Normativa de ciberseguridad desde el punto de vista del docente.

- ¿Qué normativas existen relacionadas con la ciberseguridad?¿Específicamente para la enseñanza de ciberseguridad, cuáles nos aplicarían desde un punto de vista de docente, y en qué situaciones?

RESPUESTA: En el Estado español se ha recogido un Código relacionado con la Ciberseguridad que se encuentra publicado aquí. Si bien este código contiene absolutamente toda la normativa estatal que hace referencia a la ciberseguridad de un modo transversal debe tenerse en cuenta que:

La normativa básica que debe contemplarse es la que hace referencia a:

1. Los posibles **delitos** que se pudieran cometer (Código Penal, ver la versión extractada que se dispone en el mismo Código de Ciberseguridad y que aplica directamente a los estudios sobre los que se lleva a cabo esta formación). Además de la **responsabilidad de la persona jurídica, e**s decir, de la empresa para la que estemos trabajando (artículo 31 bis del Código Penal).
2. Esquema Nacional de Seguridad, si estamos trabajando para empresa pública o para empresa privada que ofrezca / concurse para dar servicios a la Administración pública.
3. Reglamento General de Protección de Datos y Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales.
4. Reglamento de Inteligencia Artificial
5. NIS- 2 - homogeneización de la ciberseguridad en Europa (versión mejorada y ampliada de la NIS - 1 para servicios esenciales y digitales. ahora también de red, gestión de dominios, prestación de servicios de certificación, etc. ..
   Ver: Directiva NIS-2
   INCIBE: Faq's sobre NIS-2

Además, según el modelo de negocio de la empresa para la que estemos colaborando deberá darse cumplimiento a la normativa sectorial. Esto último forma parte de lo que se denominan los programas de cumplimiento de las empresas.

- ¿Cómo podríamos dar un enfoque más práctico al módulo de Normativa de Ciberseguridad?

RESPUESTA: Primero, a esta cuestión, no existe como tal "normativa de ciberseguridad" sino que, los desarrollos de software, la programación, el hacking y diferentes actividades que impliquen la Informática y las Telecomunicaciones vienen a implicar a normativa de carácter transversal que hace referencia a los impactos que pudiera producirse en terceros.

De este modo, consideramos tanto los posibles delitos que el propio trabajador / desarrollador pudiera cometer con ocasión de su trabajo, como los posibles impactos en cuestión de daños y perjuicios.
De este modo, optaría por poner ejemplos para cada una de las especialidades a las que pudieran optar los estudiantes para que vean el escenario real en el que pueden ver limitada su actividad: ejemplos:

a. Desarrolladores de aplicaciones: protección de datos en cuanto a la privacidad desde el diseño y por defecto. Transparencia en el tratamiento de los datos. Información al usuario de todos los tratamientos que hagan las aplicaciones.
    i. A título personal / profesional: no dejar ninguna puerta abierta para hacer monitorizaciones / seguimientos de los usuarios y vender los perfilados, por ejemplo. No utilizar los datos personales para extorsionar, vulnerar la intimidad de terceros, etc..
    ii. Implementar las medidas de seguridad necesarias para mantener a salvo los datos de los usuarios.
b. Desarrolladores de software: atender al contrato cerrado con el cliente, implementar las medidas de seguridad suficientes, considerar las actualizaciones de software y las mejoras continuas, etc..
c. Hacking ético: Tanto si somos equipo rojo como si somos equipo azul, deberemos atender a la relación contractual establecida que deberá considerar los límites al hacking (white hat, grey hat, black hat). Bajo criterios de derecho mercantil (contractual) hacer referencia a qué se ha de hacer con los resultados obtenidos y qué no ha de hacerse con ellos. Se establecerá de forma específica qué herramientas se van a utilizar para llevar a cabo el trabajo y se desarrollará un apartado en el que se especifique las medidas de seguridad de que disponemos.

- Dado que has tratado el tema como docente, coméntanos cómo lo has enfocado en tu caso. Danos 2-3 ejemplos de posibles tareas, escenarios, etc. que puedan usarse en clase.

    - Compliance

    RESPUESTA: El compliance sería el “estado ideal” que toda compañía debería cumplir y que desde el Compliance Officer debería estar al día en todos los aspectos que tengan relación con:
    - **Normativa sectorial propia** del modelo de negocio de la compañía. Por ejemplo, un laboratorio farmacéutico deberá dar cumplimiento a normativa específica en materia de Salud, tratamiento de medicamentos, farmacovigilancia, etc…
    - **Normativa en materia de protección de datos**. Siguiendo con el ejemplo del laboratorio farmacéutico deberemos disponer de un responsable en materia de protección de datos. Por tratarse de materia sensible (datos médicos, historiales clínicos, ADN,.. por ejemplo) lo ideal es que el Delegado de Protección de Datos (figura que estarían obligados a disponer) sea asumido por un consultor externo a la compañía.
    - Según la envergadura de la compañía (más de 49 empleados o tratamiento de datos sensibles) deberán tener en cuenta la normativa antisoborno y

anticorrupción (**Reglamento Whistleblowing**) creando un Canal de denuncias al que puedan dirigirse tanto personal interno, como proveedores y colaboradores externos a la compañía.
- **Compliance penal**, en el sentido de crear un plan de cumplimiento interno basado en un análisis de riesgos de los posibles delitos que pudieran cometerse en materia penal por los trabajadores, directores o los propios Administradores de las compañías.
- **NIS 2-**

- Protección de datos

RESPUESTA: La materia de protección de datos será considerada siempre en el tratamiento de esta formación puesto que de un modo u otro todos los desarrollos van a estar dirigidos al tratamiento de datos personales.
Ejemplo: hay productos y servicios que se venden únicamente como una licencia de uso a través de un contrato SaaS, ejemplo un SAGE o SAP, pero, aunque sea explotado por tercero, SAGE tendrá potencialmente acceso a todos los datos que trate su cliente por lo que sin ninguna duda deberá firmarse un contrato de Encargado de Tratamiento que obliga el Reglamento General de Protección de Datos.
El tratamiento de datos personales, por experiencia profesional, viene implicado en todos los productos y servicios tecnológicos y de desarrollo de software.

- Normativa, a nivel nacional e internacional

RESPUESTA: la normativa nacional e internacional tendrá relación con la normativa europea y ya está contestado arriba: Protección de datos, Canal de denuncias (corrupción Whistleblowing), NIS 2- y Reglamento de Inteligencia Artificial.

- Existen, a parte de estas 3, otras normativas que consideres importantes y de actualidad que merezca la pena tratarlas en clase?

RESPUESTA: No debemos olvidar, en ningún caso, la recién aprobada normativa europea de regulación de la Inteligencia Artificial. Una normativa basada en el riesgo y que tiene como punto de partida para la efectividad de la regulación una evaluación de las herramientas de IA desde el punto de vista del análisis de riesgos. Las IA vienen categorizadas en menor o mayor medida según los impactos que puedan producir en terceros. A cada una de las categorías le corresponderá dar cumplimiento a una serie de medidas de seguridad.
Por ejemplo, en el sector de los Seguros, si bien se levantaron voces que solicitaban que el sector del Seguro no fuera calificado de Alto Riesgo, no ha sido así. La clave está en la posibilidad tan alta de hacer perfilado de la población y, de hecho, la venta de sus productos y servicios se lleva a cabo con un estudio previo de la situación y circunstancias que rodean a los potenciales clientes para ofrecer un producto diseñado exclusivamente para cubrir sus necesidades.
Un ejemplo de ello, respecto al riesgo de los perfilados de población, podemos encontrarlo en el siglo pasado, cuando, gracias a un sistema super eficiente de calificación de la población en Holanda, incluyendo la religión que profesaban, permitió exterminar al 75% de

la población judía cuando se produjo la invasión alemana. Los sistemas de categorización / perfilado de la población, aunque pudieran parecer aparentemente inocuos, conllevan un riesgo muy alto.

- Hacking ético. Qué se considera dentro de esta denominación. Qué medidas podemos/debemos tomar a la hora de realizar un ejercicio de este tipo.

RESPUESTA: Hacking hace referencia a los ejercicios de intrusión al Sistema. Las medias que deben tomarse son :

- redacción contractual del servicio
- establecer el punto de partida (white hat, grey hat, black hat)
- establecer el marco en el que va a actuarse sobre el Sistema, es decir, partes el Sistema que van a auditarse.
- Tiempo de duración del "ejercicio"
- Equipo auditor
- Régimen de obligaciones y responsabilidades de ambas partes
- Elaboración de informe de resultados
- Establecer qué se va a hacer con los resultados obtenidos (de quién son o las obligaciones de destrucción de los mismos).
- Establecer que el equipo auditor, si es testigo de la comisión de delitos a través del sistema no queda eximido de denunciar los hechos a las FFCCSE.
- Precio del servicio y detalle de servicios que no se encuentran incluidos.

- Respecto a las prácticas relacionadas con la ciberseguridad, muchas veces se usan los centros como entornos de pruebas para el aprendizaje. ¿Algo que se tenga que tener en cuenta para estos casos?

RESPUESTA: Desde el punto de vista del Centro Educativo, lo ideal sería poner en conocimiento de los alumnos a través de un documento y que firmaran que las técnicas empleadas lo son en un entorno de laboratorio con finalidades educativas y que el Centro no se responsabiliza de su uso para fines distintos fuera del entorno de pruebas.

    - Ejercicio de phishing dentro de un centro. ¿Podrías realizar los alumnos la campaña, contra otros alumnos? ¿Podrían realizar los docentes este ejercicio, con los alumnos como víctimas? ¿La variable de si son mayores o menores repercute en algo?

RESPUESTA: Dado que estamos en un contexto formativo en ciberseguridad, lo lógico es que los alumnos experimenten en sí mismos lo que están aprendiendo. Lo ideal sería informar al alumnado al principio de curso, mediante un formulario, que el Centro va a llevar a cabo ejercicios / simulacros de ataques de ciberseguridad y de incendios no solo con fines educativos sino como garantía del propio Sistema de Información y de las Instalaciones.
Tened en cuenta que la seguridad física y la seguridad lógica van cogidas de la mano, por lo que tiene todo el sentido que hagamos esta advertencia.
Estos ejercicios nos ayudarán como Centro a conocer cuál es el nivel de seguridad (física y lógica) que realmente tenemos.

El hecho de que sean mayores o menores de edad no tiene ninguna relevancia. Tratándose de estudios especializados tiene toda la lógica que ellos mismos experimenten lo que sería implementar este tipo de pruebas en la empresa privada o pública.

Considerando que la normativa obliga a dar cumplimiento de estándares de ciberseguridad por tipología de servicios y por tratamiento de datos, está justificado llevar a cabo estos ejercicios considerando ambas vertientes (normativa / formativa).

- ¿Y contra los trabajadores?

Respecto a los TRABAJADORES: al iniciar la relación laboral / de funcionariado deben firmar un kit de bienvenida que habitualmente dispone de toda una serie de documentación relativa a las normas del Centro / empresa y a la confidencialidad. En ese "kit de bienvenida" se deberá informar al trabajador / colaborador de la posibilidad del Centro / empresa de llevar a cabo simulacros tanto en seguridad física como en seguridad lógica.
Esto tiene todo su sentido, más aun cuando podemos estar trabajando con expedientes de alumnos que contienen detalle de su situación familiar, estado de salud, estado financiero / subvenciones / becas por precariedad de los alumnos, etc..

- ¿Qué variables repercuten a la hora de realizar este tipo de prácticas?

Lo que habría que considerar en el informe final sobre el resultado de la práctica es anonimizar al alumno / miembro del personal que ha sido vulnerado. Es importante también que todo el alumnado afectado y los alumnos guarden silencio mientras dure el periodo del lanzamiento del ejercicio y hasta que haya llegado a su fin con la finalidad de no advertir a los demás.

- ¿Sería legal realizar un ejercicio de Vishing a alumnos?

RESPUESTA: En caso de duda, considerando que en los grupos puede haber aún menores de edad, o incluso, considerando que los teléfonos móviles tengan como titulares a los propios padres, sería recomendable pedir consentimiento para formar parte de los simulacros. Es una forma de crear conciencia. En la empresa privada se lleva a cabo este tipo de ejercicios para poner en evidencia la conciencia en ciberseguridad de los propios empleados.
La normativa en protección de datos exige a la empresa PROACTIVIDAD en la concienciación de sus trabajadores y uno de los medios para hacerlo es a través de los simulacros.

- ¿Dónde reside la línea entre lo legal y lo ilegal, dentro de las prácticas de ciberseguridad? ¿Existen zonas grises?
  - ¿La primera fase de la Kill Chain, reconocimiento, es legal, aunque se haga sobre destinatarios reales y sin permiso expreso?

RESPUESTA: Es legal todo reconocimiento cuando no se interactúe con los Sistemas de las Organizaciones.

- Enumerar prácticas específicas que son de reconocimiento (pasivo o activo) y su consideración legal/no legal.

    - Nmap y escaneo de puertos
    - Shodan -
    - …

RESPUESTA: en el momento en el que se está “pidiendo” información a un Sistema sobre el que no tenemos autorización de actuar, estamos interactuando con él. La respuesta que nos de va a configurar un mapa de vulnerabilidades.

Esta fase queda “oculta” a los ojos de terceros cuando se trata de una prueba que lanza un alumno, por ejemplo, sin embargo, si explotamos las vulnerabilidades, la acción anterior de reconocimiento activo del Sistema formará parte de los **actos preparatorios del delito** e igualmente condenable junto con el delito principal.

- Otro perito informático plantea que copiar una IP de shodan en el navegador es “entrar”, y por lo tanto no legal. Sin embargo, comenta que entre profesionales hay discusiones al respecto. Cual es tu opinión al respecto, y podrías darnos alguna sentencia/jurisprudencia que lo corrobore.

RESPUESTA: No hay absolutamente ninguna sentencia que vincule un acto de reconocimiento con un delito. Desde mi punto de vista, estamos ante lo que se denomina “actos preparatorios punibles” y que únicamente serán conocidos cuando se haya perpetrado el delito. No todos los actos preparatorios son punibles, sino únicamente aquellos que vengan así declarados por el tipo penal.

Ej. desarrollar un software para cometer una intrusión es un acto preparatorio que tiene identidad propia y sería condenable en relación con el delito perpetrado, ej, revelación de secretos / intrusión en un sistema sin estar autorizado a ello (197 bis), etc…

AP Málaga, sec. 3ª, S 23-05-2000, nº 177/2000, rec. 458/2000; FUNDAMENTOS DE DERECHO

PRIMERO.-

Se plantea en el recurso la cuestión del límite o frontera entre la fase de **preparación del delito** y el inicio de la esfera de la ejecución del mismo. Pese a reconocer que no hay aún respuesta uniforme y comúnmente aceptada en la doctrina penal al debate suscitado por el apelante, la solución propuesta por el juzgador, en el segundo párrafo del primero de los fundamentos de derecho, se adecua a la postura mantenida en sentencias de la Sala Segunda del Tribunal Supremo de 13 de mayo de 1.993, 30 de noviembre de 1.999 y 20 de diciembre de 1.999. La doctrina clásica distingue el carácter equívoco de los actos preparatorios, que no pueden ser diferenciados de los actos lícitos, en tanto que los actos de ejecución son claramente inequívocos en cuanto muestran ya en sí su dirección hacia la consumación delictiva. La teoría objetivo-material exige para considerar que se ha realizado un acto de ejecución que éste ponga ya en peligro o inicie la lesión del bien jurídico tutelado por el delito, en tanto que para la teoría objetivo-formal los actos ejecutivos son sólo aquellos que pertenecen a la conducta o acción

descrita por el verbo rector del tipo. Pues bien, todas estas teorías, según puede leerse en las sentencias mencionadas, adolecen del mismo defecto: delimitan de forma indudable los casos que ya de por sí serían claros, esto es, aquéllos en que la ejecución de la acción típica se ha iniciado, pero dejan en la zona de la duda los supuestos en que la conducta externa del autor se ve interrumpida en el momento en que está a punto de iniciar el comportamiento propiamente típico, esto es, el que nítidamente cumpliría la conducta descrita por el verbo rector. Por ello hoy se tiende a complementar aquellos criterios con una referencia al plan del autor, considerando en una tesis que puede calificarse de mixta que deben jugar los tres criterios de la finalidad o plan del agente, la iniciación del riesgo para el bien jurídico protegido y la inmediatez de esos actos que, sin necesidad de eslabones o estadios intermedios, se encaminan ya a la fase delictiva de la consumación, esto es, se aproximan al límite inicial de la acción típica o de la realización de uno de los elementos iniciales del tipo. Esta combinación de los criterios diferenciadores armoniza con la definición de la tentativa contenida en el párrafo 2ø del artículo 3 del Código Penal de 1973 (EDL 1973/1704) , que exigía dar principio a la ejecución, y fue aceptada por la doctrina la Sala Segunda del Tribunal Supremo en sentencia de 5 de diciembre de 1985. Desde esta perspectiva, forzoso es convenir con el sentenciador en que el hecho de saltar la valla que circunda el recinto dónde se guardaban los vehículos es un claro comienzo de ejecución, pues es sumamente razonable inferir que el ánimo que guiaba tales comportamientos era la sustracción de algo indeterminado que se guardara en el interior del recinto, máxime cuando la explicación que dieron los acusados, que refirieron pretender dormir dentro de una furgoneta, no sólo es escasamente convincente sino que resulta absurda, si tenemos en cuenta que el vigilante del recinto declaró en el plenario que vio llegar una furgoneta de la que salieron los acusados y saltaron la valla. Obvio es que si lo que buscaban era una furgoneta para dormir en su interior, ya la tenían. Siendo, por consiguiente, adecuada la calificación jurídica de los hechos y correcta su punición, se impone la desestimación del recurso interpuesto y la íntegra confirmación de la sentencia de instancia.

- ¿Qué ocurre si en horas de clase un alumno realiza un ataque contra una víctima real? Es decir, un ataque por su cuenta totalmente ajeno a cualquier planteamiento del profesor. ¿Qué implicaciones legales tendría eso para el profesor/centro?

RESPUESTA: Aquí entraría en juego la documentación que debería firmar el alumno al iniciar el curso responsabilizándose de las acciones ilícitas ocurridas mientras se encuentre en el Centro educativo.
Si el alumno sale con vuestra dirección IP o con algún registro que os pueda identificar como el atacante, podríamos incurrir en una responsabilidad civil por daños a terceros.

Entiendo aquí que la actividad desde un centro público nos situaría en una reclamación por daños de la Administración Pública en el ejercicio de sus funciones.
Ningún profesor debería ser imputado penalmente, más allá de las medidas disciplinarias que pudieran imponerse si no se ha previsto las suficientes cautelas.

El menor / alumno mayor de edad no quedará exento de responder penal y civilmente por los daños que pudiera haber causado a terceros.

- Tema NDA-s. A la hora de realizar un ejercicio de pentesting, campaña de phishing, etc. ¿Qué documentos hay que firmar para estar blindados ante la ley? Entendiendo que no hay plantillas oficiales al respecto, ¿qué apartados deben tratar cada documento?

RESPUESTA: un NDA se firma en la fase PRE-CONTRACTUAL, es decir, los intervinientes en unas relaciones de planificación de lo que puede ser el servicio van a intercambiar información. Con la recepción de la información se va a preparar una propuesta de contrato para proveer un producto / servicio. El NDA es previo a cualquier relación contractual. Puede ser unilateral (obliga a guardar confidencialidad únicamente a quien recibe la información) o puede ser bilateral (ambas partes guardarán confidencialidad sobre toda la información que compartan).

- ¿En un centro de formación, en nuestro caso de FP, quién puede firmar un NDA?¿A la hora de hacer un ejercicio de phishing/vishing, etc., es suficiente el consentimiento del director (algunos profesores se quejan de que el correo del centro es suyo, personal)?

RESPUESTA: el NDA previo a la relación contractual lo firmará el representante del Centro Educativo.
A continuación se deberá confeccionar un documento con el receptor del servicio en el que se detalle:

- qué se va a hacer
- qué medios se van a emplear
- quién va a intervenir
- durante cuánto tiempo
- qué técnica se va a llevar a cabo
- cuáles son las obligaciones de las partes
- qué va a pasar con los resultados obtenidos
- precio, si lo hay.. etc..

- ¿Los centros públicos de FP del País Vasco tienen independencia a la hora de firmar un NDA (todos tienen el mismo CIF, el de educación)?

RESPUESTA: Aunque todos tengan el mismo CIF, no todos deberían tener el mismo número de centro, ni el mismo representante legal. Cuando un alumno se pre-inscribe a un Grado de FP deberá señalar el Centro del que viene (número del centro) y el Centro en el que quiere inscribirse (número del centro). Incluso los correos electrónicos de cada centro educativo son independientes y propios para cada uno de ellos.

LA CLAVE: la clave está en especificar de forma clara en qué va a consistir el ejercicio

NOTA DE IBAI: En este punto, hemos comentado internamente que sería adecuado un comentario respecto al alcance del servicio contratado. Nos comentan de empresas, que muchos pentesters noveles meten la pata en ese respecto. Si te han contratado para realizar un testeo, no puedes utilizar ese permiso para ver, copiar, etc. documentos que

accedes como consecuencia de ese ejercicio. Lo dejamos a tu criterio, pero creo que es una apreciación importante.

- Un alumno ha detectado un intento de estafa mediante suplantación de identidad en instagram en la cuenta @xxxxyyy. ¿Hasta dónde podría llegar para desenmascarar al culpable? Es decir, alguien con conocimientos de ciberseguridad, ¿Qué podría hacer en este caso, y qué no?

RESPUESTA: Mientras que la actuación de un menor / alumno esté destinada a la captación de evidencias para ayudar a un tercero sin llegar a la provocación del delito, las evidencias podrán ser tenidas en cuenta. Todas las pruebas captadas deberán ser validadas en juicio, es decir, quien intervino en la investigación porque sus conocimientos podían ayudar y facilita las pruebas a los afectados, deberá acudir a juicio como testigo para que sean válidas.

Las pruebas son siempre válidas cuando no se haya vulnerado derechos ni cometido ninguna ilegalidad para obtenerlas, si no es así, se considerará como corruptas y no válidas.

La mejor opción, ponerse en contacto con el afectado y facilitarle las evidencias para que las proponga a los cuerpos policiales en caso de interponer denuncia.

- ¿Cuáles son los casos más habituales que llegan al juzgado, relacionados con la ciberseguridad?

RESPUESTA: estafas, fraudes, suplantaciones de identidad, estafas del CEO, blanqueo por imprudencia (mulas digitales), exfiltración y robo de datos por empleados, intrusión, daños informáticos, …

- A raíz de los últimos hackeos a grandes empresas españolas como Banco Santander, DGT, Iberdrola, Telefónica, Ticketmaster, Decathlon… ¿Qué medidas reactivas se toman por parte de las empresas en cuanto al ámbito legal?

- Caso práctico respecto a la protección de datos. Has sido cliente de Iberdrola hasta hace un año, pero haciendo referencia a la RGPD, pides que se borren tus datos cumpliendo con los procedimientos que dan para ello: *https://www.iberdrola.es/informacion/politica-privacidad*
    - Ha pasado un mes, y no has recibido respuesta. ¿Cuál sería el siguiente paso? ¿Reportarlo a la AEPD?

RESPUESTA: SÍ

    - Has recibido respuesta de que tus datos han sido borrados. 2-3 meses después, te llama un comercial en nombre de Iberdrola y al preguntarle de

dónde ha sacado tu número de teléfono te cuelga. ¿Cúal sería el siguiente paso a realizar? ¿Cómo puedes asegurar te de que, efectivamente, se han borrado tus datos?

RESPUESTA: Volver a interponer reclamación a la AEPD acompañando la reclamación previa

- En el caso de algunas empresas, como Iberdrola, utilizan empresas subcontratadas para las labores comerciales. ¿Cómo puedes asegurarte de que también se han borrado los datos de las subcontratas?

RESPUESTA: No podemos asegurarlo. Muchas veces se reactivan las listas de correo y es el momento de interponer reclamación.

- ¿Cúal es la realidad, en este tipo de casos, más allá de las normativas?

- ¿Hasta qué punto es interesante que nuestros alumnos sepan de compliance?

RESPUESTA: Deben conocer que sus acciones pueden impactar en varios flancos de protección de las organizaciones.

- Existe algún tipo de software que se utilice para la comprobación de normativas o ISOs? ¿Podrías recomendarnos alguna aplicación GRC para el aula? (incluidas las de pago)

RESPUESTA: Sobre herramientas de GRC no conozco ninguna que haga análisis completo. Una que he trabajado y es bastante completa es OneTrust trabaja sobre evaluación de riesgos, tratamiento de datos, ciberseguridad. Es bastante cara.

Dudas respecto a obligaciones/responsabilidades de los centros

- ¿Cuáles son las obligaciones legales que tiene un centro de FP en cuanto a ciberseguridad y/o protección de datos (LOPD/GPRD)? ¿esto a qué le compromete al centro? ¿Cuáles son las vulneraciones o fallos más habituales al respecto?

RESPUESTAS: Un Centro Educativo público está obligado a dar cumplimiento a los mínimos de seguridad / ciberseguridad para las Administraciones públicas (ENS). En la página web de CCN-CERT hay varias herramientas para el sector público para evaluación de la seguridad.

- ¿Quién sería el responsable último en caso de no acatar estas obligaciones? ¿Es el director responsable legal ante este tipo de infracciones?

RESPUESTA: Tratándose de un servicio público diría que el Departamento de Educación / Consejería de Educación. Un director de Centro Educativo no puede ser responsable de que la Administración no de cumplimiento a sus obligaciones.

- ¿Podría un profesor también enfrentarse a consecuencias legales por incumplir alguna ley de protección de datos?

RESPUESTA: En este escenario, lo lógico es que cualquier reclamación se dirija al Centro Educativo y al Departamento de Educación.

- ¿Hay diferencias entre un centro público/concertado en cuanto a responsabilidades legales?

RESPUESTA: Imagino que depende de para qué y cuál es el régimen que se ha pactado en esa relación público-privada.

ANEXO 1 - DCB Asignatura Normativa de ciberseguridad (Especialización IT)

Módulo Profesional: Normativa de ciberseguridad.

Código: 5026.

Créditos ECTS: 3.

Resultados de aprendizaje y criterios de evaluación.

1. Identifica los puntos principales de aplicación para asegurar el cumplimiento normativo reconociendo funciones y responsabilidades.

Criterios de evaluación:

a) Se han identificado las bases del cumplimiento normativo a tener en cuenta en las organizaciones.

b) Se han descrito y aplicado los principios de un buen gobierno y su relación con la ética profesional.

c) Se han definido las políticas y procedimientos, así como la estructura organizativa que establezca la cultura del cumplimiento normativo dentro de las organizaciones.

d) Se han descrito las funciones o competencias del responsable del cumplimiento normativo dentro de las organizaciones.

e) Se han establecido las relaciones con terceros para un correcto cumplimiento normativo.

2. Diseña sistemas de cumplimiento normativo seleccionando la legislación y jurisprudencia de aplicación.

Criterios de evaluación:

a) Se han recogido las principales normativas que afectan a los diferentes tipos de organizaciones.

b) Se han establecido las recomendaciones válidas para diferentes tipos de

organizaciones de acuerdo con la normativa vigente (ISO 19.600 entre otras).

c) Se han realizado análisis y evaluaciones de los riesgos de diferentes tipos de organizaciones de acuerdo con la normativa vigente (ISO 31.000 entre otras).

d) Se ha documentado el sistema de cumplimiento normativo diseñado.

3. Relaciona la normativa relevante para el cumplimiento de la responsabilidad penal de las organizaciones y personas jurídicas con los procedimientos establecidos, recopilando y aplicando las normas vigentes.

Criterios de evaluación:

a) Se han identificado los riesgos penales aplicables a diferentes organizaciones.

b) Se han implantado las medidas necesarias para eliminar o minimizar los riesgos identificados.

c) Se ha establecido un sistema de gestión de cumplimiento normativo penal de acuerdo con la legislación y normativa vigente (Código Penal y UNE 19.601, entre otros).

d) Se han determinado los principios básicos dentro de las organizaciones para combatir el soborno y promover una cultura empresarial ética de acuerdo con la legislación y normativa vigente (ISO 37.001 entre otros).

4. Aplica la legislación nacional de protección de datos de carácter personal, relacionando los procedimientos establecidos con las leyes vigentes y con la jurisprudencia existente sobre la materia.

Criterios de evaluación:

a) Se han reconocido las fuentes del Derecho de acuerdo con el ordenamiento jurídico en materia de protección de datos de carácter personal.

b) Se han aplicado los principios relacionados con la protección de datos de carácter personal tanto a nivel nacional como internacional.

c) Se han establecido los requisitos necesarios para afrontar la privacidad desde las bases del diseño.

d) Se han configurado las herramientas corporativas contemplando el cumplimiento normativo por defecto.

e) Se ha realizado un análisis de riesgos para el tratamiento de los derechos a la protección de datos.

f) Se han implantado las medidas necesarias para eliminar o minimizar los riesgos identificados en la protección de datos.

g) Se han descrito las funciones o competencias del delegado de protección de datos dentro de las organizaciones.

5. 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.

Criterios de evaluación:

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 normativo de las nuevas normativas. incluidas en el plan de revisiones.

Duración: 48 horas.

Contenidos básicos:

Puntos principales de aplicación para un correcto cumplimiento normativo:

− Introducción al cumplimiento normativo (Compliance: objetivo, definición y

conceptos principales).

− Principios del buen gobierno y ética empresarial.

− Compliance Officer: funciones y responsabilidades.

− Relaciones con terceras partes dentro del Compliance.

Diseño de sistemas de cumplimiento normativo:

− Sistemas de Gestión de Compliance.

− Entorno regulatorio de aplicación.

− Análisis y gestión de riesgos, mapas de riesgos.

− Documentación del sistema de cumplimiento normativo diseñado.

Legislación para el cumplimiento de la responsabilidad penal:

− Riesgos penales que afectan a la organización.

− Sistemas de gestión de Compliance penal.

− Sistemas de gestión anticorrupción.

Legislación y jurisprudencia en materia de protección de datos:

− Principios de protección de datos.

− Novedades del RGPD de la Unión Europea.

− Privacidad por Diseño y por Defecto.

− Análisis de Impacto en Privacidad (PIA), y medidas de seguridad.

− Delegado de Protección de Datos (DPO).

Normativa vigente de ciberseguridad de ámbito nacional e internacional:

− Normas nacionales e internacionales.

− Sistema de Gestión de Seguridad de la Información (estándares internacionales)

(ISO 27.001).

− Acceso electrónico de los ciudadanos a los Servicios Públicos.

Esquema Nacional de Seguridad (ENS).

− Planes de Continuidad de Negocio (estándares internacionales) (ISO 22.301).

− Directiva NIS.

− Legislación sobre la protección de infraestructuras críticas.

Ley PIC (Protección de infraestructuras críticas).

Orientaciones pedagógicas.

Este módulo profesional contiene la formación necesaria para desempeñar la función de diseñar el sistema de cumplimiento normativo de ciberseguridad en una organización.

La función de diseñar un sistema de cumplimiento normativo incluye aspectos como la caracterización de los principales aspectos de las diferentes normativas de ciberseguridad de obligado cumplimiento para la organización.

Las actividades profesionales asociadas a esta función se aplican en la integración, de las últimas actualizaciones en normativa de ciberseguridad a nivel nacional e internacional que apliquen, en el sistema de cumplimiento normativo de la organización.

La formación del módulo contribuye a alcanzar los objetivos generales o), p), q), r), s), t), u) y v) y las competencias j), k), l), m), n) y ñ) del curso de especialización.

Las líneas de actuación en el proceso de enseñanza aprendizaje que permiten alcanzar los objetivos del módulo versarán sobre:

– La identificación de los cambios de la normativa de ciberseguridad, tanto nacional como internacional, que afectan a la organización.

– La elaboración de mapas de riesgos.

ANEXO 2 - CHARLAS O VIDEOS RELACIONADAS CON LEGISLACIÓN Y CIBERSEGURIDAD

1. ¿Por qué necesito una autorización para hacer Hacking Ético?

https://www.a2secure.com/blog/por-que-necesito-una-autorizacion-para-hacer-hacking-etico/

2. El pentesting a tu alcance. ¿Reportar Vulnerabilidades? No.

https://legalconsultors.es/pentesting-reportar-vulnerabilidades/

3. La curiosidad mató al hacker

https://www.youtube.com/watch?v=h6xDWLgj3KA

4. He descubierto un delito, ¿y ahora qué?

https://www.securityartwork.es/2018/06/22/he-descubierto-un-delito-y-ahora-que/

5. Securiters entrevista (2023)

https://www.youtube.com/watch?v=zCn_LoT_8gg

6. Navaje Negra - Veo tu cuenta (2019)

https://www.youtube.com/watch?v=XeaWFyA35a8

7. Navaje Negra.

https://www.youtube.com/watch?v=sB4n5qQJ0fw

8. Intel2023 - El valor probatorio del Informe de Inteligencia

https://www.youtube.com/watch?v=LTQwh-Z3n5o

9. La tecnología lo permite, pero es ilegal

https://www.youtube.com/watch?app=desktop&v=S0lGh-LOpgo

10. Entrevista Ruth Sala

https://www.youtube.com/watch?v=Yc2JZv1x-h0&t=1156s

ANEXO 3 - LINKS SOBRE CONTENIDO DE LA CHARLA

Web de Amador Aparicio (Scan an Android app to obtain a full privacy report based on permission analysis)
https://apkfalcon.infor.uva.es/

Noticia: “Detenidos un estudiante de FP y su cómplice por hackear la DGT, ayuntamientos, bancos, universidades y más de 100 administraciones”
https://www.elmundo.es/espana/2024/06/28/667d97d8fc6c832a6c8b4576.html