QUESTIONÁRIO DE FIXAÇÃO 02

Responder individualmente e enviar para o email joao.gress@iesgo.edu.br até 17AGO25, 2359h.

O não envio acarretará em penalizações de pontuação para a equipe dos integrantes.

QUESTÃO 01

A gestão de riscos em segurança da informação é um processo contínuo que envolve identificar, analisar, avaliar e tratar riscos que possam comprometer a confidencialidade, integridade e disponibilidade dos ativos de informação.
Normas como a ISO 31000 e a ISO 27005 estabelecem diretrizes para que organizações desenvolvam metodologias estruturadas, baseadas na probabilidade de ocorrência e no impacto potencial de eventos adversos. A correta aplicação dessas práticas permite priorizar recursos, prevenir incidentes e manter a resiliência operacional, integrando-se a políticas corporativas, planos de continuidade e estratégias de segurança.
Entretanto, a eficácia da gestão de riscos depende não apenas da implementação de controles, mas também de uma cultura organizacional que compreenda, aceite e atue sobre o conceito de risco, promovendo comunicação e monitoramento constantes.

Questão:
Considerando o texto-base e o conhecimento sobre gestão de riscos em segurança da informação, discorra sobre a importância da integração entre metodologias normativas e cultura organizacional para a eficácia do processo. Em sua resposta, aborde: (i) como a aplicação estruturada de normas contribui para a identificação e tratamento de riscos; (ii) de que forma a cultura organizacional influencia a percepção e o gerenciamento de riscos; e (iii) por que o monitoramento contínuo e a comunicação

eficaz são elementos essenciais para a resiliência em segurança da informação.

(Limite: 20 linhas – Valor: 10,0 pontos)

As normas (como ISO) fornecem a base técnica (matrizes, processos) para gerenciar riscos.

A cultura determina se os colaboradores seguem essas práticas no dia a dia.

á o monitoramento corrige falhas e adapta controles, fechando o ciclo da melhoria contínua.

Sem cultura, normas viram "papel"; sem monitoramento, riscos evoluem sem resposta.

Normas dao "como fazer"

cultura define " fazer acontecer "

e o monitoramento garante melhoria contínua.

Metodologias normativas = Fornece um caminho de como tratar os erros e risco, ela usa tambem matriz (prob/impact)

A cultura organizacional = define o que o colaborador ou participante da equipe deve agir frente a esses riscos

monitoramento e comunicação = garante que aqueles riscos sejam revisados por colaboradores e ajustados , mantendo a resiliencia

Questão 02

A gestão de riscos em segurança da informação consiste em um conjunto de processos sistemáticos para identificar, analisar, avaliar e tratar riscos que possam comprometer ativos críticos da organização. Normas como a ISO
31000 e a ISO 27005 fornecem diretrizes para estruturar essa prática, utilizando escalas de probabilidade e impacto para priorização e tomada

de decisão. Entretanto, a eficácia do processo depende também de fatores humanos, como a cultura organizacional, a conscientização dos colaboradores e a comunicação interna, que garantem a correta percepção dos riscos e o engajamento na aplicação de medidas preventivas e corretivas.

Questão:
De acordo com as boas práticas de gestão de riscos em segurança da informação, qual das alternativas abaixo apresenta, simultaneamente, um elemento de caráter técnico e um elemento de caráter organizacional essenciais para a eficácia do processo?

B) Aplicação de escalas de probabilidade x impacto e promoção de uma cultura de segurança entre os colaboradores.

Questão 03

Uma empresa de comércio eletrônico decidiu revisar seu processo de gestão de riscos de acordo com as diretrizes da ISO 31000 e ISO 27005. Durante a análise, a equipe de segurança identificou quatro situações envolvendo diferentes estratégias de tratamento de risco.

Situações apresentadas:
I) Implementação de autenticação multifator para reduzir a probabilidade de acesso não autorizado.
II) Contratação de seguro cibernético para cobrir perdas financeiras decorrentes

de incidentes.
III) Decisão de encerrar um serviço online que apresentava alto risco de exploração e custo elevado de mitigação.
IV) Manutenção de um risco classificado como baixo devido ao alto

custo de controles em relação ao impacto esperado.

Associe cada situação à respectiva estratégia de tratamento de risco:

1. Redução
2. Transferência
3. Evitação
4. Aceitação

Em seguida, assinale a alternativa que apresenta a **sequência correta de associação**:

A) I–1 II–2 III–3 IV–4

Questão 04

Uma instituição de ensino superior está revisando seu plano de gestão de riscos para a área de TI, alinhado à ISO 27005. Durante a avaliação, foi identificado que a probabilidade de ocorrer uma invasão ao sistema de matrícula é **média**, mas o impacto potencial sobre as operações e dados de alunos é **crítico**.

No comitê de análise, discutiu-se a relação entre esses dois fatores na classificação do risco e a priorização das ações de tratamento.

I – A classificação de um risco leva em consideração tanto a probabilidade quanto o impacto, permitindo sua priorização na matriz de riscos.
PORQUE
II – Um risco com impacto crítico, independentemente da probabilidade, deve ser tratado como de alta prioridade para mitigação.

C) A asserção I é uma proposição verdadeira, e a II é uma proposição falsa.

Questão 05

O gerenciamento de riscos em segurança da informação visa reduzir a probabilidade e o impacto de eventos adversos que possam comprometer os ativos organizacionais. Entre as estratégias de tratamento de risco, destacam-se a **redução**, a **transferência**, a **aceitação** e a **evitação**. A escolha da estratégia deve considerar critérios como custo-benefício, criticidade do ativo, requisitos legais e impacto no negócio.

Organizações que adotam práticas de gestão de riscos baseadas em normas como a ISO 31000 e ISO 27005 conseguem priorizar ações e implementar controles mais eficazes, aumentando a resiliência e garantindo a continuidade das operações.

Explique, com base nas boas práticas de gestão de riscos, **como uma organização pode aplicar diferentes estratégias de tratamento para mitigar ameaças identificadas**. Em sua resposta, mencione **pelo menos dois tipos de controles aplicáveis (técnico, físico ou administrativo)** e **um exemplo prático de aplicação em ambiente corporativo**.

(Limite: 20 linhas – Valor: 10,0 pontos)

Uma organização aplica estratégias de tratamento de risco conforme impacto e criticidade dos ativos.
A redução usa controles técnicos (firewall, autenticação multifator) ou administrativos (políticas de acesso, treinamentos).
A transferência pode ser feita via seguro cibernético,
a aceitação quando o risco é baixo e o custo de mitigação alto,
e a evitação eliminando atividades de alto risco.
Exemplo prático: usar autenticação multifator e treinamento de conscientização para reduzir ataques de phishing,
protegendo dados e garantindo resiliência operacional.

Questão 06

Uma instituição financeira, após um processo completo de gestão de riscos baseado na ISO 31000 e ISO 27005, implementou um conjunto de controles técnicos, físicos e administrativos para reduzir a probabilidade de ataques cibernéticos a seus sistemas de transações. Entre as medidas aplicadas estavam: autenticação multifator, criptografia de dados em repouso e em trânsito, monitoramento contínuo por SIEM e auditorias internas periódicas.

Mesmo após a adoção dessas medidas, a equipe de segurança identificou que certos cenários de ataque ainda poderiam ocorrer, embora com probabilidade

reduzida, como tentativas sofisticadas de spear phishing direcionadas a executivos e vulnerabilidades zero-day não corrigidas imediatamente. Esse conjunto de riscos que permanece após a aplicação de controles foi registrado no relatório final como parte do processo de gestão.

No comitê de governança, surgiu um debate sobre a natureza desses riscos e sobre como avaliar a real eficácia das medidas adotadas, considerando o custo de implementação, o nível de exposição remanescente e a necessidade de planos de contingência.

Analise as asserções a seguir:

I – O risco residual corresponde ao nível de risco que permanece após a aplicação de medidas de tratamento, devendo ser monitorado e, quando necessário, mitigado com controles adicionais ou planos de contingência.
PORQUE
II – A avaliação da eficácia de controles considera não apenas a redução da probabilidade e do impacto dos riscos, mas também o

custo-benefício das medidas implementadas em relação à exposição residual.

A) As asserções I e II são proposições verdadeiras, e a II é uma justificativa correta da I.

Questão 07

Durante uma atividade em sala de aula sobre gestão de riscos, os alunos receberam quatro situações hipotéticas e deveriam classificá-las de acordo com as estratégias de tratamento: **redução**, **transferência**, **aceitação** e **evitação**.

Situações analisadas:
I) Contratar seguro cibernético para cobrir perdas por incidentes.
II) Encerrar um serviço online inseguro e de alto custo de mitigação.
III) Manter um risco classificado como baixo devido ao custo elevado de controle.

IV) Implementar autenticação multifator para reduzir a probabilidade de acesso não autorizado.

Associe corretamente cada situação à respectiva estratégia de tratamento:

1. Redução
2. Transferência
3. Aceitação
4. Evitação

Assinale a alternativa que apresenta a **sequência correta para I, II, III e IV**:

A) 2 – 4 – 3 – 1

Questão 08

Uma empresa de tecnologia está conduzindo um processo formal de **gestão de riscos** seguindo as diretrizes da ISO 31000 e da ISO 27005. O objetivo é identificar pontos de fragilidade que possam comprometer a segurança dos ativos de informação, considerando as dimensões física, lógica e organizacional.

Durante a fase de identificação de riscos, foram observadas quatro situações reais, ocorrendo de forma rotineira, que podem ser exploradas por agentes maliciosos e gerar impacto significativo nos pilares da segurança da informação (confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade).

A equipe de análise deve identificar **o risco ou vulnerabilidade associado a cada cenário** e **justificar com base nos princípios de gestão de riscos e segurança da informação**, considerando probabilidade, impacto e possíveis estratégias de tratamento.

a) Terceirizados responsáveis pela manutenção de infraestrutura com acesso físico irrestrito a salas de servidores.

a) acesso indevido de uma pessoal mal intencionada , manipulção equipamentos, roubo de dados. | monitoramento com cameras , cadeados , ou chaves de acesso

b) Contas de usuários inativas mantidas no sistema sem exclusão ou bloqueio.

b) contas inativas , podem ser acessadas por pessoas não autorizadas, compromentendo dados pessoais. | adicionar uma politica de desativação automatica , adicionar

uma opção de exclusao de conta para o usuario, adicionar um TTL.

c) Funcionário acessando documentos críticos de um projeto em rede Wi-Fi pública durante viagem de negócios.

c) colocar o roteador em modo promiscuo interceptando dados sensiveis. | usar VPN, nao conectar em redes sem senhas.

d) Uso compartilhado de credenciais administrativas por membros de uma mesma equipe técnica.

d) não tem como descobrir quem vazou a senha | criar usuario , adicionar uma tela de logon para que quem entre seja identificado ,e cada um tenha uma senha diferente

Questão 09

Uma empresa do setor financeiro está revisando seu plano de gestão de riscos em segurança da informação. Após identificar ameaças e vulnerabilidades críticas, a equipe de segurança classificou cada cenário de acordo com a estratégia de tratamento mais adequada: **redução (mitigação)**, **transferência**, **aceitação** e **evitação**.

A análise correta dessas situações é fundamental para que a organização direcione recursos de forma eficiente e mantenha sua resiliência operacional.

Com base nas situações descritas a seguir, identifique a **estratégia de tratamento de risco** mais adequada para cada caso:

I) Implementação de firewall de próxima geração e segmentação de rede para diminuir a superfície de ataque.
II) Contratação de apólice de seguro cibernético para cobertura de perdas financeiras decorrentes de ataques.
III) Decisão de não realizar uma campanha online devido a riscos de

vazamento de dados que seriam onerosos para mitigar.

IV) Manutenção de um risco classificado como baixo, pois o custo de controles excede o impacto potencial.

V) Uso de autenticação multifator para reduzir a probabilidade de acesso não autorizado a contas críticas.

Assinale a alternativa que apresenta a **associação correta entre as situações**
I a V e as estratégias de tratamento de risco a seguir:

1. Redução (Mitigação)
2. Transferência
3. Aceitação
4. Evitação

A) I–1, II–2, III–4, IV–3, V–1

Questão 10

A gestão de riscos em segurança da informação envolve a identificação, análise, avaliação e tratamento de riscos que possam comprometer a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade dos ativos organizacionais. A **matriz de riscos** é uma ferramenta essencial nesse processo, permitindo cruzar a probabilidade de ocorrência de um evento com o impacto potencial, facilitando a priorização das ações de mitigação.

Normas como a ABNT NBR ISO/IEC 27005 fornecem diretrizes para o uso da matriz de riscos, descrevendo metodologias para estimativa, categorização e decisão sobre o tratamento adequado. O correto entendimento de como utilizar essa ferramenta é fundamental para que as organizações otimizem recursos e mantenham a resiliência

operacional.

Considerando o uso da matriz de riscos e sua aplicação na gestão de segurança da informação, assinale a alternativa que apresenta corretamente os conceitos e aplicações relacionados:

B) A matriz de riscos cruza probabilidade e impacto, permitindo classificar riscos em níveis como baixo, médio e alto para orientar decisões de tratamento.