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.

PREGUNTA TEÓRICA (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 Directiva NIS2 es una directiva de la Unión Europea (UE) que surge como respuesta a la 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 UE. Amplía su ámbito de aplicación, para incluir sectores esenciales e importantes según su criticidad, tamaño o servicios, refuerza los requisitos de seguridad, regula la notificación de incidentes, mejora la seguridad en la cadena de suministro, fomenta el intercambio de información y la divulgación de vulnerabilidades, y crea la red europea de soporte de crisis (EU-CYCLONe).

   Apartado: ¿Qué es la Directiva NIS2?

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.

Apartado: ¿Cuándo entró en vigor la NIS2 y cuando aplicará en España?

El incumplimiento de esta directiva puede acarrear sanciones para las entidades que incumplan sus obligaciones en materia de ciberseguridad. Entre ellas, encontramos las siguientes:

1. Apercibir por incumplimiento.
2. Adoptar instrucciones vinculantes o requerimientos de subsanación.
3. Ordenar el cese de una conducta que infrinja la directiva.
4. Ordenar que se garanticen las medidas de gestión de riesgos o las obligaciones de información de manera y en un plazo determinados.
5. Imponer multas administrativas.

Apartado: ¿Qué multas y sanciones están contempladas en la NIS2 en caso de incumplimiento?

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 NIS2 aplica a medianas y grandes empresas, ya sean públicas o privadas, de los sectores de alta criticidad y otros sectores críticos que presten sus servicios o lleven a cabo sus actividades en la UE. El enunciado no especifica si la empresa opera en la UE, pero en caso afirmativo, la directiva sí que aplicaría, puesto que es una empresa mediana que pertenece a un sector de alta criticidad.

Apartado: Soy una entidad privada, ¿me afecta la Directiva NIS2?

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

En el supuesto de entidades esenciales, el régimen de supervisión deberá ser proporcionado, efectivo y disuasorio, es decir, se aplicará tanto a priori como a posteriori con respecto a los posibles incidentes y podrá conllevar suspensiones, prohibiciones temporales o multas. La persona física responsable de la entidad esencial o su representante podrá ser responsable por tales incumplimientos.

En el supuesto de las entidades importantes, la supervisión será únicamente reactiva, es decir, a posteriori. En este caso, el régimen de supervisión, llevado a cabo por profesionales cualificados, podrá conllevar multas administrativas.

Apartado: ¿La supervisión se aplicará de la misma manera a todos los tipos de entidades?

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

La NIS2 contempla excepciones para pequeñas empresas y microempresas que cumplan con criterios específicos que pongan de manifiesto su papel clave para la sociedad, la economía o para determinados sectores o tipos de servicios queden incluidas dentro de su ámbito de aplicación. Por tal motivo, e independientemente de su tamaño, las siguientes pequeñas empresas y microempresas podrían quedar incluidas dentro de su ámbito de aplicación:

- Entidades de alguno de los tipos mencionados en los anexos I o II.
- Entidades que se identifiquen como entidades críticas con arreglo a la Directiva (UE) 2022/2557.
- Entidades que presten servicios de registro de nombres de dominio.

Apartado: Y si soy una pequeña empresa, ¿me afectará la Directiva 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.

Las medidas indicadas como mínimas son las que se incluyen a continuación y se exigirán siempre de forma proporcional a los riesgos y vulnerabilidades específicas y al tamaño de las entidades:

a. las políticas de seguridad de los sistemas de información y análisis de riesgos;

b. la gestión de incidentes;

c. la continuidad de las actividades, como la gestión de copias de seguridad y la recuperación en caso de catástrofe, y la gestión de crisis;

d. la seguridad de la cadena de suministro, incluidos los aspectos de seguridad relativos a las relaciones entre cada entidad y sus proveedores o prestadores de servicios directos;

e. la seguridad en la adquisición, el desarrollo y el mantenimiento de sistemas de redes y de información, incluida la gestión y divulgación de las vulnerabilidades;

f. las políticas y los procedimientos para evaluar la eficacia de las medidas para la gestión de riesgos de ciberseguridad;

g. las prácticas básicas de ciberhigiene y formación en ciberseguridad;

h. las políticas y procedimientos relativos a la utilización de criptografía y, en su caso, de cifrado;

i. la seguridad de los recursos humanos, las políticas de control de acceso y la gestión de activos;

j. el uso de soluciones de autenticación multifactorial o de autenticación continua, comunicaciones de voz, vídeo y texto seguras y sistemas seguros de comunicaciones de emergencia en la entidad, cuando proceda.

Todas las medidas deben:

- Ser proporcionadas al riesgo, tamaño, coste e impacto y gravedad de los incidentes.
- Tener en cuenta el estado de la técnica, y cuando proceda, las normas europeas e internacionales.

Por otro lado, la directiva recoge en su articulado obligaciones de notificación de cualquier incidente significativo. La directiva define como incidente significativo aquel que:

1. Ha causado o puede causar graves perturbaciones operativas de los servicios o pérdidas económicas para la entidad afectada.
2. Ha afectado o puede afectar a otras personas físicas o jurídicas al causar perjuicios materiales o inmateriales considerables.

Apartado: ¿Qué obligaciones tendrán las entidades afectadas?

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**	**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.

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

   a) Los datos son hechos objetivos sobre acontecimientos, que no tienen un significado inherente por sí mismos y que no han sido seleccionados ni procesados.

   b) 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.

   c) 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.

   d) 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.

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. 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.

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 (Engancha el resultado):
   https://www.incibe.es/empresas/herramientas/conoces-tus-riesgos

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

   - **Personas**:
     - Formar a los empleados, ya que la mayoría de los ataques aprovechan su falta de concienciación sobre la importancia de la ciberseguridad.
     - En caso de que la empresa disponga de una página web, es importante mantener actualizados tanto los contenidos como las credenciales de acceso, ya que se puede publicar material que pueda ocasionar daños de imagen a la empresa.
     - Asignar la realización de copias de seguridad rutinarias a una persona o equipo antes de que sea demasiado tarde, ya que un error en algún sistema

puede provocar el colapso de la infraestructura tecnológica de la empresa durante horas e incluso días.

- Restringir cuentas de usuario con privilegios de administrador a personas que estén autorizadas para este cometido.
- En caso de que se pueda acceder a aplicaciones internas desde el exterior, hay que pensar concienzudamente sobre qué permisos otorgar a los usuarios.
- Para los smartphones corporativos que usan el equipo de ventas y los directores, es necesario establecer y comunicar una política que indique los usos permitidos y no permitidos. Además, es importante instaurar medidas de seguridad como el mantenimiento, la actualización o la sincronización del dispositivo.
- Contratar a personal experto en ciberseguridad para asegurar la correcta puesta en marcha de las medidas propuestas en este apartado.

- **Procesos**:
  - Establecer reglas para la actualización periódica de contraseñas, así como medidas que comprueben su fortaleza.
  - Establecer políticas de destrucción de la información para la correcta eliminación de datos sensibles.
  - Establecer procesos para realizar copias de seguridad frecuentes (a poder ser, diarias).
  - Realizar auditorías de seguridad periódicas de protección de datos, sobre todo teniendo en cuenta el ataque de phishing que sufrieron dos trabajadores el año pasado.
  - Establecer los servidores y routers de la empresa en un lugar seguro y con acceso restringido para evitar alguna manipulación de los mismos. Como mecanismos de seguridad, se pueden instalar cámaras y elementos físicos que bloqueen la entrada al sitio en el que están alojados los materiales. Para poder acceder a ellos, se requerirán tarjetas de acceso o llaves. En casos de empresas con una infraestructura tecnológica mayor, se podría contemplar también la posibilidad de contratar a un guardia de seguridad.
  - Establecer un plan B en caso de que ocurra algún imprevisto que afecte a la ciberseguridad de la empresa con el fin de poder adaptarse a las circunstancias y remediar el problema con la mayor celeridad posible.
  - Si se contratan servicios informáticos, hay que comprobar que contemplen las condiciones de ciberseguridad necesarias para hacer que su información esté

segura. Es necesario que se cumpla con la Ley Orgánica de Protección de Datos (LOPD).

- **Tecnología**:
  - Cifrar los datos sensibles de clientes y empleados almacenados en los servidores.
  - Exigir doble factor de autenticación (2FA) para añadir una capa extra de seguridad al binomio usuario/contraseña. También se puede contemplar la autenticación multifactor (MFA).
  - Evitar que los empleados reutilicen las contraseñas entre sus cuentas personales y corporativas. Para conseguirlo, la empresa debería ser la responsable de generar contraseñas seguras y proporcionárselas a los empleados. Hacerlo cada 6 meses, tal y como tiene establecido la empresa, es un periodo de tiempo razonable.
  - Tomar medidas de protección y analizar los intentos de ataque recibidos. Para lograrlo, se pueden establecer, por ejemplo, pruebas de penetración (*pentesting*).
  - Renovar las licencias de los antivirus para evitar el escenario en el que las licencias estén caducadas y los equipos sean vulnerables a cualquier tipo de amenaza.
  - Actualizar periódicamente los sistemas para tener instalados los parches de seguridad más recientes.

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
Formación en ciberseguridad para empleados	Organizar talleres y cursos de concienciación sobre ciberseguridad	Departamento de RRHH y TI	1 mes
Asignación de un administrador para las cuentas de correo electrónico	Designar una persona o equipo responsable de la administración y seguridad de cuentas	Dirección de TI	2 semanas
Actualización de contenidos y credenciales en la página web	Establecer un protocolo para actualizar regularmente los accesos y revisar los contenidos	Equipo de Marketing y TI	1 mes
Realización de copias de seguridad rutinarias	Asignar un equipo responsable de programar y realizar copias de seguridad periódicamente	Departamento de TI	2 semanas
Restricción de cuentas de usuario con privilegios de administrador	Definir permisos de acceso solo para empleados autorizados según políticas internas	Dirección de TI	2 semanas
Contratación de personal experto en ciberseguridad	Reclutar especialistas para implementar y supervisar las medidas de ciberseguridad	Dirección General y RRHH	2 meses
Política de uso para smartphones corporativos	Crear y comunicar una política clara sobre el uso permitido, junto con medidas de seguridad	Dirección de TI y RRHH	3 semanas