

Tarea online NDC05.

Título de la tarea: Normativa vigente de ciberseguridad de ámbito nacional e internacional.

Ciclo formativo y módulo: Curso de especialización en ciberseguridad en entornos de las tecnologías de la información - Normativa de Ciberseguridad.

¿Qué contenidos o resultados de aprendizaje trabajaremos?

Resultados de aprendizaje

- ✓ **RA5.** Recopila y aplica la normativa vigente de ciberseguridad de ámbito nacional e internacional, actualizando los procedimientos establecidos de acuerdo con las leyes y con la jurisprudencia existente sobre la materia.

Contenidos

Normativa vigente de ciberseguridad en el ámbito nacional e internacional.

- 1.- Normas nacionales e internacionales.
 - 1.1.- Sistema de Gestión de Seguridad de la Información.
 - 1.2.- Sistema de Gestión de Continuidad de Negocio con ISO 22301.
 - 1.3.- Acceso electrónico de los ciudadanos a los Servicios Públicos.
 - 1.4.- Esquema nacional de Seguridad.
 - 1.5.- La Directiva NIS.
 - 1.6.- Ley de Protección de Infraestructuras Críticas.

A1.- Contenidos adicionales.

1.- Descripción de la tarea.



Caso práctico



[isftic](#). Antena de Telecomunicaciones (CC BY-NC-SA)

La compañía ACME S.A. se encarga de proveer servicios de telecomunicaciones enfocados en comunicaciones internacionales tanto a particulares como a empresas.

ACME tiene una cartera de 300.000 clientes en España a los que ofrece estos servicios y por los cuales cobra una tarifa media de 23,5 € mensuales.

ACME está presente en 32 países, y se aprovecha de esta situación para dar servicio a multinacionales. Durante el año 2022 ACME ha logrado adjudicarse el servicio de telecomunicaciones de todas las embajadas en España.

Uno de sus clientes multinacionales es una entidad bancaria, con un nivel de madurez en seguridad elevado, uno de los requisitos que establece es la certificación ISO27001 en los servicios de comunicaciones.

La sede central de ACME se encuentra en Madrid, fue abierta en el año 2020, sus oficinas cuentan con climatización inteligente, jardines en las azoteas para mejorar la climatización y aprovechar el agua de la lluvia para los riegos de sus zonas verdes y paneles solares para mejorar la eficiencia energética.

Además, parte de los terrenos de la organización, han sido convertidos en parques públicos que pueden ser utilizados por los residentes de la zona, y los accesos por carretera a la zona han sido acondicionados, mejorados y reasfaltados.

En los últimos meses ACME esta de enhorabuena, ha logrado la adjudicación de un contrato mayor para la prestación de servicios de comunicaciones a una institución de las Fuerzas y Cuerpos de Seguridad del Estado. Dado el servicio que provee ha sido designado como proveedor de servicio esencial.

Dados los compromisos existentes hasta la fecha y con los nuevos contratos adjudicados, ACME va a abordar el proyecto de despliegue de un Sistema de Gestión de Seguridad de la Información, así como un Sistema de Gestión de Continuidad de Negocio. Asimismo, con el contrato otorgado para Fuerzas y Cuerpos de Seguridad del Estado, debe cumplir con la normativa del Esquema Nacional de Seguridad y con la Directiva NIS.

En esta tarea se requerirá de los conocimientos adquiridos a lo largo de la unidad para desarrollar los contenidos requeridos en el ejercicio.

¿Qué te pedimos que hagas?

Teniendo en cuenta la compañía descrita en el escenario anterior, da respuesta a las siguientes preguntas:

✓ Apartado 1: Normas nacionales e internacionales

¿Podrías proponer tres controles de cada proceso de seguridad de la normativa NIST?

✓ Apartado 2: Sistema de gestión de seguridad de la información basado en ISO 27001

- Desarrolla un contexto descriptivo de la organización alineado con los requisitos de información del estándar.
- Propón al menos tres controles para la mitigación de riesgos identificados.
- Desarrolla tres métricas de seguridad para ACME.

✓ Apartado 3: Sistema de gestión de continuidad de negocio basado en ISO 22301

El escenario a utilizar para este análisis de impacto es del de los sistemas centralizados que dan servicio a la red de comunicaciones de manera centralizada. En caso de indisponibilidad de estos sistemas, la red completa no podría funcionar.

Lucro cesante, provocado por la incapacidad de facturación ocasionada por la parada de los servicios de red. Se estima que la organización factura 100.000 € por hora.

Compensaciones, provocado por los perjuicios que pudieran ocasionar a las empresas a las que ACME da servicio. Según los contratos firmados con los clientes empresa, se garantiza un 99% de servicio, y únicamente se debe compensar en caso de que la caída dure más de 30 minutos, y si el cliente corporativo lo reclama. Se ha estimado que, a partir de la primera hora, las compensaciones supondrían 500.000€ por cada hora de caída.

Imagen, la confianza en la organización y en los servicios que provee se vería afectada. Esto supondría una pérdida de un 1% de la cartera de clientes por cada incidencia. Además, se estima que habría una caída de altas nuevas. Este tipo de perjuicios se ha cuantificado en 200.000€ por incidencia.

Sanciones, la comisión del mercado de las telecomunicaciones puede actuar en caso de una pérdida de servicio elevada, además al haber un designio de operador de servicio esencial, una caída prolongada podría ocasionar pérdidas económicas por sanciones.

Se estima que esta situación se daría únicamente en caso de caídas repetidas y de larga duración.

La organización no está dispuesta a asumir pérdidas mayores a 1,5 millones de €.

- ✓ Realiza un análisis de impacto en continuidad sobre los sistemas asociados al servicio de telecomunicaciones.
- ✓ Establece un valor justificado para los parámetros MTPD, RPO y RTO.

✓ **Apartado 4: Esquema nacional de seguridad**

Categoriza los sistemas asociados al servicio de telecomunicaciones en función al escenario definido en el caso práctico, por la prestación de servicios a FCSEs.

Desarrolla una declaración de aplicabilidad justificada.

2.- Información de interés.

Recursos necesarios y recomendaciones

Recomendaciones

- ✓ Antes de abordar la tarea:
 - ➡ lee con detenimiento la unidad, consulta los enlaces para saber más, examina el material proporcionado por el profesor y aclara las dudas que te surjan con él.
 - ➡ Realiza el examen online de la unidad, y consulta nuevamente las dudas que te surjan. Solo cuando lo tengas todo claro, debes abordar la realización de la tarea.
- ✓ No olvides elaborar el documento explicativo.



Indicaciones de entrega

Una vez realizada la tarea, el envío se realizará a través de la plataforma. El archivo se nombrará siguiendo las siguientes pautas:

Apellido1_Apellido2_Nombre_NDC05_Tarea

Asegúrate que el nombre no contenga la letra ñ, tildes ni caracteres especiales extraños. Así por ejemplo la alumna **Begoña Sánchez Mañas para la primera unidad del MP de CETI_NDC05**, debería nombrar esta tarea como...

sanchez_manas_begona_CETI_NDC05_Tarea

3.- Evaluación de la tarea.

Criterios de evaluación implicados

Criterios de evaluación RA5

- ✓ a) Se ha establecido el plan de revisiones de la normativa, jurisprudencia, notificaciones, etc. jurídicas que puedan afectar a la organización.
- ✓ b) Se ha detectado nueva normativa consultando las bases de datos jurídicas siguiendo el plan de revisiones establecido.
- ✓ c) Se ha analizado la nueva normativa para determinar si aplica a la actividad de la organización.
- ✓ d) Se ha incluido en el plan de revisiones las modificaciones necesarias, sobre la nueva normativa aplicable a la organización, para un correcto cumplimiento normativo.
- ✓ e) Se han determinado e implementado los controles necesarios para garantizar el correcto cumplimiento

¿Cómo valoramos y puntuamos tu tarea?

Rúbrica de la tarea	
Apartado 1: Normas nacionales e internacionales ¿Podrías proponer tres controles de cada proceso de seguridad de la normativa NIST?	2 puntos
Apartado 2: Sistema de gestión de seguridad de la información basado en ISO 27001 <ul style="list-style-type: none">✓ Desarrolla un contexto descriptivo de la organización alineado con los requisitos de información del estándar.✓ Identifica tres riesgos asociados al negocio.✓ Propón al menos tres controles para la mitigación de dichos riesgos.✓ Desarrolla tres métricas de seguridad para ACME.	3 puntos

<p>Apartado 3: Sistema de gestión de continuidad de negocio basado en ISO 22301</p> <ul style="list-style-type: none"> ✔ Realiza un análisis de impacto en continuidad sobre los sistemas asociados al servicio de telecomunicaciones. ✔ Establece un valor justificado para los parámetros MTPD, RPO y RTO. 	<p>2 puntos</p>
<p>Apartado 4: Esquema nacional de seguridad</p> <ul style="list-style-type: none"> ✔ Categoriza los sistemas asociados al servicio de telecomunicaciones en función al escenario definido en el caso práctico, por la prestación de servicios a FCSEs. ✔ Desarrolla una declaración de aplicabilidad justificada. 	<p>3 puntos</p>
<p>Redacción clara y correcta, sin errores ortográficos</p>	<p>Se resta 0,1 puntos por cada error ortográfico o expresiones incorrectas.</p>