Administración y Gestión de Organizaciones – PEC4/Reto4

Presentación

Esta es la PEC que aborda, tal y como se ha desarrollado en el plan docente, las competencias y contenidos correspondientes al Reto 4 de la asignatura denominado Datos, organizaciones y resiliencia.

Competencias

Del conjunto de competencias abordadas en la asignatura y que se detallan en el plan docente, las que se trabajan en esta PEC son:

C6. Capacidad para identificar el papel que juegan las TIC en las organizaciones.

CGEC. Actuar de manera honesta, ética, sostenible, socialmente responsable y respetuosa con los derechos humanos y la diversidad, tanto en la práctica académica como en la profesional.

Objetivos

Comprender los conceptos introducidos en el módulo y saberlos identificar o aplicar a problemas teóricos y situaciones que emulen la realidad.

Resolución de la PEC

Para resolver con éxito esta PEC es necesario seguir el ciclo metodológico indicado en el plan docente:

1. Leer las indicaciones de la Guía de Aprendizaje para el módulo y sus recursos de aprendizaje correspondientes.

2. Leer, comprender y estudiar los recursos de aprendizaje correspondientes, siguiendo las indicaciones de la Guía de Aprendizaje.

3. Iniciar la resolución de la PEC a partir:

    a. De lo que se habrá aprendido en los recursos de aprendizaje.

    b. De las posibles indicaciones que dé el profesor vía Anuncios.

    c. De aquella información adicional que el estudiante deba obtener a partir de la bibliografía o de otras fuentes que acceda por su cuenta.

4. Compartir dudas o sugerencias mediante el foro y / o el buzón del profesor.

Recursos

Los recursos básicos para desarrollar esta PEC son los recursos de aprendizaje asociados al Reto 4 que se encuentran en el aula. La utilización de recursos complementarios puede ser necesaria en función de las necesidades del estudiante. En la Guía de Aprendizaje y en el espacio del aula *Contenidos* el estudiante encontrará el acceso a la bibliografía recomendada, a otras fuentes de información y herramientas de soporte adicional. En el caso de utilizar fuentes externas es imprescindible referenciarlas adecuadamente.

Criterios de valoración

La puntuación de cada pregunta se indica en cada enunciado. Se valorará principalmente la corrección de las respuestas, la capacidad de razonamiento o de justificación, y la capacidad de síntesis, así como la consecución de los objetivos y competencias de la asignatura con relación a esta PEC; pero también la corrección formal de las respuestas y, si aplica, su claridad discursiva o de desarrollo.

Formato y fecha de entrega

La entrega de las respuestas debe realizarse en la pestaña del aula denominada Entrega de Actividades, en un fichero o conjunto de ficheros .pdf, .doc, .rtf, o .odt. No es necesario que dicho archivo contenga los enunciados. Al pie de página escribís vuestro nombre completo y el número total de páginas que contiene la respuesta.

El nombre del fichero es irrelevante porque el Registro de Evaluación Continuada lo asigna automáticamente.

La fecha límite de entrega son las 24 horas del día 27 de diciembre de 2024.

Las soluciones de la PEC4 aparecerán en el aula el día 30 de diciembre de 2024.

Enunciado de la PEC

Recuerda que la capacidad de razonamiento y de síntesis se tendrán en cuenta en la valoración de las cuestiones planteadas.

PREGUNTAS TEÓRICAS (3 puntos) No está permitido el uso de la IA.

PREGUNTA 1 (3 puntos) No está permitido el uso de la IA.

A partir de la información del enlace https://www.incibe.es/incibe-cert/sectores-estrategicos/FAQNIS2, responde a las siguientes cuestiones sobre la nueva directiva europea NIS2 de ciberseguridad:

1.- ¿Qué es NIS2 y cuándo entra en vigor? ¿El incumplimiento de NIS2 podría incurrir en sanciones? (0,6 puntos)

La continua evolución de las amenazas cibernéticas ha dado origen a nuevos desafíos, poniendo de manifiesto ciertas limitaciones que dificultan abordar de manera eficaz los retos actuales y emergentes en el ámbito de la ciberseguridad. Esta realidad ha impulsado la necesidad de revisar y actualizar la legislación europea vigente en materia de ciberseguridad. En este contexto, la Directiva NIS1 de 2016 (UE 2016/1148), a pesar de haber sido un pilar esencial, estableciendo un marco normativo de medidas destinadas a garantizar un alto nivel de seguridad de las redes y sistemas de información en la Unión Europea, ha ido quedando obsoleta con el tiempo, resultando imperativo la pronta elaboración de un nuevo texto normativo que abordase de manera integral todas las amenazas emergentes en el ámbito de la ciberseguridad.

La Directiva NIS2 (Directiva (UE) 2022/2555) surge como respuesta a esa necesidad de actualización y fortalecimiento de las medidas establecidas en la Directiva NIS1, erigiéndose como un marco normativo estratégico para abordar los retos actuales en materia de ciberseguridad en el marco de la Unión Europea. Es por ello por lo que se procede a la actualización y derogación de la Directiva NIS1, cuya

trasposición en nuestro ordenamiento jurídico se materializó mediante el Real Decreto-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y su normativa de desarrollo, el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre.

La Directiva NIS 2 fue aprobada formalmente en noviembre de 2022, publicándose en el Diario Oficial de la UE (DOUE) el 27 de diciembre de 2022, y entró en vigor el 16 de enero de 2023, 20 días después de su publicación en el DOUE.

Los Estados miembros deberán adoptar y publicar las medidas necesarias para dar cumplimiento a lo establecido en la Directiva antes del 17 de octubre de 2024, comunicando de manera inmediata el texto de dichas disposiciones, las cuales resultarán de aplicación a partir del 18 de octubre de 2024.

Por otra parte, la Directiva NIS2 endurece las sanciones en caso de incumplimientos.

2. ¿Aplicaría NIS2 a una empresa Data Center con servicios de IaaS formada por 60 personas con una facturación de 65 millones de euros? (0.6 puntos)

La directiva aplica a medianas y grandes empresas, ya sean públicas o privadas, de los sectores de alta criticidad y otros sectores críticos indicados en sus anexos I y II, respectivamente, que presten sus servicios o lleven a cabo sus actividades en la Unión Europea.

De cara a valorar si una empresa es considerada como microempresa, pequeña, mediana o gran empresa, se debe atender a lo expuesto en la Recomendación 2003/361/CE que cita la NIS2, y que define dichas categorías de la siguiente manera:

- Microempresa: empresa que ocupa a menos de 10 personas y cuyo volumen de negocios anual o cuyo balance general anual no supera los 2 millones de euros.
- Pequeña empresa: empresa que ocupa a menos de 50 personas y cuyo volumen de negocios anual o cuyo balance general anual no supera los 10 millones de euros.
- Mediana empresa: empresa que ocupa entre 50 y 250 personas y cuyo volumen de negocios anual no excede de 50 millones de euros o cuyo balance general anual no excede de 43 millones de euros.
- Gran empresa: empresa que ocupa más de 250 personas y cuyo volumen de negocios anual o cuyo balance general anual sea superior a 43 millones de euros.

En NIS2 se amplían las entidades del sector de infraestructura digital, incluyendo proveedores de redes de servicios de computación en la nube.

En nuestro caso podría aplicar porque se trataría de una empresa mediana perteneciente al sector de infraestructura digital, que incluye proveedores de redes de servicios de computación en la nube.

3.- ¿La aplicación de la Directiva NIS2 es la misma para las entidades esenciales y para las entidades importantes? (0.6 puntos)

La Directiva NIS2, a efectos de cumplimiento de las medidas de gestión de riesgos, distingue entre entidades esenciales e importantes, en función del grado de criticidad de sus sectores o del tipo de servicio que prestan, así como de su tamaño.

Se consideran entidades esenciales:

- Grandes empresas de los sectores de alta criticidad del anexo I.
- Independientemente de su tamaño, los prestadores cualificados de servicios de confianza y registros de nombres de dominio de primer nivel y los proveedores de servicios de DNS.
- Medianas empresas proveedoras de redes públicas de comunicaciones electrónicas o de servicios de comunicaciones electrónicas disponibles para el público.

Se consideran entidades importantes todas aquellas de uno de los tipos mencionados en los anexos I o II que no puedan considerarse entidades esenciales.

4. ¿Hay algún caso en el que a una pequeña empresa le aplicaría NIS2? (0.6 puntos)

Un Estado miembro puede identificar a una entidad, independientemente de su tamaño, como esencial o importante cuando:

- La entidad sea el único proveedor en un Estado miembro de un servicio esencial para el mantenimiento de actividades sociales o económicas críticas.
- Una perturbación del servicio prestado por la entidad pudiera tener repercusiones significativas sobre la seguridad pública, el orden público o la salud pública.
- Una perturbación del servicio prestado por la entidad pudiera inducir riesgos sistémicos significativos, en particular para los sectores en los que tal perturbación podría tener repercusiones de carácter transfronterizo.

Por tanto, una pequeña empresa podría tener que cumplir NIS2.

5.- ¿A qué está obligada una empresa que le afecta NIS2 (0,6 puntos)

Todas las entidades dentro del ámbito de aplicación de la directiva deberán aplicar las medidas para la **gestión de riesgos de ciberseguridad**, así como cumplir con las obligaciones de **notificación de incidentes de ciberseguridad.**

PREGUNTAS TEST (2 puntos: 0,5 puntos / pregunta) No está permitido el uso de la IA.

Este test está formado por 4 preguntas en las que sólo hay una respuesta correcta. Intenta entender los conceptos y aspectos que se plantean para una mejor comprensión del contenido de los recursos docentes. Utiliza la tabla adjunta para indicar las respuestas.

1	2	3	4
D	C/G	B	D

1. ¿Cuál de las siguientes afirmaciones es falsa?:

   a) El plan de continuidad de negocio es de carácter voluntario para las empresas.
   b) Es necesario que los responsables de la empresa y el personal técnico conozcan el plan de continuidad del negocio.
   c) El Plan de crisis documenta la respuesta a la contingencia. A partir de las estrategias de recuperación escogidas, se seleccionan e implementan las iniciativas necesarias.
   d) Las cuatro fases principales de la gestión de las crisis y desastres son variación, recuperación, prevención y sanción.

   4.4) INCIBE Plan de contingencia y continuidad de negocio.

2. ¿Cuál de las siguientes afirmaciones es falsa?:

   e) Los datos son hechos objetivos sobre acontecimientos, que no tienen un significado inherente por sí mismos y que no han sido seleccionados ni procesados.
   f) Los activos intangibles como son los datos y la información, tienen como activos un potencial para aportar valor en un contexto organizativo, pero también son susceptibles de restar valor.
   g) Los datos no son demasiado útiles en la toma de decisiones, ya que la toma de decisiones es más efectiva y rápida cuanto menor es el nivel de datos.

h) Una gobernanza inteligente se basa en el uso de grandes cantidades de datos que la administración pública genera y recaba en el desarrollo de sus actividades y en sus relaciones con la ciudadanía y las empresas.

4.1) Datos, organizaciones y resiliencia.

3. Respecto a los cuadros de mando:

a) Los cuadros de mando y la inteligencia de negocio han de ofrecer una visión sesgada y subjetiva de la información importante de una empresa.
b) Un cuadro de mando es una representación resumida del nivel de cumplimiento de varios indicadores o métricas clave para la estrategia de una organización. Esto permite a los directivos de la organización supervisar el rendimiento en relación con dichos indicadores y tomar decisiones adecuadas para mejorar dicho rendimiento.
c) Los cuadros de mando son gestionados siempre por la Dirección General de la empresa.
d) Todas las respuestas anteriores son correctas.

4.1) Datos, organizaciones y resiliencia.

4. Sobre el concepto de resiliencia:

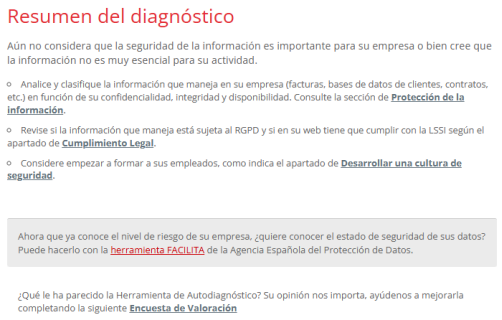
a) La resiliencia permite a las empresas flexibilidad.
b) La resiliencia según Denyer es: «La capacidad de una organización para anticiparse, prepararse, responder y adaptarse al cambio incremental y a las disrupciones bruscas para sobrevivir y prosperar».
c) Una cultura organizacional que valore a los empleados y potencie la formación en las competencias de adaptación al cambio, innovación, flexibilidad y autonomía, puede favorecer la resiliencia
d) Todas las respuestas anteriores son correctas.

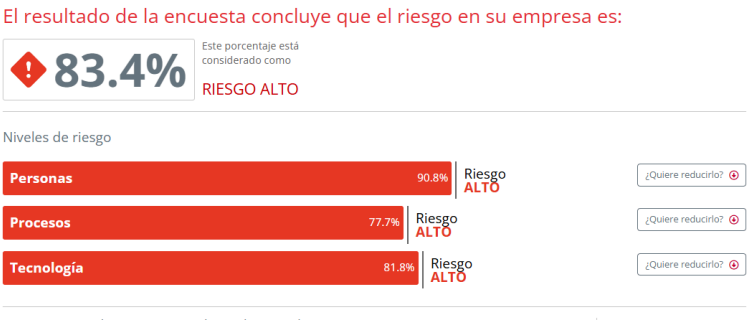
4.1) Datos, organizaciones y resiliencia.

EJERCICIO PRÁCTICO (5 puntos) No está permitido el uso de la IA.

1.Realiza el diagnóstico de tu empresa o entorno de trabajo que propone INCIBE desde el siguiente LINK: https://www.incibe.es/empresas/herramientas/conoces-tus-riesgos

Un posible resultado podría ser:





2. El propio INCIBE propone medidas para reducir cada tipo de riesgo. ¿Cuáles te propone para cada elemento analizado?

Para el riesgo en PERSONAS:

3,- A partir de las acciones propuestas por INCIBE elabora una Planificación de medidas de tratamiento de riesgos en PERSONAS:

Planificación de medidas PERSONAS:

Medida	Acciones	Responsable	Plazo

Por ejemplo:

Planificación de medidas PERSONAS:

Medida	**Acciones**	**Responsable**	**Plazo**
Formar a los empleados	Realizar concienciación en ciberseguridad de 2 horas de duración cada tres meses con contenidos actualizados según alertas.	Responsable de seguridad de la información.	31-12-25
Administración de cuentas de correo concentradas en una persona	Nombrar al Responsable de Seguridad de la información como administrador de las cuentas de correo y en su defecto al Director de la empresa.	Dirección	31-12-25
Actualizar contenido de la página web	Actualizar el contenido de la página web y revisar su seguridad cada tres meses.	Dirección MKT Responsable de seguridad de la información.	31-12-2025
Planificar las copias de seguridad.	Disponer de tres copias de seguridad en dos medios distintos y como mínimo uno de ellos externo.	Director de sistemas	31-12-2025