Bases Específicas: TITULADO SUPERIOR CIBERSEGURIDAD

Por la presente se convoca un proceso selectivo, para cubrir **1 puesto de Titulado Superior Ciberseguridad** en los términos anunciados en el BOCM de 19 de abril de 2023, y según lo acordado en la Comisión Paritaria de 7 de febrero de 2024, en la que se acuerda seguir aplicando las bases que estaban vigentes durante el año 2023, hasta el 30 de abril de 2024.

REQUISITOS PARA PARTICIPAR Y CARACTERÍSTICAS DEL PUESTO:

Podrán participar en el proceso selectivo, aquellos candidatos que cumplan, los requisitos mínimos que se establecen en las bases generales y en las presentes **"Bases específicas".**

Quedarán excluidos del proceso selectivo los candidatos que no cumplan algunos de los requisitos mínimos fijados en las bases generales o en la presente ficha y, en particular, los que no acrediten la titulación y experiencia requerida a que se hace referencia en el presente apartado.

Nombre del puesto: **TITULADO SUPERIOR CIBERSEGURIDAD**

Número de plazas:

PROCEDIMIENTO	PLAZAS
Turno Libre	1
Total plazas	**1**

Jornada: Las plazas se ajustarán a la jornada continuada de mañana de lunes a viernes.

Lugar de trabajo: Ámbito territorial de aplicación del II Convenio Colectivo de Canal de Isabel II, S.A.

Retribución anual: A fecha de publicación de estas bases específicas, la retribución fija anual es de **41.104,04€.**

GRUPO PROFESIONAL	SUBGRUPO	ÁREA FUNCIONAL
TITULADOS UNIVERSITARIOS	A	Técnica

Complementos variables adicionales (**hasta** un máximo de un **21,5%*** del salario del puesto):

- Complemento por objetivos
- Incentivo de productividad
- Complemento por desempeño

**Se aplicarán conforme a lo establecido en el II Convenio Colectivo de Canal de Isabel II, S.A.*

Titulación requerida: Estar en posesión de una de las siguientes titulaciones:

- Licenciatura en Ingeniería Informática.
- Licenciatura en Matemáticas, especialidad de Computación.
- Licenciatura en Física, especialidad en Cálculo Automático.
- Licenciado en Informática.
- Ingeniero de telecomunicaciones.
- Grado en Ingeniería de Tecnologías y servicios de Telecomunicación.
- Grado en Ingeniería Informática.

- Grado en Seguridad Informática.
- Grado en Ingeniería de la Ciberseguridad.
- Grado en Ingeniería en Sistemas de la Información.
- Grado en Matemáticas e Informática.
- Grado en Ingeniería de Computadores.

Y, para los grados arriba indicados como "Titulación requerida", al menos uno de los siguientes Masters reconocidos como titulaciones oficiales por el Ministerio de Educación en Informática y Telecomunicaciones, Ciberseguridad y Tecnologías de la Información y Comunicación (TIC):

- Máster en Ciberseguridad.
- Máster Universitario en Seguridad de la Información.
- Máster Universitario en Seguridad de Tecnologías de la Información y de las Comunicaciones.
- Máster Universitario en Análisis de Datos, Ciberseguridad y Computación en la Nube.
- Máster Universitario en Ciberseguridad y Privacidad.
- Máster Oficial en Ingeniería de Seguridad de la Información y las Comunicaciones.
- Máster Universitario en Ingeniería de la Seguridad Informática e Inteligencia Artificial.
- Máster Universitario en Investigación en Ciberseguridad.
- Máster Universitario en Investigación en Ingeniería de Software y Sistemas Informáticos.
- Máster FP de Ciberseguridad en Entornos de las Tecnologías de la Información.
- Máster en Ingeniería Informática.
- Máster en Sistemas Informáticos.
- Máster Oficial - Ingeniería Informática / Computer Engineering.
- Máster Universitario en Ciencias y Tecnologías de la Computación.
- Máster Universitario en Soft Computing y Sistemas Inteligentes.
- Máster Universitario en Sistemas Inteligentes.
- Máster Universitario en Nuevas Tecnologías en Informática
- Máster Universitario en Ingeniería de Telecomunicación.
- Máster Universitario en Ingeniería Matemática.
- Máster Universitario en Matemática Computacional.
- Máster Universitario en Ingeniería Computacional y Matemática.
- Máster Universitario en Ingeniería de Computadores y Redes.
- Máster Universitario Oficial en Ciencia de Datos e Ingeniería de Computadores.
- Máster Universitario en Automática y Robótica.
- Máster Universitario en Automática e Informática Industrial.
- Máster Universitario en Ingeniería de Control, Automatización y Robótica.
- Máster Universitario en Inteligencia Artificial.

Idioma

El requisito de inglés, podrá acreditarse mediante alguno de los siguientes certificados:

- EOI: 1er y 2do cursos de Nivel Avanzado o Certificado de Nivel Avanzado (Plan antiguo: 1er y 2do curso Ciclo Superior o Certificado de Aptitud).
- Cambridge First Certificate in English (CFE).
- Certificado ISE II del Trinity College de Londres.
- GESE 7-12 del Trinity College de Londres.
- TOEFL iBT, con una puntuación total a partir de 72.
- TOEFL pBT, con una puntuación total a partir de 567.
- TOEFL cBT, con una puntuación total a partir de 220.
- IELTS, con una puntuación total a partir de 5,5.
- TOEIC, puntuación mínima en alguna de las siguientes destrezas: Listening and Reading ≥ 785.
- APTIS for Teachers/APTIS General de British Council, cuya puntuación acredite un nivel B2.
- Business Language Testing Service (BULATS), con una puntuación total a partir de 60.
- Oxford Test of English (OTE), prueba on-line cuya puntuación acredite un nivel B2.
- Pearson Test of English General- Level 3 (B2).
- Certificación CertAcles English B2, expedida por universidades españolas y reconocida por la Asociación de Centros de Lenguas de la Enseñanza Superior (ACLES).
- Anglia ESOL Examinations-Advanced (B2)

***Nota**: es conveniente marcar la correspondiente casilla en la página de presentación de solicitudes para, caso de que sea necesario, permitir a Canal de Isabel II, S.A. realizar prueba objetiva de inglés para acreditar el nivel B2 solicitado.*

Experiencia requerida: Poseer experiencia mínima demostrable de **18 meses** como titulado superior en las titulaciones requeridas.

Carné de Conducir: Carné de conducir B en vigor.

PROCEDIMIENTO DE SELECCIÓN:

El proceso se ajustará a lo establecido en las bases generales, y a lo acordado en la Comisión Paritaria de 7 de febrero de 2024, en la que se acuerda seguir aplicando las bases que estaban vigentes durante el año 2023, hasta el 30 de abril de 2024.

1º.- PRESENTACIÓN DE SOLICITUDES

Los candidatos presentarán su solicitud de participación a través de la página web de Canal de Isabel II, S.A.: www.canaldeisabelsegunda.es, en el apartado Empleo.

La inscripción en el proceso selectivo se realizará conforme a lo indicado en las bases generales.

El plazo de admisión de **solicitudes finaliza a las 23:59 horas del día 11 de marzo de 2024,** no admitiéndose ninguna solicitud posterior a dicha fecha. La no presentación de la solicitud en tiempo y hora supondrá la exclusión del aspirante.

2 º.- ÓRGANO DE SELECCIÓN:

El Órgano de Selección designado para la evaluación y corrección de las pruebas estará compuesto por los siguientes miembros:

	TITULARES	SUPLENTES
Presidente/a	Susana Pérez Martínez	Eratsi Rangel Gutiérrez
Vocal	Alberto Escribano García	Miguel Rodríguez Sáinz
Vocal	Olga Morales Cobos	Pepe Somoza Colino
Vocal	Alfonso Sandoval Santos	Alfredo Pintado de Santiago
Vocal	Javier Solís Blanco	Javier González Martín

3º.- PRUEBAS

La puntuación global máxima que podrá obtenerse en el proceso de selección será de **15 puntos**:

FASES	PUNTUACIÓN MÁXIMA	CARÁCTER ELIMINATORIO
Teórico-prácticas	10 puntos	Sí
Evaluación de potencial y competencias	5 puntos	Sí
Total	**15 puntos**	

4º.- PRUEBA TEÓRICA/PRÁCTICA

Se realizará prueba teórica/práctica para evaluar si los candidatos cuentan con los conocimientos, así como la habilidad o destreza en el ejercicio profesional necesarios para el adecuado desempeño del puesto de trabajo, atendiendo a lo señalado en los apartados “Conocimientos necesarios” y “Actividad a desarrollar”, de las bases específicas.

Esta prueba tendrá carácter eliminatorio y será obligatoria para todos los aspirantes, consistirá en realizar un cuestionario tipo test, compuesto de **100 preguntas** con **3 alternativas de respuesta** y una sola respuesta correcta.

Cada respuesta correcta será puntuada con **1 punto**, las incorrectas penalizarán **0,33333333 puntos. Las preguntas no contestadas no puntúan ni penalizan**. Con carácter general, en el cuestionario test se incluirán 10 preguntas adicionales de reserva, ordenadas de la 101 a la 110 que servirán para sustituir, si procede, preguntas que pudieran ser anuladas.

La duración máxima para la realización de esta prueba **será de 2 horas y 30 minutos.**

La puntuación máxima de estas pruebas una vez ponderados los resultados en base 10 será de **10 puntos** y para superarlas los candidatos deberán obtener una puntuación mínima de **5 puntos**.

Los candidatos que opten a la realización de las pruebas teórico-prácticas, deberán presentarse en el lugar y hora publicados. Deberán asistir con el DNI, NIE y/o pasaporte en vigor, no pudiendo estar caducados los documentos que acrediten la identidad. Si se produjera esta situación es necesario presentar un documento que justifique la no vigencia, pudiendo mostrar un resguardo de renovación o denuncia en caso de hurto o robo.

Se prohibirá acceder a la realización de esta prueba con cualquier dispositivo electrónico (móvil, tableta, calculadoras programables, relojes inteligentes, etc.), considerando causa de exclusión el incumplimiento de esta restricción.

Al finalizar el examen, los candidatos conservarán una copia de la hoja de respuestas que garantizará la asistencia y la comprobación de la realización del ejercicio.

La no asistencia a la prueba será motivo de exclusión del proceso selectivo.

5º.- EVALUACIÓN DE POTENCIAL Y COMPETENCIAS

Esta prueba permitirá evaluar el potencial y competencias de los candidatos para valorar su adecuación al puesto. Adoptarán con carácter general la forma de una entrevista de evaluación y se realizarán por técnicos cualificados en esta materia.

Su valoración máxima será de **5 puntos** y tendrá carácter eliminatorio, por lo que será necesario obtener una nota mínima de **2,5 puntos.**

CONOCIMIENTOS NECESARIOS:

- **NORMATIVA EN SEGURIDAD DE LA INFORMACIÓN**
  - Estrategia Nacional de Ciberseguridad 2019.
  - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
  - R.D. 1720/2007 Reglamento que desarrolla la Ley de protección de datos.
  - Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
  - R.D. 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
  - Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas (LPIC) y Real Decreto 704/2011 de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
  - Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea (“Ley NIS”).
  - Reglamento Europeo (UE) N.º 910/2014, del 24 de julio de 2014, de identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento eIDAS).

- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

- **CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS**

  - Modelo de seguridad orientada a la gestión del riesgo relacionado con el uso de los sistemas de información
  - Relación de las amenazas más frecuentes, los riesgos que implican y las salvaguardas más frecuentes
  - Salvaguardas y tecnologías de seguridad más habituales
  - La gestión de la seguridad informática como complemento a salvaguardas y medidas tecnológicas

- **ANÁLISIS DE IMPACTO DE NEGOCIO**

  - Identificación de procesos de negocio soportados por sistemas de información
  - Valoración de los requerimientos de confidencialidad, integridad y disponibilidad de los procesos de negocio
  - Determinación de los sistemas de información que soportan los procesos de negocio y sus requerimientos de seguridad

- **GESTIÓN DE RIESGOS**

  - Aplicación del proceso de gestión de riesgos y exposición de las alternativas más frecuentes
  - Metodologías comúnmente aceptadas de identificación y análisis de riesgos
  - Aplicación de controles y medidas de salvaguarda para obtener una reducción del riesgo

- **PLAN DE IMPLANTACIÓN DE SEGURIDAD**

  - Determinación del nivel de seguridad existente de los sistemas frente a la necesaria en base a los requerimientos de seguridad de los procesos de negocio
  - Selección de medidas de salvaguarda para cubrir los requerimientos de seguridad de los sistemas de información
  - Guía para la elaboración del plan de implantación de las salvaguardas seleccionadas

- **IDENTIFICACIÓN DE SERVICIOS**

  - Identificación de los protocolos, servicios y puertos utilizados por los sistemas de información
  - Utilización de herramientas de análisis de puertos y servicios abiertos para determinar aquellos que no son necesarios
  - Utilización de herramientas de análisis de tráfico de comunicaciones para determinar el uso real que hacen los sistemas de información de los distintos protocolos, servicios y puertos

- **IMPLANTACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS**

  - Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
  - Criterios de seguridad para la segregación de redes en el cortafuegos mediante Zonas Desmilitarizadas (DMZ)
  - Utilización de Redes Privadas Virtuales (VPN) para establecer canales seguros de comunicaciones
  - Definición de reglas de corte en los cortafuegos
  - Relación de los registros de auditoría del cortafuegos necesario para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
  - Establecimiento de la monitorización y pruebas de los cortafuegos

- **ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN**

  - Introducción al análisis de riesgos
  - Principales tipos de vulnerabilidades, fallos de programa, programas maliciosos y su actualización permanente, así como criterios de programación segura
  - Particularidades de los distintos tipos de código malicioso
  - Principales elementos del análisis de riesgos y sus modelos de relaciones
  - Metodologías cualitativas y cuantitativas de análisis de riesgos
  - Identificación de los activos involucrados en el análisis de riesgos y su valoración
  - Identificación de las amenazas que pueden afectar a los activos identificados previamente
  - Análisis e identificación de las vulnerabilidades existentes en los sistemas de información que permitirían la materialización de amenazas, incluyendo el análisis local, análisis remoto de caja blanca y de caja negra
  - Optimización del proceso de auditoría y contraste de vulnerabilidades e informe de auditoría
  - Identificación de las medidas de salvaguarda existentes en el momento de la realización del análisis de riesgos y su efecto sobre las vulnerabilidades y amenazas

- **USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS**

  - Herramientas del sistema operativo tipo Ping, Traceroute, etc.
  - Herramientas de análisis de red, puertos y servicios tipo Nmap, Netcat, NBTScan, etc.
  - Herramientas de análisis de vulnerabilidades
  - Analizadores de protocolos tipo WireShark, DSniff, etc.
  - Analizadores de páginas web
  - Ataques de diccionario y fuerza bruta tipo Brutus, John the Ripper, etc.

- **DESCRIPCIÓN DE LOS ASPECTOS SOBRE CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS**

  - Principios generales de cortafuegos
  - Componentes de un cortafuegos de red
  - Relación de los distintos tipos de cortafuegos por ubicación y funcionalidad
  - Arquitecturas de cortafuegos de red
  - Otras arquitecturas de cortafuegos de red

- **GUÍAS PARA LA EJECUCIÓN DE LAS DISTINTAS FASES DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN**

  - Guía para la auditoría de la documentación y normativa de seguridad existente en la organización auditada
  - Guía para la elaboración del plan de auditoría
  - Guía para las pruebas de auditoría
  - Guía para la elaboración del informe de auditoría

- **SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)**

  - Conceptos generales de gestión de incidentes, detección de intrusiones y su prevención
  - Identificación y caracterización de los datos de funcionamiento del sistema
  - Arquitecturas más frecuentes de los sistemas de detección de intrusos
  - Relación de los distintos tipos de IDS/IPS por ubicación y funcionalidad
  - Criterios de seguridad para el establecimiento de la ubicación de los IDS/IPS

- **IMPLANTACIÓN Y PUESTA EN PRODUCCIÓN DE SISTEMAS IDS/IPS**

  - Análisis previo de los servicios, protocolos, zonas y equipos que utiliza la organización para sus procesos de negocio.
  - Definición de políticas de corte de intentos de intrusión en los IDS/IPS
  - Análisis de los eventos registrados por el IDS/IPS para determinar falsos positivos y caracterizarlos en las políticas de corte del IDS/IPS
  - Relación de los registros de auditoría del IDS/IPS necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de intentos de intrusión
  - Establecimiento de los niveles requeridos de actualización, monitorización y pruebas del IDS/IPS

- **CONTROL DE CÓDIGO MALICIOSO**

  - Sistemas de detección y contención de código malicioso
  - Relación de los distintos tipos de herramientas de control de código malicioso en función de la topología de la instalación y las vías de infección a controlar
  - Criterios de seguridad para la configuración de las herramientas de protección frente a código malicioso
  - Determinación de los requerimientos y técnicas de actualización de las herramientas de protección frente a código malicioso
  - Relación de los registros de auditoría de las herramientas de protección frente a código maliciosos necesarios para monitorizar y supervisar su correcto funcionamiento y los eventos de seguridad
  - Establecimiento de la monitorización y pruebas de las herramientas de protección frente a código malicioso
  - Análisis de los programas maliciosos mediante desensambladores y entornos de ejecución controlada

- **RESPUESTA ANTE INCIDENTES DE SEGURIDAD**

  - Procedimiento de recolección de información relacionada con incidentes de seguridad
  - Exposición de las distintas técnicas y herramientas utilizadas para el análisis y correlación de información y eventos de seguridad
  - Proceso de verificación de la intrusión
  - Naturaleza y funciones de los organismos de gestión de incidentes tipo CERT nacionales e internacionales

- **PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN**

  - Establecimiento de las responsabilidades en el proceso de notificación y gestión de intentos de intrusión o infecciones
  - Categorización de los incidentes derivados de intentos de intrusión o infecciones en función de su impacto potencial
  - Criterios para la determinación de las evidencias objetivas en las que se soportara la gestión del incidente
  - Establecimiento del proceso de detección y registro de incidentes derivados de intentos de intrusión o infecciones
  - Guía para la clasificación y análisis inicial del intento de intrusión o infección, contemplando el impacto previsible del mismo
  - Establecimiento del nivel de intervención requerido en función del impacto previsible
  - Guía para la investigación y diagnóstico del incidente de intento de intrusión o infecciones
  - Establecimiento del proceso de resolución y recuperación de los sistemas tras un incidente derivado de un intento de intrusión o infección

- Proceso para la comunicación del incidente a terceros, si procede
- Establecimiento del proceso de cierre del incidente y los registros necesarios para documentar el histórico del incidente

- **ANÁLISIS FORENSE INFORMÁTICO**

  - Conceptos generales y objetivos del análisis forense
  - Exposición del Principio de Locard
  - Guía para la recogida de evidencias electrónicas
  - Guía para el análisis de las evidencias electrónicas recogidas, incluyendo el estudio de ficheros y directorios ocultos, información oculta del sistema y la recuperación de ficheros borrados
  - Guía para la selección de las herramientas de análisis forense
  - Establecimiento de los escenarios de riesgo entendidos como pares activo-amenaza susceptibles de materializarse
  - Determinación de la probabilidad e impacto de materialización de los escenarios
  - Establecimiento del nivel de riesgo para los distintos pares de activo y amenaza
  - Determinación por parte de la organización de los criterios de evaluación del riesgo, en función de los cuales se determina si un riesgo es aceptable o no
  - Relación de las distintas alternativas de gestión de riesgos
  - Guía para la elaboración del plan de gestión de riesgos
  - Exposición de la metodología Magerit versión 3

- **CANAL DE ISABEL II:** Misión; Valores; Estrategia (Líneas y Planes). El Canal y el Ciclo integral del agua en la Comunidad de Madrid (Captación, Tratamiento, Distribución, Saneamiento, Calidad de las Aguas).
  https://www.canaldeisabelsegunda.es/documents/20143/26004946/InformeSostenibilidad2022.pdf/8b2019e2-09ed-629d-d63f-b24f4bf3402f?t=1685606241503

- **II Convenio Colectivo de Canal de Isabel II, S.A.:**

  - Título II: Organización del Trabajo
  - Título III: Clasificación profesional
  - Título VI: Seguridad y Salud Laboral
  - Título IX: Régimen Sancionador.

  https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-3895

- **Prevención de riesgos laborales**

Legislación aplicable en materia de seguridad y salud en el trabajo. En concreto, la siguiente normativa consolidada (u otra que la sustituyera, llegado el caso), las guías técnicas de Instituto Nacional de Seguridad y Salud en el Trabajo que las desarrolla y aspectos clave en prevención de riesgos laborales de aplicación. Normativa:

- Real Decreto 486/1997, de 14 de abril, por el que se establecen las disposiciones mínimas de seguridad y salud en los lugares de trabajo.
- Real Decreto 485/1997, de 14 de abril, sobre disposiciones mínimas en materia de señalización de seguridad y salud en el trabajo.
- Real Decreto 488/1997, de 14 de abril, sobre disposiciones mínimas de seguridad y salud relativas al trabajo con equipos que incluyen pantallas de visualización

- **Funciones y Responsabilidades del Recurso Preventivo.**

- Ley 31/1995, de 8 de noviembre de Prevención de Riesgos Laborales (LPRL) y la Ley 54/2003, de 12 de diciembre, de reforma del marco normativo de la prevención de riesgos laborales.
- RD 39/1997, de 17 de enero, por el que se aprueba el Reglamento de los Servicios de prevención (RSP).

BIBLIOGRAFÍA RECOMENDADA:

En relación con la normativa citada, las normas legales que se citan hacen referencia al documento consolidado de las mismas vigente en la fecha de publicación de la convocatoria. Además de la normativa, legislación y páginas webs detalladas en los conocimientos mínimos necesarios, se facilita la siguiente bibliografía para preparar la prueba de conocimientos:

- (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide.
- Official (ISC)2 Guide to the CISSP CBK.
- Norma UNE-EN ISO/IEC 27001:2017.
- Norma UNE-EN ISO/IEC 27002:2017.
- ISACA CISA Review Manual.
- ISACA CRISC Review Manual.
-

ACTIVIDAD A DESARROLLAR:

Las funciones principales del puesto son las siguientes:

- Colaborar en el desarrollo, implantación e impulso de todas las políticas de seguridad informática, todos los procedimientos generales de seguridad (PGS) y todas las instrucciones técnicas (IT) de seguridad de la información.

- Colaborar en la actualización del SGSI:
  - Análisis de riesgos anual
  - Valoración de activos
  - Clasificación de activos
  - Y todo lo relacionado con los controles del Anexo A de la norma ISO/IEC 27001:2013 y la norma ISO/IEC 27002:2013
  - Soporte a la redacción de controles SCIIF asignados a Seguridad Informática, actualización de los mismos, test de diseño y test manuales de efectividad
  - Soporte a la gestión de los riesgos corporativos definidos en los controles internos asignados a Seguridad Informática.
  - Formar parte del equipo de monitorización efectiva de la seguridad a través de eventos para la identificación temprana de amenazas y posibles incidentes de seguridad.
  - Colaborar en la creación de estándares y buenas prácticas relacionados con la seguridad informática y la construcción y desarrollo de software de aplicaciones; supervisando su aplicación.
  - Colaborar en el aseguramiento de los activos de información mediante la supervisión y el control centralizados sobre las políticas, estándares, mejores prácticas, procedimientos y guías relacionados con la seguridad informática; definiendo e implantando métricas.
  - Colaborar activamente en la realización de auditorías periódicas de seguridad (código, aplicaciones, infraestructura, equipamiento, etc.) y protección de la información, ayudando en la revisión de los resultados de las mismas, así como en las recomendaciones para la resolución de los problemas de seguridad detectados o, en su caso, la adopción de las medidas de contención que permitan minimizar el riesgo existente.

- Evaluaciones y estudios de seguridad de software y aplicativos de seguridad a adquirir por Canal de Isabel II.
- Participación en la gestión de proyectos en general dentro de Canal de Isabel II:
- Requisitos de seguridad.
- Evaluación de los requisitos de seguridad en las ofertas.
- Seguimiento.
- Gestión de los proyectos propios relativos a la seguridad de la información.
- Notificar, gestionar e investigar los incidentes de seguridad.
- Conocer, proponer y supervisar la aplicación de las últimas tecnologías en materia de seguridad de la información, así como el estado del arte en lo relativo a amenazas, tendencias, herramientas y soluciones tecnológicas existentes, procedimientos, metodologías, buenas prácticas, etc.
- Colaborar en las iniciativas de la Dirección de Seguridad para asegurar el cumplimiento de todas las leyes existentes que afecten a la seguridad de la información (Ley de Protección de Infraestructuras Críticas (LPIC), Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea (“Ley NIS”), etc.)
- Colaborar en la realización de las auditorias de control de accesos recogidas en el RLOPD.
- Supervisar y certificar el establecimiento de un framework de desarrollo seguro de aplicaciones
- Participación en la divulgación de la seguridad de la información entre los usuarios (revisión de contenidos, campañas de phishing, pruebas de seguridad, redacción de mensajes de aviso, etc.), lo que incluye soporte personalizado a todos los usuarios de la casa en temas de seguridad informática (dudas, cómo actuar, etc.).
- Participación en los Ciber Ejercicios en los que participe Canal de Isabel II.
- Vigilancia y seguimiento del cumplimiento técnico-legal de las actividades.

- Actuará como Recurso Preventivo en las actuaciones que así lo exijan.

Y, en general, todas aquellas que se deriven del desempeño del puesto de trabajo.

Fecha 1 de marzo de 2024
Isabel Pemau González
Directora de Recursos