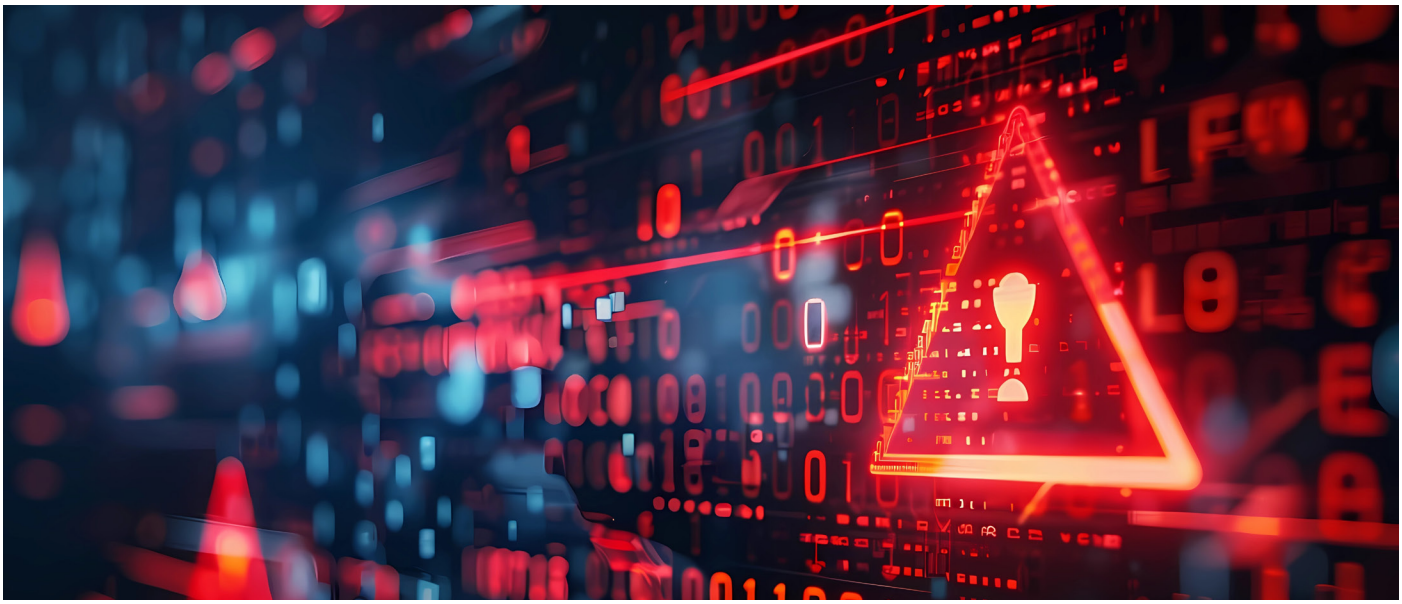

CYBER
ACADEMY
FEBRABAN

MÓDULO 5

Avaliação de Riscos de Segurança



Gerenciamento de Riscos segundo a ISO 27005

Gerenciamento de riscos é o processo de planejar, organizar, conduzir e controlar as atividades de uma organização visando minimizar os efeitos do risco sobre o capital e o lucro de uma organização.

Riscos podem surgir da incerteza do mercado financeiro, de falhas de projeto, de responsabilidades legais, de risco de crédito, de acidentes, de causas naturais e desastres, bem como de ataques deliberados de adversários. Diversos padrões de gerenciamento de riscos foram desenvolvidos, incluindo os do Project Management Institute (PMI), National Institute of Science and Technology (NIST) e padrões ISO. Métodos, definições e objetivos variam muito. Por exemplo: se o método de gerência de riscos se encontra no contexto da gerência de projetos, segurança, engenharia, processos industriais, carteiras financeiras, avaliações atuariais ou segurança e saúde pública.

A estratégia de risco pode incluir transferir o risco para outra parte, evitar o risco, reduzir o efeito negativo do risco e aceitar algumas ou todas as consequências de um risco em particular.

Gerenciamento de riscos é um processo contínuo que se aplica a todos os aspectos dos processos operacionais. Em grandes organizações, a tarefa de monitorar esse processo é conduzida por um especialista em segurança da informação, tal como um encarregado de segurança da informação (Information Security Officer) ou chefe de segurança da informação (Chief Information Security Officer – CISO), que é designado especialmente para essa função e responsável pelo mais alto nível de gestão.

Requisitos de segurança da informação

É essencial que uma organização identifique seus requisitos de segurança. Existem 03 principais fontes de requisitos de segurança:

a) A avaliação dos riscos à organização, levando em conta a estratégia e os objetivos globais de negócio da organização. Por meio de uma avaliação do risco, as ameaças aos ativos são identificadas, a vulnerabilidade e a probabilidade de ocorrência são avaliadas e o potencial impacto é estimado.
b) Os requisitos legais, determinados por estatutos, regulamentos e contratos que uma organização, seus parceiros comerciais, contratantes e provedores de serviço têm que satisfazer, e seu ambiente sociocultural.
c) O conjunto de princípios, objetivos e requisitos de negócio para o manuseio, processamento, armazenamento, comunicação e arquivamento da informação que uma organização desenvolveu para apoiar suas operações.

Os recursos empregados na implementação de controles precisam ser equilibrados de acordo com os prejuízos de negócio que podem resultar de problemas de segurança na ausência de tais controles. O resultado da avaliação do risco irá ajudar a guiar e a determinar as ações de gestão adequadas e as prioridades para gerir os riscos da segurança da informação e a implementar os controles selecionados para proteger contra esses riscos.

A ISO/IEC 27005:2011 fornece orientações para a gestão de riscos de segurança da informação, incluindo recomendações sobre avaliação do risco, tratamento do risco, aceitação do risco, comunicação do risco, monitoramento do risco e revisão do risco.

Avaliação do Risco

O capítulo 4 da ISO 27002:2005 foi dedicado inteiramente à avaliação do risco e ao tratamento do risco. Na ISO 27002:2013, a avaliação do risco e o tratamento do risco não são mais especificamente mencionados. Esses conceitos são parte da abordagem completa do gerenciamento de riscos. O capítulo 6 da ISO 27002:2013, especialmente a seção 6.1.5, segurança da informação na gerência de projetos, afirma que os objetivos da segurança da informação estão incluídos nos objetivos do projeto. Uma avaliação do risco da segurança da informação é conduzida nas primeiras etapas do projeto para identificar os controles necessários, enquanto a segurança da informação é parte de todas as fases da metodologia de projeto aplicada.

Entretanto, é muito importante que a segurança da informação inicie bem no começo da fase de delineamento de qualquer projeto, a fim de alcançar a segurança pela concepção. Além disso, a avaliação do risco não deve ser limitada apenas a projetos. Em um mundo ideal, a segurança da informação é parte das operações diárias. Todos os funcionários estão cientes da segurança e reconhecem as falhas de segurança. A segurança da informação é implementada em todos os sistemas e um alto nível de maturidade é alcançado. Avaliações do risco devem identificar, quantificar e priorizar os riscos segundo critérios de aceitação do risco e objetivos que são relevantes para a organização. Os resultados devem guiar e determinar as prioridades e ações de gerência adequadas para gerir os riscos de segurança da informação e implementar os

controles selecionados para proteger contra esses riscos.

O processo de avaliação de riscos e seleção de controles pode ter de ser realizado um certo número de vezes para cobrir diferentes partes da organização ou sistemas de informação individuais. A avaliação do risco deve incluir uma abordagem sistemática para estimar a magnitude dos riscos (análise do risco) e o processo de comparar o risco estimado em relação a um critério a fim de determinar a importância do risco (estimativa do risco).

As avaliações do risco também devem ser analisadas periodicamente para tratar de mudanças nos requisitos de segurança e nas situações de risco, por exemplo, em ativos, ameaças, vulnerabilidades, impactos, estimativa do risco e quando ocorrerem mudanças significativas. Essas avaliações do risco devem ser realizadas de maneira metódica, capaz de produzir resultados comparáveis e reprodutíveis. A avaliação do risco da segurança da informação deve ter um âmbito claramente definido, a fim de ser eficaz, e deve incluir as relações com as avaliações de risco de outras áreas, se for o caso.

O âmbito de uma avaliação do risco pode ser toda a organização, partes da organização, um sistema de informação individual, componentes específicos do sistema ou serviços onde isso for viável, realista e útil.

Referências Bibliográficas:

Capeletti, Lucas. Fundamentos de Gestão de Acesso e Identidade (IAM) (Portuguese Edition).
Lisboa Melo, Jefferson; Vieira de Oliveira, Alexandre; Mauser, Daniel. Do Iniciante ao Profissional em Segurança Cibernética. SF Editorial e AcademiaTI.
Fernandes, Victor. Inteligência Artificial para Leigos (Portuguese Edition).
Wendt, Emerson; Jorge, Higor Vinicius Nogueira. Crimes Cibernéticos 3a edição: Ameaças e procedimentos de investigação (Portuguese Edition). BRASPORT.
Baars, Hans; Hintzbergen, Kees; Hintzbergen, Jule; Smulders, André. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002 (Portuguese Edition). BRASPORT.
R., Raphael. Segurança Cibernética: Protegendo Infraestruturas e Dados (Portuguese Edition).

CYBER
ACADEMY

FEBRABAN