Segurança da Informação 2020
CESPE - Miscelânea

Prof. Walter Cunha

falecomigo@waltercunha.com

[Professor] – WALTER CUNHA

Outros Cursos no Provas de TI:
http://bit.ly/2RsnuhF

Canal do Telegram:
https://t.me/patreontimasters

Outros:
https://linktr.ee/waltercunha

[Questão 01]

(CESPE/TJPA 2020) O efeito da incerteza sobre os objetivos consiste em

A ameaça.
B vulnerabilidade.
C consequência.
D risco.
E probabilidade.

[Questão 01] – Comentários

ISO 31000

Risco ***é o efeito da incerteza nos objetivos.***

2.18 consequência resultado de um evento (2.17) que afeta os objetivos.

2.19 probabilidade (likelihood) chance de algo acontecer.

Vulnerabilidade – fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

Ameaça – causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

[Questão 01]

(CESPE/TJPA 2020) O efeito da incerteza sobre os objetivos consiste em

A ameaça.
B vulnerabilidade.
C consequência.
D risco.
E probabilidade.

GabOf. D

[Questão 02]

(CESPE/ME 2020) Risco é o efeito da incerteza nos objetivos, sendo normalmente expresso em termos de fontes de risco, eventos potenciais, suas consequências e suas probabilidades.

[Questão 02] – Comentários

ISO 31000

Fonte de Risco é um "elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco (Nota: uma fonte de risco pode ser tangível ou intangível)".

Oportunidades, Ameaças e Perigos são Fontes de Risco, ou ainda: Oportunidade = Fonte de Ganhos; Ameaça = Fonte de Perdas; Perigo = Fonte de Danos.

Lembre-se sempre da relação:
Causa (Fonte de Risco) >> Fato (Evento) >> Efeito (Consequência).

https://iso31000.net

[Questão 02]

(CESPE/ME 2020) ***Risco é o efeito da incerteza nos objetivos, sendo normalmente expresso em termos de fontes de risco, eventos potenciais, suas consequências e suas probabilidades.***

CERTA

[Questão 03]

(CESPE/ME 2020) Um dos princípios de dados abertos é o acesso não discriminatório, ou seja, os dados estão disponíveis independentemente de identificação ou registro do usuário.

[Questão 03] – Comentários

Em 2007, um grupo de trabalho de 30 pessoas reuniu-se na Califórnia, Estados Unidos da América, para definir os princípios dos Dados Abertos Governamentais. Chegaram num consenso sobre os seguintes **8 princípios**:

Completos. Todos os dados públicos são disponibilizados. Dados são informações eletronicamente gravadas, incluindo, mas não se limitando a, documentos, bancos de dados, transcrições e gravações audiovisuais. Dados públicos são dados que não estão sujeitos a limitações válidas de privacidade, segurança ou controle de acesso, reguladas por estatutos.

Primários. Os dados são publicados na forma coletada na fonte, com a mais fina granularidade possível, e não de forma agregada ou transformada.

Atuais. Os dados são disponibilizados o quão rapidamente seja necessário para preservar o seu valor.

Acessíveis. Os dados são disponibilizados para o público mais amplo possível e para os propósitos mais variados possíveis. (...)

[Questão 03] – Comentários

Em 2007, um grupo de trabalho de 30 pessoas reuniu-se na Califórnia, Estados Unidos da América, para definir os princípios dos Dados Abertos Governamentais. Chegaram num consenso sobre os seguintes **8 princípios**:

(...)

Processáveis por máquina. Os dados são razoavelmente estruturados para possibilitar o seu processamento automatizado.

Acesso não discriminatório. Os dados estão disponíveis a todos, sem que seja necessária identificação ou registro.

Formatos não proprietários. Os dados estão disponíveis em um formato sobre o qual nenhum ente tenha controle exclusivo.

Licenças livres. Os dados não estão sujeitos a restrições por regulações de direitos autorais, marcas, patentes ou segredo industrial. Restrições razoáveis de privacidade, segurança e controle de acesso podem ser permitidas na forma regulada por estatutos.

[Questão 03]

(CESPE/ME 2020) ***Um dos princípios de dados abertos é o acesso não discriminatório, ou seja, os dados estão disponíveis independentemente de identificação ou registro do usuário.***

CERTA

[Questão 04]

(CESPE/ME 2020) Com relação às políticas de auditoria na gestão de segurança da informação, julgue o item seguinte, com base no Decreto n.º 9.637/2018.

O referido decreto estabelece que qualquer auditoria de segurança da informação deve ser autorizada pelo gestor de tecnologia da informação do órgão.

[Questão 04] – Comentários

Decreto n.º 9.637/2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação

Art. 15. Aos órgãos e às entidades da administração pública federal, em seu âmbito de atuação, compete:
(...)
IX - consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão de segurança da informação;

[Questão 04]

(CESPE/ME 2020) Com relação às políticas de auditoria na gestão de segurança da informação, julgue o item seguinte, com base no Decreto n.º 9.637/2018.

O referido decreto estabelece que qualquer auditoria de segurança da informação deve ser autorizada pelo gestor de tecnologia da informação do órgão.

ERRADA

[Questão 05]

(CESPE/ME 2020) Com relação às políticas de auditoria na gestão de segurança da informação, julgue o item seguinte, com base no Decreto n.º 9.637/2018.

Cabe aos órgãos e às entidades da administração pública federal, em seu âmbito de atuação, analisar os resultados dos trabalhos de auditoria sobre a gestão de segurança da informação.

[Questão 05] – Comentários

Decreto n.º 9.637/2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação.

Art. 15. Aos órgãos e às entidades da administração pública federal, em seu âmbito de atuação, compete:
(...)
IX - consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão de segurança da informação; e

X - aplicar as ações corretivas e disciplinares cabíveis nos casos de violação da segurança da informação.

[Questão 05]

(CESPE/ME 2020) Com relação às políticas de auditoria na gestão de segurança da informação, julgue o item seguinte, com base no Decreto n.º 9.637/2018.

Cabe aos órgãos e às entidades da administração pública federal, em seu âmbito de atuação, analisar os resultados dos trabalhos de auditoria sobre a gestão de segurança da informação.

CERTA

[Questão 06]

(CESPE/ME 2020) Em organizações públicas e privadas, o plano de continuidade de negócio deve garantir a segurança e a integridade dos dados armazenados.

[Questão 06] – Comentários

PCN

O propósito de um plano de continuidade de negócios, é permitir que uma organização recupere ou mantenha suas atividades em caso de uma interrupção das operações normais de negócios. Os PCN são ativados para dar suporte às atividades críticas necessárias para cumprir os objetivos da organização.

[Questão 06]

(CESPE/ME 2020) ***Em organizações públicas e privadas, o plano de continuidade de negócio deve garantir a segurança e a integridade dos dados armazenados.***

CERTA

[Questão 07]

(CESPE/TJPA 2020) A respeito das políticas de segurança da informação nas organizações, julgue os itens a seguir.

I Essas políticas provêm fundamentos conceituais para a construção de uma infraestrutura de segurança da informação nas organizações.
II Devem-se evitar, nas políticas de segurança, definições de papéis internos à organização ou de diretrizes de acessos a recursos, em razão do nível de detalhamento exigido nessas definições.
III Uma política de segurança da informação deve identificar realisticamente os recursos informacionais, as atividades e operações críticas da organização, além de apoiar a gestão da segurança da informação.
IV A definição da política de segurança da informação deve contemplar requisitos oriundos de ameaças identificadas para a segurança da informação da organização, atuais e futuras.

Estão certos apenas os itens
A I e II. B I e III. C II e IV D I, III e IV. E II, III e IV.

[Questão 07] – Comentários

ISO27002:2013

6 Organização da segurança da informação

6.1 Organização interna

Objetivo: Estabelecer uma estrutura de gerenciamento, para iniciar e controlar a implementação da segurança da informação dentro da organização.

6.1.1 Responsabilidades e papéis pela segurança da informação

[Questão 07]

(CESPE/TJPA 2020) A respeito das políticas de segurança da informação nas organizações, julgue os itens a seguir.

I Essas políticas provêm fundamentos conceituais para a construção de uma infraestrutura de segurança da informação nas organizações.

II ***Devem-se evitar***, nas políticas de segurança, definições de papéis internos à organização ou de diretrizes de acessos a recursos, em razão do nível de detalhamento exigido nessas definições.

III Uma política de segurança da informação deve identificar realisticamente os recursos informacionais, as atividades e operações críticas da organização, além de apoiar a gestão da segurança da informação.

IV A definição da política de segurança da informação deve contemplar requisitos oriundos de ameaças identificadas para a segurança da informação da organização, atuais e futuras.

Estão certos apenas os itens

A I e II. B I e III. C II e IV ***D I, III e IV.*** E II, III e IV.

[Questão 08]

(CESPE/TJPA 2020) Em relação aos conceitos, processos e metodologias utilizadas na gestão de risco, é correto afirmar que, para o cálculo de risco de

A interrupção de energia de um datacenter, é indicada a análise quantitativa, que utiliza uma escala de valores baseados em séries históricas.

B interrupção de energia de um datacenter, é indicada a análise qualitativa, que utiliza uma escala de valores baseados em séries históricas.

C ataque cibernético, é indicada a análise quantitativa, que utiliza uma escala de valores baseados em opiniões subjetivas das partes interessadas.

D ataque cibernético, é indicada a análise qualitativa, que utiliza uma escala de valores baseados em séries históricas.

E ataque cibernético, é indicada a análise qualitativa, que utiliza uma escala de valores baseados em opiniões subjetivas das partes interessadas e em séries históricas.

[Questão 08]

(CESPE/TJPA 2020) Em relação aos conceitos, processos e metodologias utilizadas na gestão de risco, é correto afirmar que, para o cálculo de risco de

A interrupção de energia de um datacenter, é indicada a análise quantitativa, que utiliza uma escala de valores baseados em séries históricas.

B interrupção de energia de um datacenter, é indicada a análise qualitativa, que utiliza uma escala de valores baseados em séries históricas.

C ataque cibernético, é indicada a análise quantitativa, que utiliza uma escala de valores baseados em opiniões subjetivas das partes interessadas.

D ataque cibernético, é indicada a análise qualitativa, que utiliza uma escala de valores baseados em séries históricas.

E ataque cibernético, é indicada a análise qualitativa, que utiliza uma escala de valores baseados em opiniões subjetivas das partes interessadas e em séries históricas.

[Questão 09]

Determinado tribunal atende atualmente 325 estruturas judiciárias, entre as quais, 112 comarcas, promovendo acesso aos sistemas judiciários e salvaguarda dos processos digitais. Em razão da importância regional do tribunal, foi implantada uma gestão de risco institucional, com o objetivo de identificação, mensuração e tratamento do risco, com intuito de atender a população de forma ininterrupta. Alinhado com o processo de risco, foi disparado o processo de continuidade de negócio, tendo ficado a cargo do gestor da área de tecnologia da informação e comunicações (TIC) o plano de recuperação de negócio. O datacenter do tribunal conta com sala cofre, nobreaks, geradores, equipamentos de refrigeração e sistema de supressão de incêndio de alta disponibilidade. Estima-se em torno 15 dias a recuperação do ambiente a partir do zero, o que significa reconfigurar todos os servidores e posteriormente recuperar os becapes. A restauração dos serviços críticos para um ambiente secundário, no qual já estejam configurados os servidores, mas necessitam de sincronização dos dados, leva em torno de dois dias. O tempo total de recuperação de negócio dos serviços críticos de TIC do tribunal não pode exceder três dias. Outro ponto de interesse é o cenário de restrição econômica do país, refletido no tribunal.

[Questão 09]

(CESPE/TJPA 2020) Considerando o cenário hipotético apresentado no texto 4A04-III, para o planejamento de recuperação de negócio e com o objetivo de atender o tempo de recuperação dos serviços críticos, a replicação do datacenter em outro sítio

A é recomendada com o método de hot-site.

B é recomendada com o método de mobile-site.

C é recomendada com o método de cold-site.

D é recomendada com o método de mirror-site.

E não é recomendada, haja vista a proteção existente no sítio principal.

[Questão 09] –

Recovery Strategy	Recovery Time	Advantages	Disadvantages	Comments
Commercial Hot site	24 to 48 Hours	• Best recovery time • Easiest to implement as equipment, application software, data, and OS are in place • Easy to test at any point in time • The best solution that is available to support on-going operations	• Most expensive options duplicate equipment and software plus on-going version control issues • Ongoing communication costs to duplicate data very high • Term of the agreement can limit the duration of use • If you are not the "most important customer" you could be bumped	Often the most cost-effective strategy for data center recovery strategies. Clear contract terms need to be defined which meets the enterprise service objectives. Consideration should be made for disasters that impact entire regions such as hurricanes and earthquakes.
Internal Hot site	1 to 12 hours	• Best recovery time • Easiest to implement as equipment, application software, data, and OS are in place • Easy to test at any point in time • The best solution that is available to support on-going operations	• Most expensive options duplicate equipment and software plus on-going version control issues • Ongoing communication costs to duplicate data very high	If costs can be shared among multiple facilities within the enterprise, internal provisioning can cost competitive with commercial alternatives. If no appropriate secondary space is available "co-location" facilities providers offer managed raised-floor space at very attractive rates as an alternative to building out secondary sites.
Warm Site	24 to 48 Hours	• Moderately priced • Basic infrastructure is in place to support recovery operations • Ability to pre-stage delivery and implementing of the necessary hardware, application software, OS software, data, and communications	• Not easy to test • Recovery time is longer than with hot site and is controlled by the time to locate and restore applications • Facility equipment may not be exactly what is required – Once the recovery begins delays may occur because of equipment, software, or staffing shortfalls	If costs can be shared among multiple facilities within the enterprise, internal provisioning can cost competitive with commercial alternatives. If no appropriate secondary space is available "co-location" facilities providers offer managed raised-floor space at very attractive rates as an alternative to building out secondary sites.
Mobile Site	24 to 48 Hours	• Moderately priced • Typically, can be in place for 36 to 72 hours • Can be placed in the "parking lot" adjacent to you impacted facility	• Recovery time typically is at least 2 to 5 days longer than a hot site. • Access to your impacted facility may be hindered because of the event • A trailer may not be configured exactly as you need it	This approach avoids employee travel issues but has limitations on equipment availability and outbound bandwidth if small aperture satellite terminal (VSAT) links must be used for communications. If the disaster profile includes events such as hurricanes, floods or toxic spills, these solutions may not be appropriate.
Cold Site	72 plus Hours	• Lowest cost solution • Basic infrastructure power, air, and communication are in place • Can rent the facility for a longer-term at lower cost	• Longest recovery time • All equipment must be ordered, delivered, installed and made operational • Worst solution for supporting on-going operations	"Environmentally appropriate" space can be either provisioned internally or contracted from a commercial facilities service provider. Cold-site strategies are usually based on "quick-ship" delivery agreements to allow server, storage, and communications hardware and network service providers to quickly build out the data center and/or client workspace infrastructure.
Reciprocal Agreement	12 to 48 Hours	• Least costly solution • Better than no strategy	• Seldom works • Typically, in the same geographic area and a wide range disaster like an earthquake renders it of no use • No easy way to test	This is typically a formal agreement between two trusted, non-competing partners in different industries in which each provides secure sites for the other. This option is the least favorable and has the greatest risk associated with it.
Cloud	0 to 24 Hours	• Data and applications available immediately • Location independent • Easy to test	• Security • May not allow enough time for a daily cycle processing window	Data should be in place so activation would only be limited by connectivity and network addressing (DNS propagation).

[Questão 09]

(CESPE/TJPA 2020) Considerando o cenário hipotético apresentado no texto 4A04-III, para o planejamento de recuperação de negócio e com o objetivo de atender o tempo de recuperação dos serviços críticos, a replicação do datacenter em outro sítio

A é recomendada com o método de hot-site.

B é recomendada com o método de mobile-site.

C é recomendada com o método de cold-site.

D é recomendada com o método de mirror-site.

E não é recomendada, haja vista a proteção existente no sítio principal.

Dúvidas

Prof. Walter Cunha
falecomigo@waltercunha.com

https://www.patreon.com/timasters
https://www.facebook.com/walter.cunha.7
https://www.instagram.com/walter.cunha.7/
https://twitter.com/timasters
https://www.linkedin.com/in/walter-cunha-19a90721

PROVAS DE TI
TUDO PARA VOCÊ PASSAR