Deloitte.

CNP assurances

Oficina de seguridad para la externalización del CISO

Propuesta de colaboración

Mayo de 2022

A) 174 ASS-AL/CNP ASSURANCES/01.01/DELOITTE ADVISORY

Los sectores en los que operan nuestros clientes son muy competitivos. La confidencialidad de la información es crítica. Deloitte protegerá la confidencialidad de la información de sus clientes.

Deloitte manifiesta explícitamente su compromiso con CNP Assurances de mantener estricta confidencialidad con respecto a este proceso y a cualquier información recibida durante el mismo.

Entendemos que nuestros análisis, técnicas, metodologías y herramientas expuestas en este documento son propiedad privada de Deloitte y esperamos que nuestros clientes también protejan su confidencialidad.

Bajo ninguna circunstancia deben compartirse con terceras personas ajenas a la Dirección de CNP Assurances sin el consentimiento expreso y por escrito de Deloitte.

Deloitte.

Deloitte Advisory, S.L.
Torre Picasso
Plaza Pablo Ruiz Picasso, 1 28020
Madrid, España
+34 915145000
www.deloitte.es

Oficina de ciberseguridad

Mayo de 2022

Estimados,

En respuesta a su solicitud, nos complace presentarle para su consideración nuestra propuesta de servicios profesionales relacionados con la puesta en marcha de un servicio de CISO as a Service que sirva de apoyo a CNP Assurances SA, sucursal en España para el liderazgo, coordinación, ejecución y gestión de las iniciativas de seguridad que sean necesarias durante la actividad de la entidad.

Siendo conscientes de la importancia que este trabajo tiene para ustedes, hemos elaborado esta propuesta considerando la participación de nuestras herramientas y personal más adecuado para este tipo de trabajo.

Los objetivos, alcance y descripción del servicio se exponen en la propuesta de servicios profesionales adjunta. El planteamiento descrito en ella es, a nuestro juicio, el que mejor responde a sus necesidades. Sin embargo, estamos a su entera disposición para estudiar cualquier otro enfoque alternativo que ustedes consideren más apropiado.

De acuerdo con nuestros procedimientos, les agradeceríamos nos remitiesen por escrito su aprobación a la presente propuesta en caso de conformidad con la misma.

Agradecemos muy sinceramente la oportunidad que nos brindan de ofrecerles nuestros servicios y les aseguramos nuestro mayor interés y dedicación en la realización del trabajo de esta propuesta, si nos fuera confirmada.

Sin otro particular, aprovechamos la ocasión para saludarle.

Rubén Frieiro
Socio

Daniel Hernández
Director

Índice


Si crees que la tecnología puede solventar tus problemas de seguridad, entonces no entiendes los problemas y no entiendes de tecnología
Bruce Schneier

Entendimiento de la problemática actual

¿Por qué una entidad no dispone de un CISO?

Sensación de ausencia de peligro

No somos un objetivo, no tenemos nada que le pueda importar a nadie

Sensación de impunidad

No tenemos una regulación ni un regulador que nos supervise o nos sancione

Ausencia de conocimiento experto

No tenemos recursos para contratar un CISO experimentado

Ausencia temporal del CISO

La entidad dispone de un CISO, pero durante un tiempo no podrá ejercer su función

¿Cuáles son las situaciones más comunes por las que una entidad no dispone de un CISO?

Entendimiento de la problemática actual

¿Por qué una entidad no dispone de un CISO?

Sensación de ausencia de peligro

No somos un objetivo, no tenemos nada que le pueda importar a nadie

Sensación de impunidad

No tenemos una regulación ni un regulador que nos supervise o nos sancione

Ausencia de conocimiento experto

No tenemos recursos para contratar un CISO experimentado

Ausencia temporal del CISO

La entidad dispone de un CISO, pero durante un tiempo no podrá ejercer su función

Si no tienes clientes, empleados, proveedores, inversores, competidores, propiedad intelectual, procesos de negocio..., efectivamente no serás un objetivo para ningún atacante potencial. Sin embargo, esto implicará que no tienes actividad, por lo que no tienes un negocio.

Recientes ataques de tipo *ransomware* demuestran que nadie está fuera del alcance de los ataques. La cada vez mayor interconexión de los negocios hace que un posible ataque a un proveedor pueda impactarnos significativamente, por lo que todas las entidades pueden verse afectadas. Es por esto por lo que debe existir una figura que gestione sus necesidades en ciberseguridad desde una perspectiva experta. Esta figura ayudará para la toma de decisiones en función del riesgo de la entidad.

Entendimiento de la problemática actual

¿Por qué una entidad no dispone de un CISO?

Sensación de ausencia de peligro

No somos un objetivo, no tenemos nada que le pueda importar a nadie

Sensación de impunidad

No tenemos una regulación ni un regulador que nos supervise o nos sancione

Ausencia de conocimiento experto

No tenemos recursos para contratar un CISO experimentado

Ausencia temporal del CISO

La entidad dispone de un CISO, pero durante un tiempo no podrá ejercer su función

El hecho de que las regulaciones que afectan a la entidad puedan no exigir explícitamente la figura de CISO no implica que la misma no deba ser tenida en cuenta. La gestión de los riesgos de ciberseguridad, mediante la definición, supervisión, implementación y operación de las medidas de ciberseguridad es responsabilidad del CISO, siendo necesaria una figura experta que las soporte.

Además de todo esto, son precisamente las regulaciones actuales (y sus correspondientes sanciones) las que suponen una palanca importante para abordar la mitigación de los riesgos de ciberseguridad (GDPR, Solvencia, EIOPA, PCI-DSS, PSD2, NIS, LPIC, etc.).

DC

Entendimiento de la problemática actual

¿Por qué una entidad no dispone de un CISO?

Sensación de ausencia de peligro

No somos un objetivo, no tenemos nada que le pueda importar a nadie

Sensación de impunidad

No tenemos una regulación ni un regulador que nos supervise o nos sancione

Ausencia de conocimiento experto

No tenemos recursos para contratar un CISO experimentado

Ausencia temporal del CISO

La entidad dispone de un CISO, pero durante un tiempo no podrá ejercer su función

Una de las tácticas a corto plazo utilizada en ocasiones por algunas entidades es que personas no expertas en ciberseguridad se hagan cargo de esta función. Sin embargo, la constante evolución de los ataques y las medidas de prevención requieren de un conocimiento experto específico que pueda proporcionar una visión de las necesidades en ciberseguridad ajustada a las necesidades de la entidad. De la misma manera, algunas entidades carecen de un atractivo real para un perfil experto que pueda actuar como CISO.

Evidentemente, no todas las entidades van a necesitar la misma dedicación, pero sí que la misma tenga un nivel de calidad que permita priorizar las iniciativas de seguridad a realizar por lo realmente importante, consiguiendo además que impacten lo menos posible en el negocio.

DC

Entendimiento de la problemática actual

¿Por qué una entidad no dispone de un CISO?

Sensación de ausencia de peligro

No somos un objetivo, no tenemos nada que le pueda importar a nadie

Sensación de impunidad

No tenemos una regulación ni un regulador que nos supervise o nos sancione

Ausencia de conocimiento experto

No tenemos recursos para contratar un CISO experimentado

Ausencia temporal del CISO

La entidad dispone de un CISO, pero durante un tiempo no podrá ejercer su función

Ciertas circunstancias que puedan afectar a la entidad, como una eventual ausencia no programada del CISO, la salida del CISO de la organización, o un cambio de funciones del CISO, pueden implicar un periodo de falta de responsabilidades en materia de ciberseguridad.

Ya sea durante un tiempo corto o como una solución alternativa a la espera de contratación de un nuevo CISO, es necesario disponer de un experto en la materia que pueda liderar las iniciativas en materia de ciberseguridad e identificar nuevos riesgos que puedan afectar a la entidad.

Índice

Objetivos y alcance

Alcance

CNP Assurances, consciente de la importancia de la Ciberseguridad en la estrategia y operativa de sus diferentes líneas de negocio, ha acometido un plan de acción a corto plazo con acciones muy básicas que es necesario acometer, coordinados por un servicio de Oficina de ciberseguridad de una duración reducida que externalice ciertas funciones del CISO.

Una vez realizado, se hace necesario acometer un plan a largo plazo que permita a la entidad actualizar su función de seguridad y adecuarla a las amenazas y exigencias regulatorias actuales.

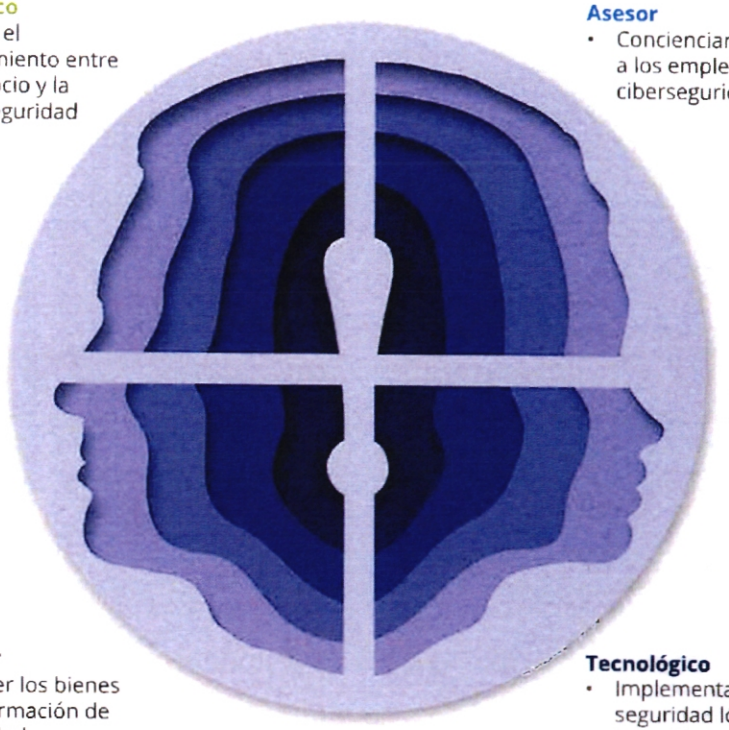
Todo esto hace que CNP Assurances considere necesario disponer de una Oficina de ciberseguridad que permita un adecuado liderazgo, coordinación y gestión de la ejecución de las iniciativas de seguridad de la entidad.

El enfoque de Deloitte propone un servicio que dé soporte en las acciones de seguridad englobando, entre otros proyectos, un análisis inicial que permita realizar dicha planificación y priorización a largo plazo de las diferentes acciones. Esto permitirá al servicio ejercer las labores de liderazgo, coordinación, ejecución y promoción de la ciberseguridad.

ROL DEL CISO

Estratégico
- Buscar el alineamiento entre el negocio y la ciberseguridad

Asesor
- Concienciar y formar a los empleados en ciberseguridad



Protector
- Proteger los bienes de información de la entidad

Tecnológico
- Implementar la seguridad lógica de la entidad

Índice

Referencias

Otras referencias en Oficinas Técnicas de Seguridad y externalización del CISO

A continuación se muestran las referencias permitidas más recientes de las Oficinas Técnicas de Seguridad para la Externalización del CISO (Ciso as a Service) realizadas por Deloitte Advisory, S.L. Las mismas son en gran parte adjudicaciones por tres años, pero se muestra el último año en el que las mismas han sido ejecutadas (la mayor parte con adjudicaciones por tres años).

Año	Proyecto	Cliente
2020	Oficina Técnica de Seguridad	Pelayo
2020	Oficina de SDLC	Banc Sabadell
2020	PMO Ciberseguridad	BBVA
2020	Oficina Técnica para la supervisión de PECA	MAPFRE
2020	Oficina de Lucha contra el fraude	MAPFRE
2020	CISO as a Service	TRIODOS Bank
2020	Oficina Técnica de Seguridad	Wizink
2020	Oficina Técnica de Seguridad Políticas y Normativas	Bankia
2020	Oficina Seguridad	Bankinter
2020	Oficina ciberseguridad Proyectos	Banco Santander
2020	Servicio de Seguridad en Nuevas Iniciativas	MAPFRE
2020	Oficina ciberseguridad	CLH

Año	Proyecto	Cliente
2020	Oficina Técnica de Seguridad	Viesgo
2020	Oficina Técnica de Seguridad	Inversis
2020	Oficina Técnica de Seguridad	Gurit
2020	Oficina de Gobierno y Cumplimiento	RACC
2020	Oficina Técnica de Seguridad	Bankia
2020	Oficina de SDLC	Ayuntamiento de Barcelona
2020	Oficina Ciberseguridad	Codere
2020	Servicio de Revisiones Técnicas	MAPFRE
2019	Asesoramiento en Oficina de Gobierno y Cumplimiento	Liberbank
2019	Oficina de Cumplimiento Normativo	Banca March
2019	Oficina de soporte al cumplimiento de LPIC	Entidad financiera
2019	Oficina Técnica de Seguridad Plan Transformación	Banco Santander
2019	Oficina Técnica de Seguridad Proyectos TyO	Airbus

Índice

Descripción de los servicios ofertados

Enfoque metodológico y aspectos clave de éxito en cada fase

- **Formalización de responsabilidades**
- **Definición del modelo de reporting del servicio**

- **Contacto constante durante todo el servicio, no solo en el retorno**
- **Gestión adecuada de la información y documentación**

Diseño

Conocer la actividad actual y determinar los requerimientos concretos de CNP Assurances para establecer las responsabilidades que asumirá el servicio, las tareas que realizará, y desarrollar el plan de transferencia y captura de conocimiento de áreas expertas de CNP Assurances.

- **Contacto desde el primer día con el responsable**
- **Recopilación de información disponible**
- **Evaluación de la situación y propuestas desde el principio**

Arranque

Puesta en marcha del Servicio: desarrollo de los procedimientos necesarios para su operación. Designación de comités de gobierno del servicio, modelo de relación con CNP Assurances. Inicio del proceso de transformación y madurez del servicio.

- **Reportes periódicos**
- **Comités de seguimiento**

Explotación

Operación normal del Servicio basado en una gestión de la demanda adecuada y de la realización de las actividades conforme a los parámetros de calidad establecidos y conforme a los acuerdos de nivel de servicio acordados en la organización.

Como parte de la explotación se contempla la mejora continua, identificando y gestionando las incidencias y desviaciones en relación al cumplimiento de los objetivos y puesta en marcha acciones correctivas. Mejorar y evolucionar el servicio, dotarlo de nuevas capacidades. Estandarización y automatización de actividades, evolucionar el modelo de madurez.

- **Gestión adecuada de la demanda**
- **Interlocución, coordinación y comunicación**
- **Seguimiento de la actividad e identificación de desviaciones**

Retorno

Asegurar que durante el transcurso del Servicio, se establece un modelo de gestión del conocimiento que permita poner a disposición de terceros o de otras áreas de CNP Assurances el control del Servicio en un plazo de tiempo determinado.

Establecer mecanismos de compartición del conocimiento.

Gestión del Servicio

Calidad y seguimiento

DC

Operación en modo BAU

Descripción de los servicios ofertados

Las labores de un CISO, de un vistazo

Mantenerse al día

- Observatorio de noticias de ciberseguridad y ataques
- Comunicación de tendencias en ciberseguridad
- Análisis de implicaciones de nuevas tendencias tecnológicas y de negocio
- Análisis temprano de impacto de nuevas regulaciones

Gestión

- Identificación de debilidades
- Resolución de dudas de seguridad
- Planificación, lanzamiento y gestión de iniciativas de seguridad
- Colaboración en la selección de proveedores
- Planificación y estimación de presupuestos de seguridad
- Contacto con áreas técnicas y de negocio
- Identificación de requisitos y riesgos asociados a seguridad
- Reporte a la Dirección
- Concienciación en seguridad

Problemas

- Punto de contacto ante problemas
- Comunicación a interlocutores
- Coordinación de involucrados
- Reporte a la Dirección

Descripción de los servicios ofertados

Las labores de un CISO, de un vistazo

Mantenerse al día

- Observatorio de noticias de ciberseguridad y ataques
- Comunicación de tendencias en ciberseguridad
- Análisis de implicaciones de nuevas tendencias tecnológicas y de negocio
- Análisis temprano de impacto de nuevas regulaciones

Aproximación Proactiva.

Screening continuo de noticias sobre nuevas tendencias, normativas y leyes

Aproximación Reactiva.

Requerimientos específicos (ad-hoc) en función de preguntas de la entidad

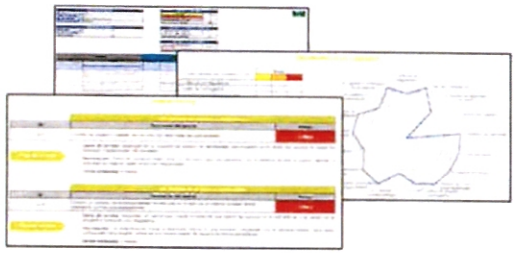
Red de Deloitte.

Presencia en más de 150 países

Ejemplos de reportes que mantendrán al día al CISO

Descripción de los servicios ofertados

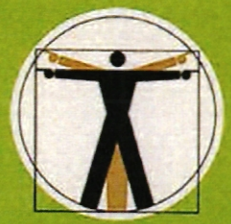
Las labores de un CISO, de un vistazo



Selección de proveedores

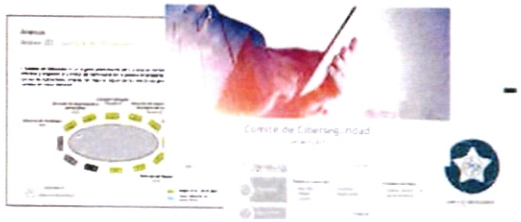
Cuadros de mando de ciberseguridad

Identificación de requisitos y controles



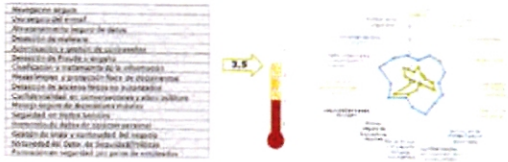
Gestión

- Identificación de debilidades
- Resolución de dudas de seguridad
- Planificación, lanzamiento y gestión de iniciativas de seguridad
- Colaboración en la selección de proveedores
- Planificación y estimación de presupuestos de seguridad
- Contacto con áreas técnicas y de negocio
- Identificación de requisitos y riesgos asociados a seguridad
- Reporte a la Dirección
- Concienciación en seguridad



Reporting a la Dirección

Planificación y gestión de iniciativas



Formación y concienciación en seguridad

DC

Descripción de los servicios ofertados

Las labores de un CISO, de un vistazo

- Definición de canales de comunicación con el servicio de CISO
- Identificación de potenciales escenarios de emergencia
- Revisión, actualización y definición de mecanismos a seguir para la comunicación, tramitación y coordinación en situaciones de emergencias
- Coordinación con los distintos interlocutores según los mecanismos establecidos
- Evaluación del resultado de la gestión, y mejora continua de los mecanismos

El presente servicio no contempla un servicio de resolución de incidentes, sino una labor de liderazgo y comunicación en la coordinación de problemas que puedan surgir en materia de ciberseguridad.

Problemas

- Punto de contacto ante problemas
- Comunicación a interlocutores
- Coordinación de involucrados
- Reporte a la Dirección

Descripción del servicio
Actividades de la Oficina de ciberseguridad

Descripción del servicio
Oficina de Seguridad | Enfoque metodológico

La **metodología** propuesta para la gestión del servicio **se basa en las mejores prácticas y estándares** de referencia existentes en el mercado y **enriquecida con la experiencia adquirida** en proyectos de oficinas técnicas de seguridad e implantación de metodologías de seguridad. El modelo planteado garantiza un enfoque PDCA:

Etapas del ciclo del servicio

Establecimiento	Fase Estable	Retorno
Diseño del servicio	**Explotación del servicio**	**Retorno del servicio**
Conocer la actividad actual y determinar los requerimientos concretos de CNP Assurances para establecer las actividades a realizar y capturar el conocimiento de áreas de competencia del servicio.	Operación normal del servicio basado en una gestión de la demanda adecuada y de la realización de las actividades conforme a los parámetros de calidad establecidos. Como parte de la explotación se contempla la mejora continua del servicio, donde se identifican y gestionan las incidencias y desviaciones en relación al cumplimiento de los objetivos y se ponen en marcha las acciones correctivas. Mejorar y evolucionar el servicio, dotándolo de nuevas capacidades, objetivos y procesos formales. Estandarización y automatización de actividades, evolucionar el modelo de madurez.	Asegurar que durante el transcurso del proyecto, se establece un modelo de gestión del conocimiento que permita la devolución del control a CNP Assurances. Establecer mecanismos de compartición del conocimiento.

Gestión del servicio

Calidad y seguimiento

DL

Descripción del servicio
Oficina de Seguridad | Enfoque metodológico

Según la información trasladada por CNP Parnerts, la Oficina de cibeguridad de Deloitte estará focalizada en los siguientes ámbitos de trabajo:

- Definir normativa de Seguridad (políticas, procedimientos,) y velar por su cumplimiento.
- Gestión de auditorías. (se daría también el apoyo necesario)
- Gestión diaria del CISO.
- Alinear estrategia de Seguridad con los objetivos de la empresa.
- Interactuar con la alta Dirección en materia de Seguridad de la Información:
  - ✓ Organización de los comités
  - ✓ Participación activa en Comités de Seguridad (métricas, reporting de riesgos, planes de acción, amenazas e incidencias)
- Decisiones relacionadas con la seguridad.
- Soporte/Liderazgo en la implantación al SGSI.
- Marcar la estrategia relacionada con:
  - ✓ Concienciar y transmitir las políticas de seguridad al resto de áreas de IT de CNP
  - ✓ Formación y Concienciación tanto a la alta Dirección como al resto de los empleados.

Para ello se establecerá un equipo de trabajo experto del área de Risk Advisory – Cyber de Deloitte compuesto por un FTE durante 6 meses contando con dos perfiles:

- 1 Perfil consultor senior de la línea **Cyber Strategy**
- 1 Perfil consultor técnico de la línea **Cyber Infrastructure Protection**

DC

Descripción del servicio
Oficina de Seguridad | Diseño del servicio

ANÁLISIS DE REQUISITOS

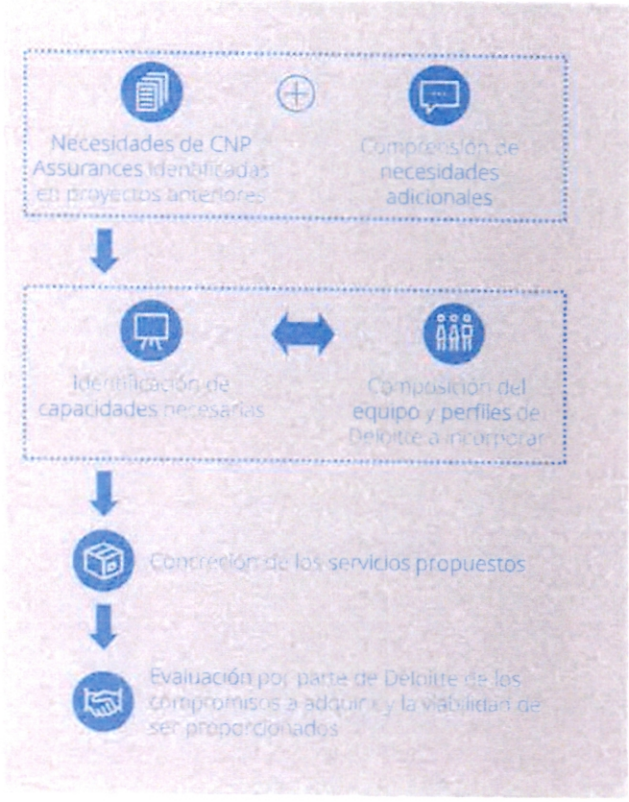
Una vez **analizadas las necesidades de CNP Assurances, se han establecido los servicios** a prestar por la Oficina Técnica de Seguridad. Se ha realizado una primera propuesta conforme a las necesidades comunicadas por CNP Assurances y el conocimiento que tiene Deloitte de la entidad, así como de las expectativas adicionales identificadas.

Los servicios identificados por Deloitte se muestran en la *fase de explotación*. Como parte de la planificación descrita en la propuesta, en la fase de diseño se podría llevar a cabo una **personalización** de dichos servicios conforme a las necesidades de CNP Assurances y la realidad existente.

ESTIMACIÓN DE CAPACIDADES

Conforme a los servicios a acometer, **se han estimado las capacidades necesarias**. Con base en dicho análisis, **Deloitte propone el equipo de trabajo** contenido en la presente oferta, el cual **se considera adecuado para garantizar la mejor prestación** del servicio solicitado.

El detalle de las capacidades solicitadas por CNP Assurances, así como las consideradas necesarias por Deloitte se detallan en el apartado *" Planificación y Equipo de trabajo"*.



Descripción del servicio
Oficina de Seguridad | Diseño del servicio

RESULTADOS ESPERADOS

Como resultado de la fase de diseño se deberá de haber obtenido un conocimiento adecuado de cómo CNP Assurances ejecuta actualmente las tareas a incluir en la Oficina Técnica de Seguridad, así como la especificación de nuevos requerimientos de CNP Assurances en relación al servicio a prestar.

Asimismo, fruto de esta fase se deberá de ser capaz de prestar el servicio actual de cara a su mejora progresiva en fases posteriores. Para ello se habrán documentado:

- **Requisitos cubiertos** por CNP Assurances actualmente que deberán ser asumidos y ejecutados por la Oficina Técnica de Seguridad.
- **Requisitos adicionales** propuestos en las actividades del servicio como parte de la propuesta y que deberán ser integrados en la Oficina Técnica de Seguridad. Para ello se definirán los modelos de integración junto con el equipo de CNP Assurances en la fase de arranque del servicio.
- **Transferencia del conocimiento** actual de CNP Assurances en la ejecución de tareas que pasarán a ser ejecutadas por Deloitte.

Deloitte ha evaluado su capacidad para poder ofrecer a CNP Assurances el servicio planteado, considerando que se dispone de los perfiles y capacidades idóneos para el mismo, así como de herramientas de valor añadido que se pondrán a disposición del Servicio.

En la fase de diseño, debe asegurarse la correcta adquisición del conocimiento técnico/funcional de las tareas ejecutadas actualmente por CNP Assurances, y el contraste de los requisitos demandados en relación a los identificados.

Descripción del servicio
Oficina de Seguridad | Explotación del servicio

Deloitte propone, como parte del servicio, establecer una Oficina Técnica de Seguridad que permita a la entidad disponer de un soporte en materia de Ciberseguridad y Seguridad de la Información

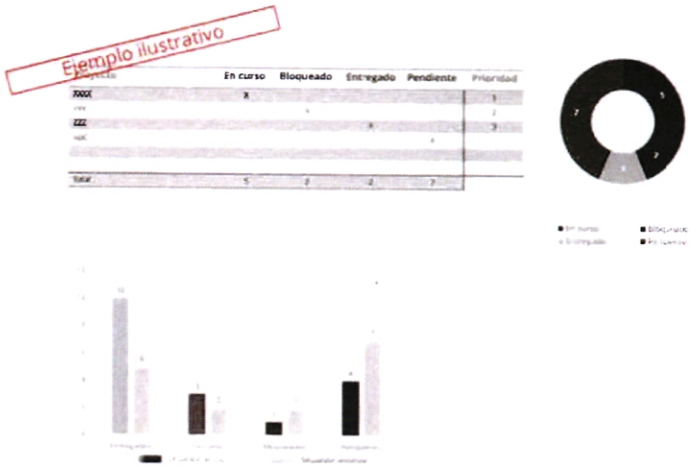
En base a este objetivo, se han definido un conjunto de tareas potenciales que se proponen a continuación, de forma que se pueda realizar el asesoramiento y colaboración circunscrito al ámbito de seguridad de la información.

Como parte del servicio se realizarán parte de estas tareas u otras similares que puedan acometerse dentro de la capacidad planificada para el servicio.

Ejemplos de potenciales tareas a realizar como parte de la colaboración

Seguimiento del cumplimiento Planes de Acción

- Elaboración de un documento ofimático para el seguimiento de los planes de acción que permita realizar un seguimiento adecuado sobre la evolución del cumplimiento.
- Elaboración de un cuadro de mando que permita realizar un adecuado reporting de la situación de los planes de acción (se propone utilizar la herramienta de Power BI Desktop).
- Seguimiento del cumplimiento de los planes y reporte periódico sobre el avance en la elaboración de acciones.



Ejemplos de potenciales tareas a realizar como parte de la colaboración

Soporte en reuniones

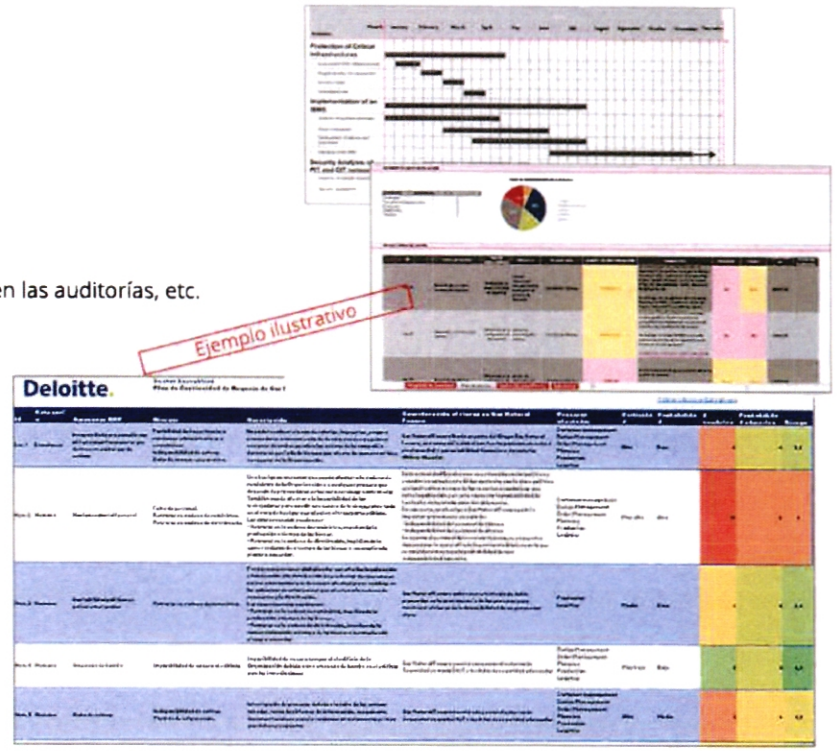
- Elaboración de presentaciones de seguimiento.
- Soporte en las reuniones a los Comités.

Actualización o correcciones referentes al SGSI y SGCN

- Soporte en la actualización del cuerpo normativo de seguridad
- Soporte en la medición de objetivos e indicadores propios de los sistemas de gestión
- Soporte en la elaboración y corrección de hallazgos y oportunidades de mejora detectadas en las auditorías, etc.
- ...

Soporte general

- Soporte adicional al Responsable de Seguridad en tareas asociadas al ámbito de Seguridad de la Información que deberán detallarse como parte del proyecto, como por ejemplo:
  - Asesoramiento sobre nuevas normativas de seguridad desde un punto de vista técnico.
  - Elaboración de presentaciones a demanda
  - Elaboración de documentos relativos a la seguridad de la información



Descripción del servicio
Oficina de Seguridad | Explotación del servicio | Aspectos clave de éxito

Uno de los aspectos de mayor importancia tenidos en cuenta por Deloitte es elaborar entregables que estén formal y correctamente realizados, de forma que el intercambio con los organismos oficiales o auditores sea lo más adecuado posible:

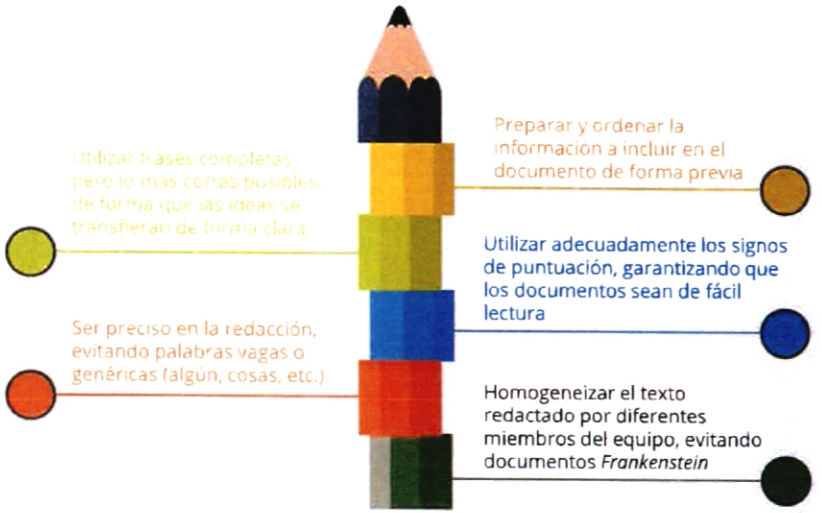
Formalización y revisión de entregables

Deloitte garantiza y pone hincapié en la relevancia de establecer mecanismos para garantizar una excelente redacción y sin errores.

Para ello, Deloitte utiliza los siguientes mecanismos

- Perfiles del área de *Cyber Strategy* encargados de la actualización de los documentos. Estos perfiles tienen un alto conocimiento técnico, pero disponen de unas habilidades muy avanzadas en redacción y elaboración de documentación.
- Los documentos serán realizados por estos perfiles, y serán revisados por parte de un equipo independiente, del gerente responsable y del gerente encargado de garantizar la calidad del trabajo. Los mismos serán:
  - Equipo independiente de revisión de los documentos.
  - Service Delivery Manager del área de *Cyber Strategy*, encargado de garantizar la calidad en los trabajos de ciberseguridad.

Claves de Deloitte en la redacción de los documentos por parte de los perfiles de *Cyber Strategy*



Descripción del servicio
Oficina de Seguridad | Retorno del servicio

CONOCIMIENTO

La información relevante debe ser documentada y compartida de manera permanente entre el equipo del servicio de Deloitte y CNP Assurances para asegurar una adecuada actualización del estado de situación de manera constante.

DOCUMENTACIÓN

Toda documentación generada por el servicio que se considere parte de un entregable o documentación de soporte para la gestión ha de estar accesible, organizada eficientemente y con capacidad de ser explotada.

COMUNICACIÓN

Se han de establecer mecanismos para garantizar que la información relevante es comunicada y conocida por todos los implicados.

La comunicación se considera un aspecto fundamental para garantizar la independencia del proveedor, facilitando a CNP Assurances el control final del servicio y la toma de decisiones relevantes.

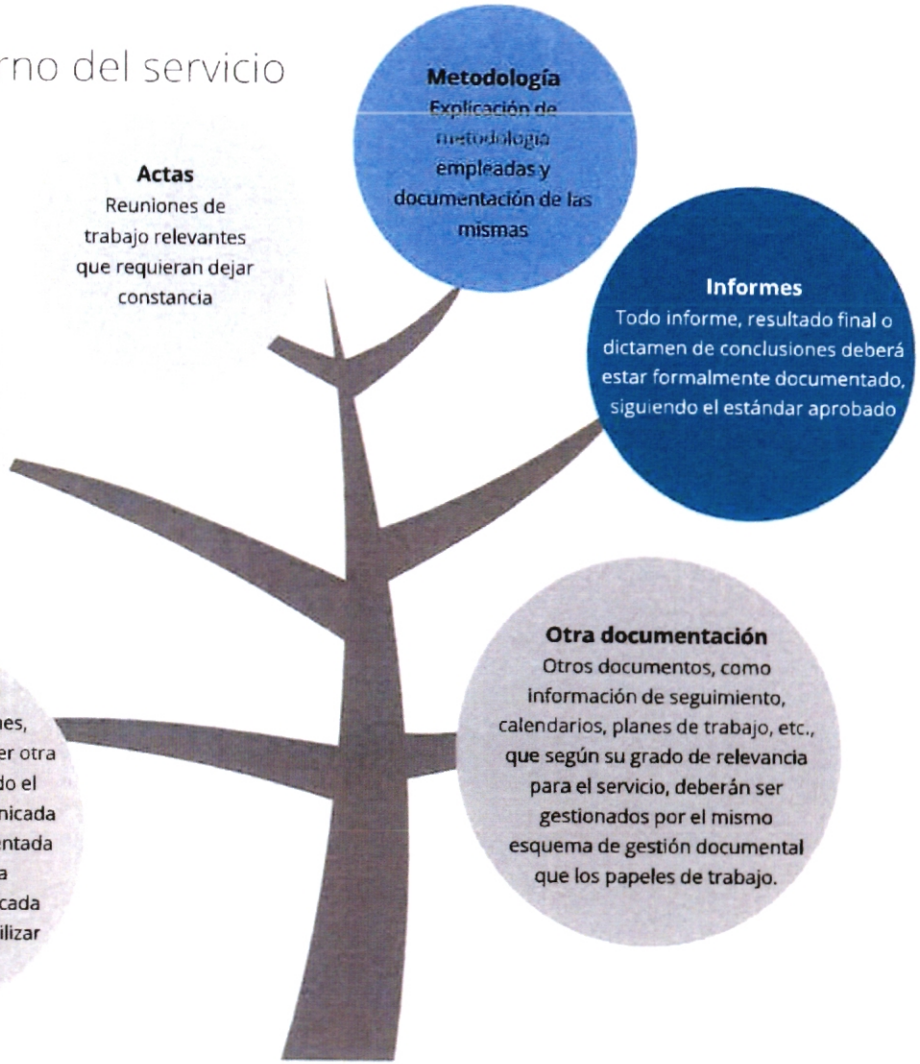
HERRAMIENTAS

Tanto en el retorno como en la mejora en la eficiencia del servicio, éste debe proporcionar medios eficientes para facilitar la gestión y transferencia del conocimiento.

Desde Deloitte, se considera fundamental ayudar a CNP Assurances en la creación de herramientas que agilicen los tiempos de respuesta, calidad de reportes y transparencia. El compromiso de Deloitte con esta tarea será máximo para, en el retorno del servicio, facilitar a CNP Assurances estas herramientas.

Descripción del servicio

Oficina de Seguridad | Retorno del servicio



A lo largo del servicio, toda la información relevante deberá ser documentada y trasladada a CNP Assurances, bien en el momento, o bien empleando las herramientas acordadas para la gestión de la documentación y transferencia del conocimiento.

Descripción del servicio
Ejemplos de iniciativas

Descripción de los servicios ofertados

Revisión, mantenimiento y mejora continua de la ciberseguridad

Las siguientes actividades son ejemplos de acciones comúnmente realizadas en este tipo de servicios, si bien las mismas se concretarán como parte de la propia operación, quedando englobadas en actividades relacionadas con el alcance de los servicios definidos en la presente propuesta y de acuerdo al plan definido al comienzo del servicio

Objetivos

El objetivo de este proyecto es potenciar las capacidades de la entidad para dar respuesta a las actividades que permitan establecer una mejora continua de la ciberseguridad.

Esto facilitará al área el seguimiento de todos los proyectos de seguridad gestionados, identificando posibles desviaciones y oportunidades de mejora que faciliten cumplir con la estrategia de ciberseguridad.

Palancas de Deloitte

Conocimiento rápido de la organización gracias a la evaluación del diagnóstico de seguridad que se realizará inicialmente.

Experiencia en la gestión y seguimiento de proyectos de seguridad de las diferentes líneas en diferentes Oficinas Técnicas de Seguridad y PMOs.

Red internacional con un profundo conocimiento del sector, la normativa de seguridad, las últimas tendencias, etc.

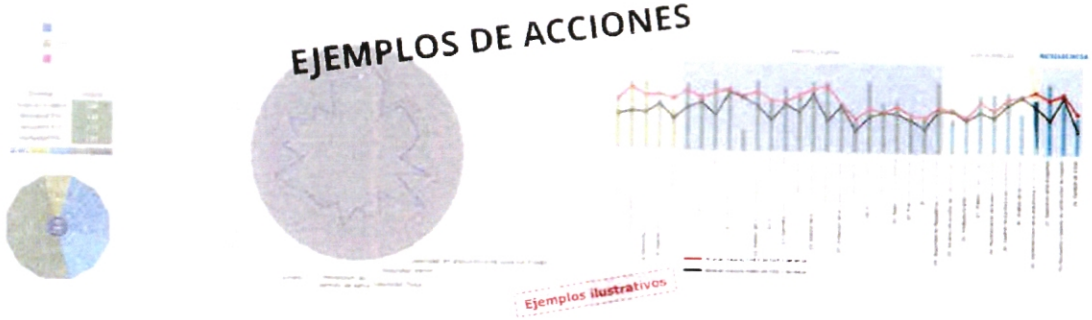
Experiencia en proyectos de levantamiento de riesgos y definición de requisitos de seguridad de diferentes tipologías.

Ejemplos de tareas

- Identificar, en función del trabajo realizado, aquellos puntos que requieren un mantenimiento de la normativa de seguridad.
- Seguimiento de proyectos gestionados por el servicio e identificación de desviaciones.
- Seguimiento y dinamización de planes de acción de ciberseguridad y peticiones de otras áreas.
- Seguimiento y reporte de los indicadores de ciberseguridad (relacionado con la elaboración de cuadros de mando).
- Revisión de requisitos de seguridad definidos y adecuación a riesgos actuales de la compañía.
- Identificar oportunidades de mejora en materia de ciberseguridad.
- Revisar el nivel de madurez de la entidad en base al Plan Director de Ciberseguridad una vez esté definido.

Ejemplos de resultados

- Reportes periódicos de seguimiento de proyectos gestionados por el Servicio, y auditorías bajo el scope, junto a la identificación de desviaciones.
- Actualización periódica del nivel de madurez de seguridad en función de los proyectos ejecutados en el Servicio, lo que permitirá conocer el nivel de riesgo de la compañía.
- Reportes de indicadores, junto a oportunidades o acciones a acometer en función de los mismos.



Descripción de los servicios ofertados

Cuerpo normativo de seguridad

Objetivos

El objetivo de este proyecto es mantener un cuerpo normativo de seguridad completo para gestionar los procesos de ciberseguridad de la compañía.

Esto permitirá a la entidad disponer de unas directrices actualizadas a las últimas tendencias y requisitos regulatorios, asignando las responsabilidades correspondientes, y facilitando el reporting del nivel de cumplimiento de dicho Cuerpo Normativo.

Palancas de Deloitte

Conocimiento de la normativa de ciberseguridad aplicable a la entidad, así como la criticidad de algunas de ellas en el sector en el que ejecuta su actividad.

Red internacional con un profundo conocimiento de la normativa de seguridad, teniendo además a disposición herramientas colaborativas para la compartición de normativa e información de seguridad.

Experiencia en proyectos de adaptación y revisión de cuerpos normativos de seguridad, tanto a nivel proyecto independiente, como formando parte de Oficinas Técnicas de Seguridad.

Expertos multidisciplinares en materia de normativa, tanto de Risk Advisory IT y Ciberseguridad, lo que facilita una visión transversal de dicho Cuerpo Normativo.

Ejemplos de tareas

- Revisar periódicamente el Cuerpo Normativo de Seguridad, e identificar aspectos a acometer para definir unos procedimientos que cumplan con los requisitos de seguridad y los procesos de la entidad, detallando, por ejemplo:
  - Descripción de actividades de ciberseguridad controles existentes para asegurar el cumplimiento de las directrices de la política
  - Mecanismos o herramientas de soporte utilizadas
  - Matriz RACI de cada una de las actividades contempladas
  - Listado de indicadores asociados al procedimiento.

Ejemplos de resultados

- Cuerpo Normativo de Seguridad actualizado, adaptado al entorno actual de la entidad y a la normativa aplicable.
- Relación de indicadores asociados al Cuerpo Normativo de Seguridad que permitan medir el cumplimiento del mismo.

Descripción de los servicios ofertados

Cuadro de mando de seguridad

Objetivos

El objetivo de este proyecto es reforzar el gobierno de la ciberseguridad en la entidad, haciendo más eficiente la identificación de información realmente importante para la organización en su toma de decisiones.

Para ello, Deloitte identificará aquellos indicadores más significativos para la entidad desde diferentes perspectivas (estratégica, económica, cumplimiento, etc.), y elaborará un cuadro de mando visual y fácil de gestionar.

Palancas de Deloitte

Experiencia en la elaboración de cuadros de mando interactivos en herramientas que permiten explotar la información de forma instantánea y visual (por ejemplo, Qlik Sense).

Profunda experiencia en el reporte a todos los niveles, desde la alta dirección a los operadores de seguridad, identificando la información necesaria para cada colectivo en diferentes perspectivas: estratégica, económica, de seguridad, normativa, externa e interna.

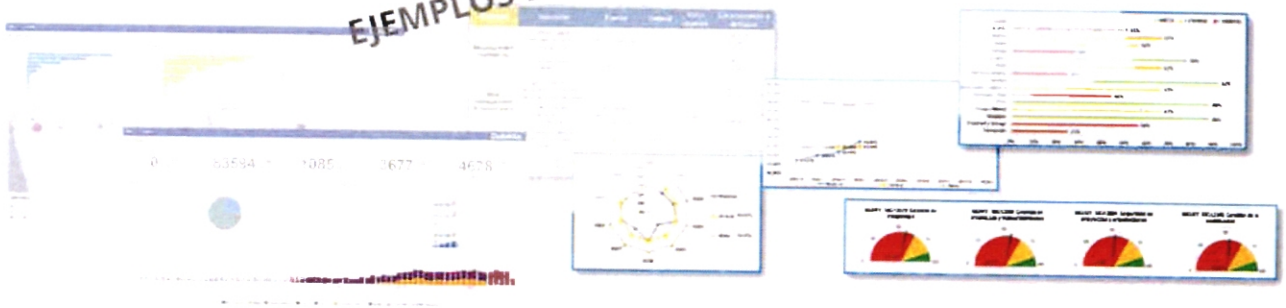
Conocimiento del las últimas tendencias en modelos de reporting, lo que facilita a Deloitte una adaptación progresiva con lo que en función de la situación actual de la entidad.

Ejemplos de tareas

- Definición y reporte periódico de un cuadro de mando que englobe todos los aspectos de la ciberseguridad en la entidad:
  - Elaboración de un catálogo de indicadores de cumplimiento que cubran todos los dominios descritos en la política de ciberseguridad, incluyendo los que ya se encuentran definidos.
  - Definición de criterios de medición, incluyendo la periodicidad, y cumplimiento objetivos para cada uno de los indicadores.
  - Establecimiento de responsabilidades de medición y revisión de cada uno de los indicadores
  - Preparación de una herramienta de soporte para los indicadores que permita obtener el nivel de cumplimiento de cada uno de ellos.
  - Elaboración de una plantilla para el reporte periódico de cumplimiento de los indicadores.

Ejemplos de resultados

- Listado de indicadores a incorporar en el cuadro de mandos de ciberseguridad.
- Plantilla de cuadro de mando para facilitar el reporte periódico para el seguimiento de los indicadores
- Propuesta de automatización de la generación de cuadro de mando interactivo (tipo Qlik Sense, o similar).
- Metodología y procedimientos para la extracción de información a incorporar en los cuadros de mando periódicos.
- Extracción de información y generación de indicadores periódicos [illegible] ación de las necesidades de reporting a Comités.



Descripción de los servicios ofertados

Coordinación y reporte a Comités

Objetivos

El objetivo de este proyecto es la formalización de un reporting a Comités en materia de ciberseguridad periódico que realice una revisión del estado de la ciberseguridad en la entidad.

En estos Comités, se deben tratar los diferentes aspectos relativos a ciberseguridad, y se apoyarán también en información proporcionada por el resto de proyectos gestionados por el Servicio.

Palancas de Deloitte

Experiencia en la adaptación de modelos de gobierno de seguridad, identificando las necesidades que deben ser implementadas y la forma en la que se debe realizar dicha adaptación.

Conocimiento de los mejores estándares en lo referente a reportes a Comités de Seguridad, de forma que pueda tomar como fuente de información los cuadros de mando para facilitar una toma de decisiones ágil.

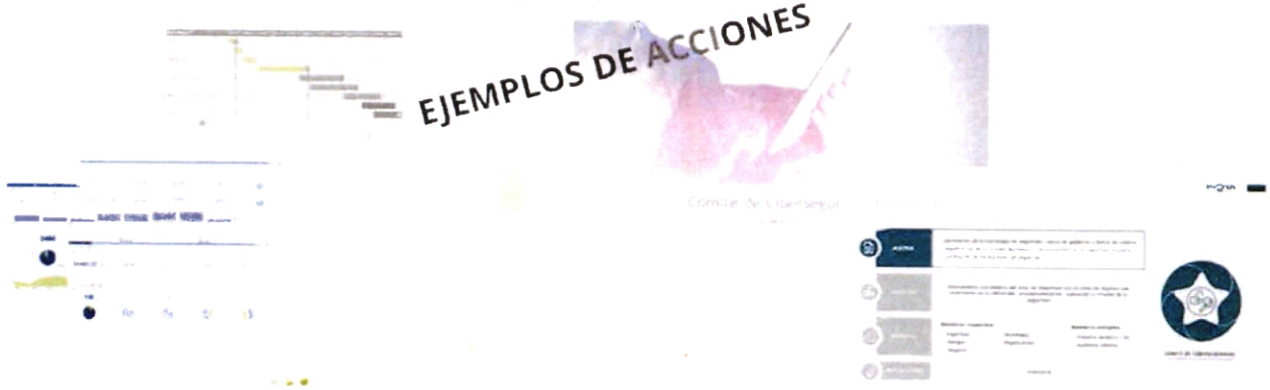
Adquisición rápida del conocimiento de la organización, lo que permite identificar aquellas figuras que son susceptibles de ser miembros (o participar ocasionalmente), en los Comités.

Ejemplos de tareas

- Ampliar las funciones y puntos de revisión de los Comités en materia de ciberseguridad, incluyendo temas como, por ejemplo:
  - Revisión de cambios en la organización o su entorno que afecten a la ciberseguridad
  - Aprobación y revisión de normativa de ciberseguridad así como autorización de excepciones a la misma
  - Estado de cumplimiento de indicadores y objetivos de ciberseguridad
  - Seguimiento de planes de acción y proyectos de ciberseguridad
  - Resultados del análisis de riesgos de ciberseguridad
  - Estado de las diferentes acciones formativas en materia de ciberseguridad
- Establecer los modelos de presentación y documentación soporte a utilizar en los Comités en materia de ciberseguridad.
- Recopilar la información necesaria a incluir en cada Comité en materia de ciberseguridad.
- Elaborar los contenidos de ciberseguridad a incluir en las presentaciones a utilizar en cada Comité.

ejemplos de resultados

- Modelos de presentación adaptados en materia de ciberseguridad para los Comités
- Información recopilada a tratar en cada Comité
- Presentaciones de soporte en materia de ciberseguridad para cada Comité



Descripción de los servicios ofertados

Soporte normativa de seguridad y estándares

Las siguientes actividades son ejemplos de acciones comúnmente realizadas en este tipo de servicios, si bien las mismas se concretarán como parte de la propia operación, quedando englobadas en actividades relacionadas con el alcance de los servicios definidos en la presente propuesta y de acuerdo al plan definido al comienzo del servicio.

Objetivos

El objetivo de esta actividad es potenciar las capacidades de la entidad para la supervisión y seguimiento de las acciones de seguridad relativas a normativas y estándares

Esto facilitará a la entidad tener un control sobre el cumplimiento de ambas normativas, identificando potenciales desviaciones respecto al mismo y definiendo acciones que será necesario acometer.

Palancas de Deloitte

Conocimiento multidisciplinar en Deloitte, que dispone de perfiles de Risk Advisory que también podrán servir de apoyo y consulta por parte del equipo para la resolución de aspectos más relacionados con requisitos regulatorios no de seguridad.

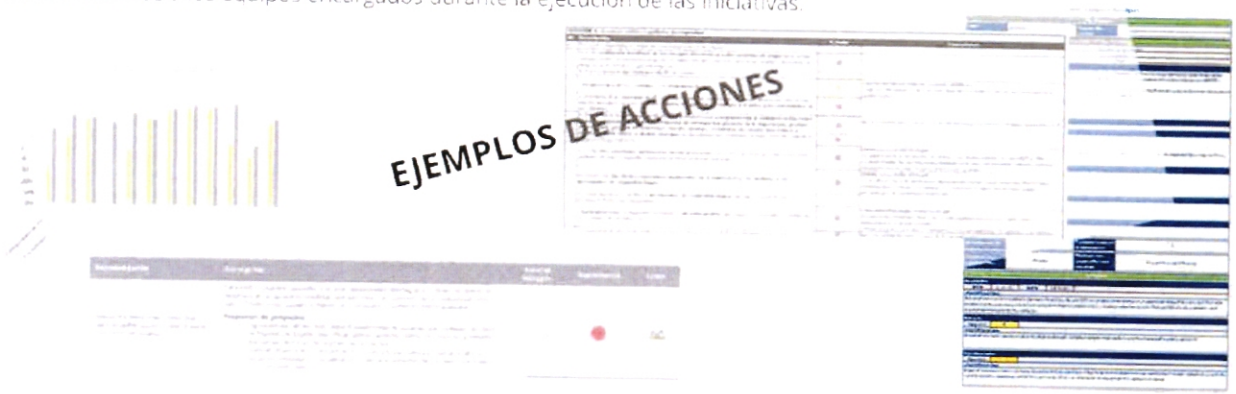
Experiencia en proyectos de adaptación de medidas de seguridad asociadas a normativas, que nos permiten conocer las dificultades a las que se enfrentan las entidades.

Ejemplos de tareas

- Identificar las acciones actualmente definidas en la entidad para la adaptación, y el seguimiento del nivel de cumplimiento en materia de seguridad en lo referente a las normativas como GDPR o estándares como NIST o ISO 27001.
- Dar seguimiento en la ejecución de acciones planificadas a corto plazo.
- Propuesta de ajuste de acciones a realizar a medio-largo plazo.
- Liderazgo de las mismas, identificando acciones e iniciativas que deban ejecutarse en la entidad para adecuarse a las normativas.
- Seguimiento de las iniciativas lanzadas, identificando potenciales desviaciones sobre el plan.
- Asesoramiento específico en materia de seguridad en la ejecución de las iniciativas por parte de los equipos asignados.

Ejemplos de resultados

- Planificación de acciones a realizar para dar seguimiento, e incrementar, el nivel de cumplimiento de GDPR o ISO27001
- Desviaciones identificadas sobre las planificaciones estimadas de iniciativas para la adaptación.
- Dudas resueltas a los equipos encargados durante la ejecución de las iniciativas.



Descripción de los servicios ofertados

Gestión de incidentes de seguridad

Objetivos

El objetivo de esta actividad es coordinar las acciones a realizar por parte de la entidad en caso de incidente de seguridad.

Esta tarea facilitará una rápida gestión de las acciones y anticiparse a las mismas de cara a que puedan realizarse las acciones más prioritarias que controlen el impacto del incidente.

Ejemplos de tareas

- Identificar el procedimiento de gestión de incidentes de seguridad.
- Mantener actualizado el mismo en función de la situación actual y los pasos que deben darse.
- Coordinar las acciones de acuerdo al procedimiento en función del procedimiento definido.
- Dar seguimiento a las acciones que deben realizarse por parte de cada uno de los involucrados en la entidad.
- Reportar el seguimiento de las acciones a realizar para controlar el incidente.
- Realizar un informe de los resultados producidos por el incidente.

Palancas de Deloitte

Experiencia en la definición de procedimientos para gestión de incidentes de seguridad.

Experiencia en la gestión de incidentes desde un punto de coordinación y también desde la propia **resolución de los mismos,** lo que nos hace conocedores de las principales dificultades a las que se enfrenta la entidad.

Amplia experiencia en ejecución de proyectos de simulaciones de crisis, lo que nos permite conocer de primera mano las reacciones de la alta dirección frente a un ciberincidente, sabiendo identificar los reportes que es necesario realizar y la gestión de los comunicados.

Ejemplos de resultados

- Procedimiento de gestión de incidentes actualizado.
- Seguimiento de acciones en caso de incidentes.
- Informe de resultados y lecciones aprendidas tras la ejecución del incidente.

EJEMPLOS DE ACCIONES

Prevención

Cierre, resumen y aprendizaje

Descripción de los servicios ofertados

Soporte y supervisión de vulnerabilidades e incidencias SOC

Objetivos

El objetivo de esta actividad es dar soporte a la entidad en la supervisión de los proyectos y servicios que actualmente tiene la entidad de análisis de vulnerabilidades e incidencias SOC

Esto permitirá a la entidad interpretar los resultados de los trabajos desde una perspectiva estratégica que facilite la toma de decisiones sobre las acciones a tomar para solucionar potenciales vulnerabilidades, interpretar posibles anomalías en los sistemas, etc.

Palancas de Deloitte

Conocimiento rápido de la organización gracias a que ya tenemos proyectos de hacking en la propia entidad.

Experiencia en la gestión y seguimiento de acciones de forma proactiva.

Capacidad de interlocución en el ámbito técnico y de negocio que facilita ser la interfaz entre los equipos encargados de los aspectos técnicos y las áreas de negocio.

Experiencia en proyectos técnicos de hacking y SIEM dentro de Deloitte que nos permite disponer de expertos que actuarán como soporte para facilitar que el equipo conozca las últimas novedades y tendencias en la materia.

Ejemplos de tareas

- Identificar la planificación de análisis de vulnerabilidades a realizar.
- Dar seguimiento al cumplimiento de la planificación definida.
- Recopilar los resultados de los informes de realizados e interpretación de los mismos.
- Interpretación de los informes y diálogo con los equipos ejecutores para conocer las consecuencias de los resultados.
- Acciones de liderazgo para la solución de las vulnerabilidades identificadas.
- Recopilar los informes sobre eventos destacados realizados a partir del servicio de incidencias SOC.
- Interpretación de los resultados y diálogo con los equipos dedicados al manejo del SOC de cara a profundizar en las consecuencias.
- Seguimiento de la resolución de eventos, incidencias y vulnerabilidades.
- Reporting sobre aquellas incidencias destacables y lanzamiento/seguimiento de acciones para solucionar las mismas.

Ejemplos de resultados

- Interpretaciones de los informes sobre análisis realizados.
- Interpretaciones de los resultados derivados de los eventos identificados por parte del servicio de SIEM.
- Levantamiento y reporting de vulnerabilidades y eventos críticos que sea necesario elevar en la propia entidad.
- Liderazgo y seguimiento de acciones para solucionar las vulnerabilidades y eventos detectados.

Descripción de los servicios ofertados

Seguridad en Proyectos

Objetivos

El objetivo de esta actividad es incorporar la seguridad desde una fase temprana de los proyectos, suponiendo un ahorro de costes al minimizar el riesgo y la necesidad de correcciones de vulnerabilidades de los productos en producción.

Esto facilitará a la entidad la reducción de vulnerabilidades y contribuye a generar, fomentar y mantener una buena imagen corporativa, incrementando incluso la reputación de la propia función de TI y Seguridad de cara al resto de Áreas de Negocio.

Palancas de Deloitte

Experiencia en proyectos de establecimiento de enfoques metodológicos para el análisis de riesgos en nuevas iniciativas/soluciones y servicios que forman parte de la estrategia de transformación digital de clientes del sector financiero.

Experiencia en proyectos de levantamiento de riesgos y definición de requisitos de seguridad en **tecnología cloud, aplicaciones móviles, externalización de servicios, servicios como producto, etc.**

Experiencia en el desarrollo, implantación y uso de **herramientas de automatización** de procesos y ejecución de controles.

Catálogos de riesgos y requisitos maduros que facilitan una adaptación rápida a la casuística particular de la entidad.

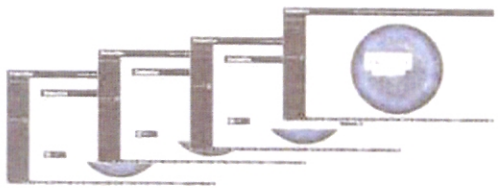
Ejemplos de tareas

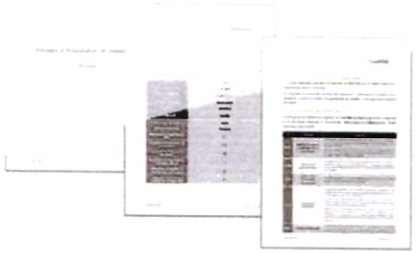
- Identificar la metodología de análisis de riesgos y de definición de requisitos actualmente utilizada.
- Identificación, análisis y actualización del catálogo de riesgos y requisitos de seguridad.
- Definición de requisitos de seguridad y/o análisis de riesgos en iniciativas de la entidad que surjan desde el ámbito técnico o relacionados con el propio negocio de la entidad.
- Soporte y seguimiento relativo a la mitigación de los riesgos detectados durante el análisis de viabilidad de la solución.
- Asesorías y consultas en materia de seguridad durante todo el ciclo de vida (relativas a implementación de requerimientos, al respecto de las guías de buenas prácticas, etc.).
- Elaboración de entregables de acuerdo a las metodologías de la entidad y actualización del inventario de iniciativas junto a los parámetros del mismo.
- Identificar posibilidades para automatizar el proceso en función del nivel de madurez de la entidad.

Ejemplos de resultados

- Propuestas de ajustes de la metodología de análisis de riesgos y de definición de requisitos (en caso de que sea necesario).
- Análisis de riesgos e identificación de requisitos ad hoc para aquellas iniciativas que, debido a su criticidad, lo requieran.
- Entregables de las iniciativas según los estándares de la entidad, entre los que se encuentran:
  - Análisis de riesgos.
  - Requisitos de Seguridad.
- Garantía de la asimilación de las medidas de seguridad a implantar por parte de las áreas, mediante un seguimiento y asesoramiento que permita resolver las dudas asociadas a la implantación de los requisitos o a la mitigación de los riesgos detectados.
- Inventario de iniciativas actualizado.
- Identificación de posibilidades para automatizar el proceso.

EJEMPLOS DE ACCIONES





Descripción de los servicios ofertados

Marcos de control

Objetivos

El incremento de la presión regulatoria a la que se está viendo sometido el entorno financiero, junto con el avance en la sofisticación de los ciberataques, hacen especialmente importante que las entidades cumplan (y vigilen el cumplimiento) de las regulaciones bajo las que están sometidas.

El objetivo de la presente actividad es mantener un marco de gobierno y control que le permita cubrir los distintos requisitos a los que se encuentra sometida.

Palancas de Deloitte

Red internacional con un profundo conocimiento del sector y la normativa de seguridad, teniendo además a disposición herramientas colaborativas para la compartición de normas e información de seguridad.

Experiencia en proyectos de definición de marcos de control, tanto a nivel proyecto, como formando parte de servicios.

Expertos multidisciplinares en materia de normativa, tanto de Risk Advisory IT y Ciberseguridad.

Conocimiento de las normativas aplicables a la entidad y su sector, al haber participado de forma activa en la definición y elaboración de marcos de controles en entidades del sector financiero, lo que facilita un rápido entendimiento de la casuística específica de cada uno de los controles.

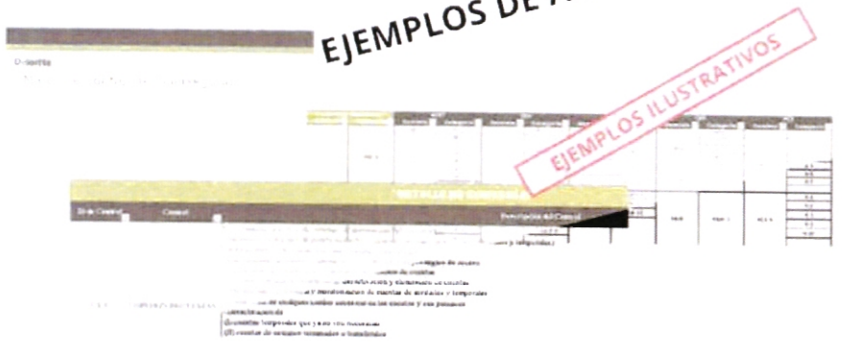
Ejemplos de tareas

- Identificar el marco de control, incluyendo aquellos controles relativos a antivirus, firewall, revisión de usuarios, etc.
- Mantener actualizado el marco de control en función de nuevos requisitos regulatorios y normativos que aparezcan.
- Proponer modificaciones en los actuales, identificando aquellos indicadores que pueden ser de especial utilidad.
- Elaborar aquellos cuadros de mando que faciliten la visualización del cumplimiento del marco de gobierno y control de la seguridad.
- Comunicar a los responsables de subsanar las debilidades de control los plazos en los que las mismas deben estar solucionadas.
- Dar seguimiento a las acciones a realizar, comunicando aquellos casos en los que no se esté cumpliendo con los plazos.
- Dar soporte mediante la resolución de dudas en aquellos aspectos de seguridad de la información y riesgos tecnológicos gestionados.

Ejemplos de resultados

- Marco de gobierno y control actualizado.
- Actualización de indicadores y/o cuadros de mando que permita conocer el nivel de cumplimiento del marco de control.
- Seguimiento de las debilidades.
- Resolución de dudas de los aspectos de seguridad de la información.

EJEMPLOS DE ACCIONES



Descripción de los servicios ofertados

Coordinación y reporte

Objetivo

El objetivo de esta actividad es la formalización del reporting periódico a Comités en materia de ciberseguridad que realice una revisión del estado de la ciberseguridad en la entidad, así como aquellos reportes mensuales que es necesario realizar a la matriz en Francia.

En estos Comités, se deben tratar los diferentes aspectos relativos a ciberseguridad, y se apoyarán también en información proporcionada por el resto de proyectos gestionados por el Servicio.

Palancas de Deloitte

Experiencia en la adaptación de modelos de gobierno de seguridad, identificando las necesidades que deben ser implementadas y la forma en la que se debe realizar dicha adaptación.

Conocimiento de los mejores estándares en lo referente a reportes a Comités de Seguridad, de forma que pueda tomar como fuente de información los cuadros de mando para facilitar una toma de decisiones ágil.

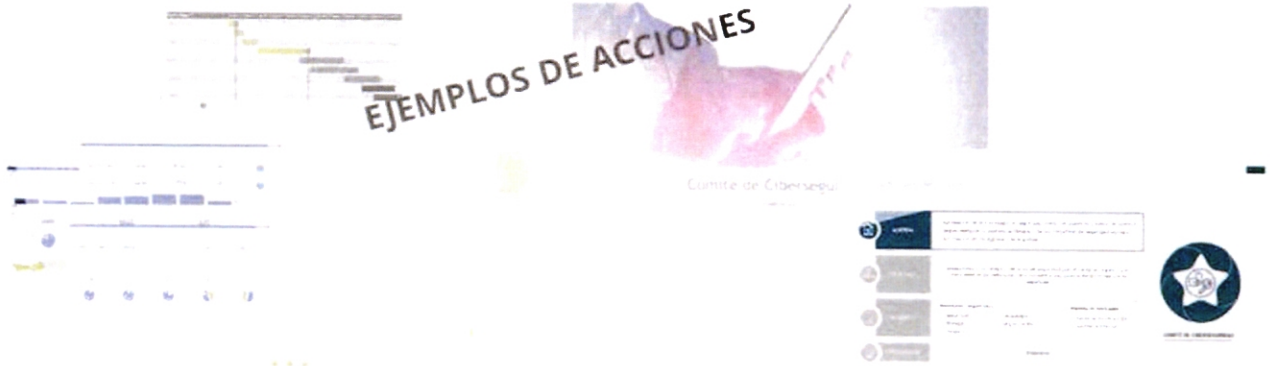
Adquisición rápida del conocimiento de la organización, lo que permite identificar aquellas figuras que son susceptibles de ser miembros (o participar ocasionalmente), en los Comités.

Ejemplos de tareas

- Identificar los reportes actualmente realizados en materia de ciberseguridad, incluidos aquellos realizados mensualmente a Francia.
- Ampliar las funciones y puntos de revisión de los reportes y Comités en materia de ciberseguridad, incluyendo temas como, por ejemplo:
  - Revisión de cambios en la organización o su entorno que afecten a la ciberseguridad
  - Aprobación y revisión de normativa de ciberseguridad así como autorización de excepciones a la misma
  - Estado de cumplimiento de indicadores y objetivos de ciberseguridad
  - Seguimiento de planes de acción y proyectos de ciberseguridad
  - Resultados del análisis de riesgos de ciberseguridad
  - Estado de las diferentes acciones formativas en materia de ciberseguridad
- Actualizar los modelos de presentación y documentación soporte a reportar en materia de ciberseguridad.
- Recopilar la información necesaria a incluir en cada reporte en materia de ciberseguridad.
- Elaborar los contenidos de ciberseguridad a incluir en las presentaciones a utilizar en cada reporte.

Ejemplos de resultados

- Modelos de presentación adaptados en materia de ciberseguridad para los distintos reportes.
- Información recopilada a tratar.
- Presentaciones de soporte en materia de ciberseguridad.



Descripción de los servicios ofertados

Concienciación de usuarios

Objetivos

La estrategia de protección de la información de cualquier organización debe incluir la adecuada preparación de sus empleados y colaboradores con acceso a los sistemas de información ante las nuevas ciberamenazas que buscan explotar el eslabón más débil dentro de la cadena de la seguridad de la información: el factor humano.

Para ello, las actividades concienciación y divulgación se deben orientar para preparar a los diferentes colectivos de trabajadores respecto a los riesgos identificados.

Palancas de Deloitte

Metodología novedosa propia de concienciación y formación en seguridad basada en los siguientes principios:

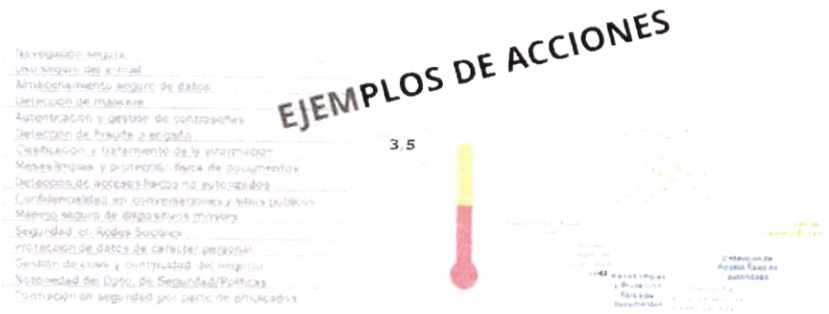
- **Medición del nivel de madurez en concienciación**. No se puede mejorar lo que no se puede medir.
- **Comparativa del nivel de madurez de la Compañía con otras compañías** similares, que ayudará a definir el nivel objetivo.
- Búsqueda de las motivaciones que hagan un cambio en el comportamiento de los empleados. Esto lo realizan perfiles especialistas en Marketing y Publicidad, mediante un **Mapa de Empatía**.
- Diseño del Plan de Concienciación incorporando **acciones eficaces en la concienciación**, y no basadas en la formación.

Ejemplos de tareas

- Identificación de colectivos para formación.
- Medición del AS-IS en concienciación, a través de cuestionarios, debilidades identificadas en las personas, etc.
- Definición de necesidades de formación y concienciación.
- Definición del TO-BE en concienciación
- Desarrollo y coordinación de material de formación y concienciación, recopilando el material que tenga actualmente la entidad y manteniéndolo actualizado.
- Ejecución y seguimiento de acciones formativas y de concienciación

Ejemplos de resultados

- Seguimiento y actualización del plan de concienciación, material asociado actualizado y ejecución de acciones de concienciación.

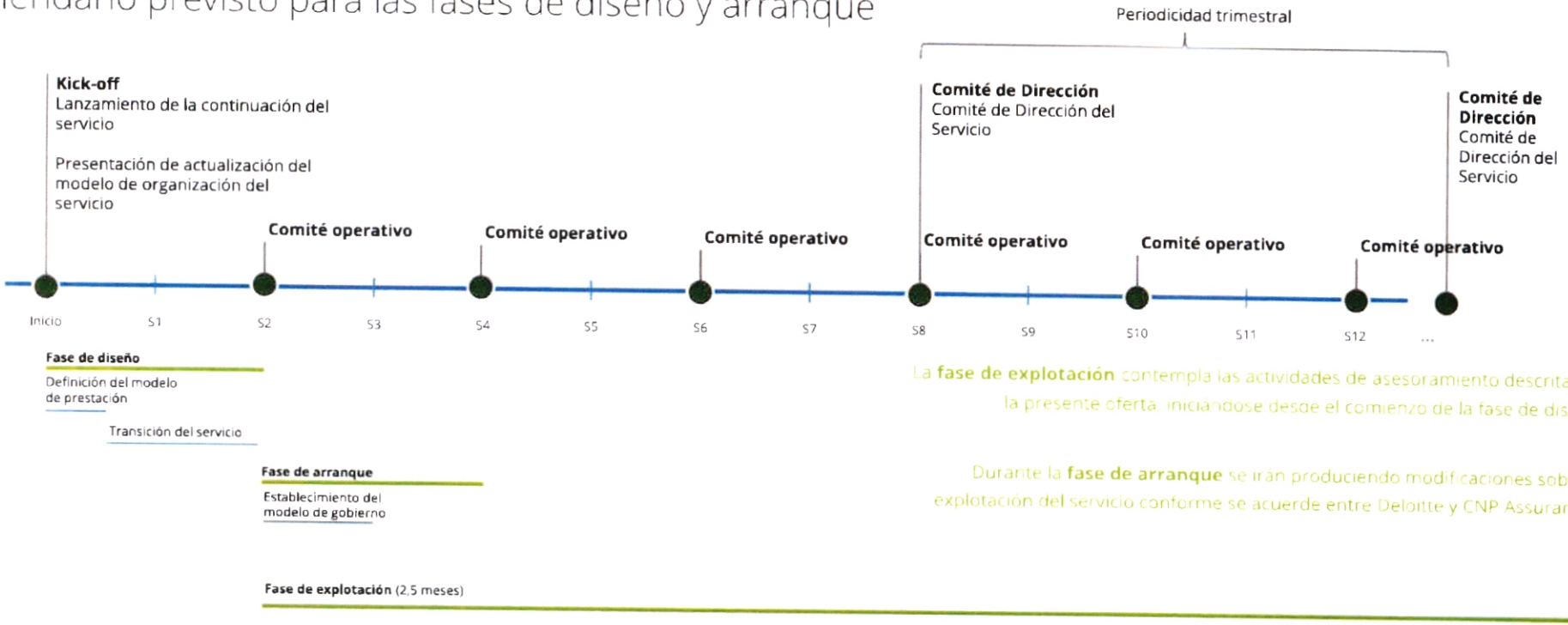


Ejemplo ilustrativo del nivel de madurez ***en concienciación de ciberseguridad***

Índice

Planificación

Calendario previsto para las fases de diseño y arranque



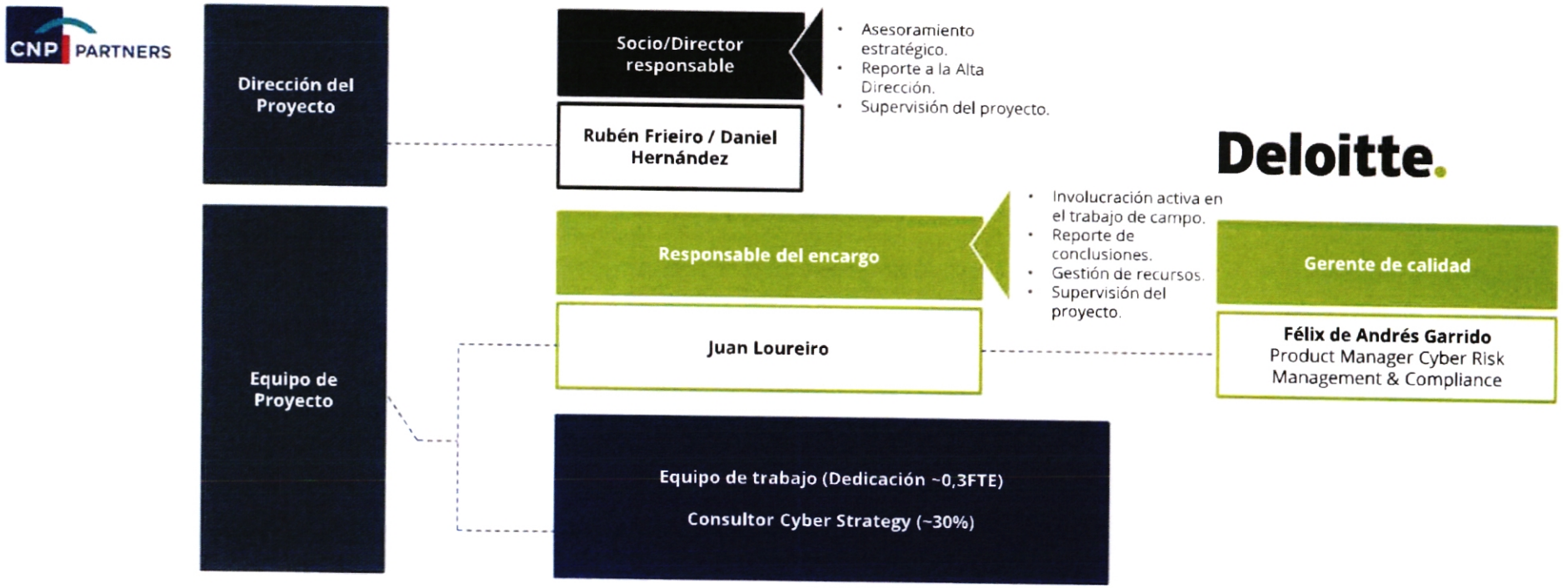
La **fase de explotación** contempla las actividades de asesoramiento descritas en la presente oferta, iniciándose desde el comienzo de la fase de diseño.

Durante la **fase de arranque** se irán produciendo modificaciones sobre la explotación del servicio conforme se acuerde entre Deloitte y CNP Assurances.

Índice

Equipo de proyecto propuesto
Modelo de relación

En base a nuestra experiencia proponemos un modelo de organización del proyecto basado en una asignación de responsabilidades y tareas de coordinación y cooperación de los equipos de trabajo de la siguiente forma:



Equipo de proyecto propuesto
Modelo de gobierno

Propuesta de establecimiento de responsabilidades

Rol	CNP Assurances	Deloitte	Descripción del rol
Responsable del contrato	Dirección de CNP Assurances	Equipo directivo Deloitte (Socio y Gerente)	CNP Assurances asume la dirección del servicio con el asesoramiento de Deloitte, tanto desde el punto de vista técnico como administrativo del contrato, con las actividades descritas en el pliego de contratación.
Gestor del Servicio	Responsable del Servicio	Gestor del servicio de Deloitte	Asumen la gestión operativa del servicio, de su seguimiento periódico y la mejora continua del mismo. Tiene por objeto evaluar la calidad del asesoramiento ofrecido.
Equipo de trabajo	Equipo de trabajo	Equipo de trabajo	Es el encargado de la prestación del servicio, de acuerdo a las actividades descritas.

Implicación

Se dispondrá de un equipo de trabajo, de los cuales uno de ellos realizará las tareas de gestión del servicio. Asimismo, el Responsable del Contrato y Deloitte se comprometen a implicarse en la correcta prestación del servicio, en la subsanación temprana de ineficiencias, y en la participación activa en comités y tareas que requiera y demande CNP Assurances.

Comités

Si bien se definirán comités periódicos, Deloitte se compromete a adaptarse a las necesidades concretas de CNP Assurances en la realización de Comités y reuniones.

Perfiles

Cada uno de los perfiles dispondrá de skills concretos potenciados en ciertas disciplinas como parte del servicio. Entre las habilidades identificadas se encuentran el conocimiento de la normativa, ciberriesgos, seguridad y modelos de gobierno. En este sentido, todos los miembros tendrán skills que permitan asumir el balanceo de carga en caso de necesidad, teniendo proactividad en la realización de las tareas y trato con los interlocutores de la entidad..

Procesos de gestión

Como parte del servicio, Deloitte hará un repaso a los procesos existentes de gestión del servicio y explotación de actividades para su adaptación a las actividades y necesidades de CNP Assurances.

Equipo de proyecto propuesto
Modelo de gobierno

Como parte del modelo de Gobierno, se contará Comités para asegurar el control y seguimiento del servicio de manera formalizada, donde se llevará a cabo el seguimiento de la actividad, indicadores, niveles de servicio establecidos, toma de decisiones asociadas a la gestión del servicio, etc.

Propuesta de comités internos del servicio

Comité	Asistentes	Descripción
Comité de dirección	Responsables del contrato y gestores del servicio	CNP Assurances coordina y desarrolla las actividades previstas para los responsables del contrato con el asesoramiento de Deloitte con la finalidad de analizar la calidad percibida del servicio, evaluar las necesidades de mejora en la prestación del mismo.
Comité operativo	Responsable del servicio de CNP Assurances, responsable de la ejecución de Deloitte, gerente responsable de Deloitte	En dicho Comité se abordará el estado actual de las acciones, el avance, los problemas existentes y la resolución de incidencias que pudieran ocurrir en las tareas.
Comité de calidad	Equipo directivo Deloitte y gestor del servicio	Coordinar y desarrollar de manera conjunta las actividades relacionadas con la gestión de la calidad del proyecto, teniendo en cuenta el manual de calidad de Deloitte. Este comité será interno del proveedor.

Equipo de proyecto propuesto
Roles y responsabilidades

Roles	Responsabilidades	Dedicación
Socio responsable	• Interlocución de Alto nivel, máximos responsables de la correcta ejecución del proyecto • Conocimiento de la cuenta y aportación de experiencia en proyectos similares • Revisión de calidad de los entregables de proyecto	Part Time
Responsable del encargo	• Gestión del equipo, distribución de tareas, reporte y revisión de la calidad de los entregables del proyecto • Soporte y seguimiento continuo de las necesidades	Part Time
Gerente de Calidad	• Aseguramiento de la calidad y provisión de recursos especializados • Gestión del equipo, distribución de tareas, reporte y revisión de la calidad de los entregables del proyecto • Soporte y seguimiento continuo de las necesidades	Part Time
Equipo de trabajo	• Llevar a cabo las tareas definidas en la presente propuesta.	Full time

Equipo de proyecto propuesto

Currículums | Socio del encargo

Rubén Frieiro Barros

Socio del proyecto

22 años de experiencia

rfrieiro@deloitte.es

Descripción

Trayectoria profesional

- Rubén se incorporó a Deloitte en 1999, como consultor del grupo de gestión de riesgos tecnológicos, encargado de la ejecución y dirección técnica de diferentes encargos de control interno y auditoría informática y consultoría sobre seguridad de la información.
- En 2005, es nombrado gerente del grupo Risk Advisory IT, con competencias en el desarrollo de servicios en el sector financiero (Seguros y Banca), experto en las áreas de Seguridad de la Información, Cumplimiento Normativo y Auditoría de Sistemas.
- En el 2015 es promocionado a Socio del grupo de Riesgos Tecnológicos, en las áreas de especialización de Auditoría Informática y Ciberseguridad.
- A lo largo de su trayectoria profesional ha colaborado en numerosas iniciativas sectoriales, como asesor del Centro Nacional de Protección de Infraestructuras Críticas para el desarrollo de los Planes Estratégicos Sectoriales de Protección de Infraestructuras Críticas.
- En la actualidad es miembro de la Comisión de Innovación y Tecnología del Instituto de Censores Jurados de Cuentas.

Formación académica y titulaciones

- Ingeniero de Telecomunicaciones por la Universidad de Vigo.
- Experto Universitario en Dirección de Seguridad por la UNED.
- CISA (Certified Information Systems Auditor).
- CISM (Certified Information Security Manager).
- CISSP (Certified Information Systems Security Professional).
- CSSLP (Certified Security Software Lifecycle Professional).
- CRISC (Certified in Risk and Information Systems Control).
- ISO 27001 Lead Auditor.
- ITIL Foundations V3.

Otros datos de interés profesional

- Profesor en el Master de Auditoría Informática de la Universidad Politécnica de Madrid en los años, 2003, 2004, 2005, 2006, 2011, 2012.
- Profesor en el Master de Dirección y Gestión de la Seguridad de la Información de la Universidad Politécnica de Madrid en los años, 2012, 2013 y 2014.
- Profesor en el master de Ciberseguridad de la Universidad Carlos III de Madrid, año 2015.
- Experto colaborador en el diseño del plan de estudios del master de Ciberseguridad de la UC3M.
- Miembro del Colegio Oficial de Ingenieros de Telecomunicaciones.
- Idiomas: Español, Gallego, Inglés.

Principales proyectos

- Revisiones de controles generales del ordenador y de la realización de pruebas de datos.
- Servicios de riesgos tecnológicos en el sector servicios y medios de pago.
- Consultoría de seguridad de la información.
- Elaboración de planes directores de seguridad, adaptaciones a la LOPD, la implantación de planes de continuidad de negocio, revisiones de seguridad y hacking ético, planes de protección de la información, concienciación en seguridad o implementación de sistemas de gestión dela seguridad.
- Implantación de herramientas para la gestión del cumplimiento normativo, integridad de la información y calidad de datos.

Principales clientes

- MAPFRE
- Banco de España
- Inditex
- Arcelor Mittal
- Ferrovial

Equipo de proyecto propuesto

Currículums | Director de la práctica Cyber en sector asegurador

Descripción

Trayectoria profesional

- Director de IT Risk Advisory y Cyber Risk, se incorporó al grupo en el año 2019, aportando una gran especialización en proyectos de transformación, estrategia y ciberseguridad, principalmente en el sector financiero y asegurador.
- Director responsable de la práctica de ciberseguridad en el sector asegurador.

Formación académica y titulaciones

- Ingeniero Superior en Informática
- Licenciado en Administración y Dirección de Empresas
- Máster Executive en IT Governance & Audit
- Programa Experto en Planificación Financiera y Control de Gestión
- Programa Experto en Dirección Estratégica Aseguradora
- Certificaciones:
  - CISA
  - ITIL Foundation v3
  - ISO 22301 Lead Auditor

Otros datos de interés profesional

- Experiencia en dirección de proyectos internacionales con equipos multidisciplinares basados en diferentes países
- Experiencia en reporte a Comité de Dirección y Consejo de Administración
- Experiencia en Oficinas de Proyectos y de Transformación a nivel estratégico
- Colaborador habitual de ICEA
- Idiomas: castellano e inglés

Principales proyectos

- Elaboración de Planes Directores de Sistemas a 3 años en entornos internacionales
- Elaboración de Planes de Transformación Digital para el sector asegurador
- Elaboración de Planes Directores de Seguridad en baca y seguros
- Definición e implementación de modelos organizativos de TI
- Dirección de departamentos de Gobierno de TI en seguros
- Auditorías Financiera, SOX y de Sistemas en entidades cotizadas en Banca y Seguros
- Implantación y revisión de Sistemas de Gestión de la Continuidad de Negocio
- Adaptación y auditorías del cumplimiento por parte de proveedores y clientes del reglamento de medidas asociado a la Ley Orgánica de Protección de Datos (LOPD) y al GDPR.
- Dirección de Oficinas de Transformación y Oficinas de proyectos, tanto del Plan Estratégico Corporativo como de Proyectos de Tecnología
- Dirección de proyectos de integración de funciones de IT tras operaciones corporativas (M&A), tanto en Banca como en Seguros
- Diseño e implementación de cuadros de mando para la Función de TI
- Diseño e implementación del Modelo de Gobierno y Estructuras de Comités dentro de la función de TI
- Diseño funcional de herramientas PPM para la gestión del portfolio y optimización de los recursos
- Definición e implementación de Oficinas de Proveedores de TI
- Definición e implantación de Oficinas de Gestión Financiera de TI

Principales clientes

Seguros:

- Pelayo
- CNP
- Caser Seguros
- Catalana Occidente
- CNP Assurances
- AXA
- Ocaso
- MAPFRE
- SegurCaixa Adeslas
- Mutua Madrileña
- VidaCaixa
- BBVA Seguros
- ICEA

Banca:

- BBVA
- Banco Popular
- Banesto
- BMN
- Bancaja

Daniel Hernández Arroyo

Director Cyber en Seguros
17 años de experiencia

dhernandezarroyo@deloitte.es
+34 911 57 74 79

Director del encargo

Equipo de proyecto propuesto

Currículums | Account Manager responsable del encargo

Descripción

Trayectoria profesional

- Gerente de IT Risk Advisory y Cyber Risk, se incorporó al grupo en el año 2010, especializándose proyectos de adaptación regulatoria y en ciberseguridad, principalmente en el sector financiero y asegurador.
- Encargado de coordinar actividades de formación interna del Grupo en Continuidad de Negocio y de coordinación de iniciativas de gestión y captación del talento.

Formación académica y titulaciones

- Licenciado en Matemáticas (especialidad de Matemática Aplicada)
- Máster en Ingeniería Matemática orientada a finanzas por la Universidad de Santiago de Compostela.
- Certificaciones:
  - CISM
  - ISO 27032 Lead Cybersecurity Manager
  - CISA
  - ISO 22301 Lead Implementer
  - ITIL Foundation v3

Otros datos de interés profesional

- Idiomas: castellano, gallego, alemán, inglés.

Principales proyectos

- Liderazgo de Oficinas Técnicas de coordinación, seguimiento y reporte de actividades en el ámbito de la gestión de Riesgos Tecnológicos y Gobierno de la seguridad IT.
- Diagnósticos y Planes Directores de Ciberseguridad.
- Auditorías de ciberseguridad.
- Implantación y revisión de Sistemas de Gestión de la Continuidad de Negocio y desarrollo de material formativo.
- Implantación, revisión y mejora continua de Planes de Recuperación ante Desastres o DRP's.
- Implementación y revisión de Sistemas de Gestión de Seguridad de la Información.
- Adaptación y auditorías del cumplimiento por parte de proveedores y clientes del reglamento de medidas asociado a la Ley Orgánica de Protección de Datos (LOPD) y al GDPR.
- Auditoría de Sistemas de Información y revisión de aplicaciones de soporte al negocio.
- Adaptación a MiFID II y PRIIPs en Entidades Financieras a nivel europeo.
- Revisión de los procesos de generación del Transaction Reporting a CNMV en Entidades Financieras españolas.
- Análisis funcional de estrategias adoptadas motivadas por la Reforma del Sistema de Postcontratación español (liquidación, compensación y custodia)
- Elaboración de procedimientos de control y planes de auditoría IT asociados a Cámaras de Compensación del mercado de valores.

Principales clientes

Productos y Servicios:

- Estrella Galicia
- Grupo Orona
- Inditex
- Ecoembes
- Siemens-Gamesa
- Tetra Pak
- MAXAM

Banca:

- Abanca
- Laboral Kutxa
- Kutxabank
- Cecabank
- BBVA
- Unicaja
- Bankinter

Seguros:

- MAPFRE
- Pelayo
- Caser

Juan Loureiro Brañas

Senior Manager
12 años de experiencia

[redacted]
+34 911 57 85 ..7

Account Manager responsable del encargo

Equipo de proyecto propuesto

Currículums | Product Manager Cyber Strategy

Descripción

Trayectoria profesional

- Se incorporó a Deloitte en 2010 en el área de Enterprise Risk – IT-ERS del área de Madrid.
- Como consultor ha desempeñado proyectos en diferentes clientes y sectores de actividad, principalmente en el sector asegurador y financiero.
- En 2017 fue promocionado a gerente como Product Manager la línea de Cyber Risk Management & Compliance dentro del área de Estrategia de ciberseguridad.

Formación académica y titulaciones

- Ingeniero Superior de Telecomunicación por la Universidad Politécnica de Madrid
- Máster en Dirección y Gestión de Seguridad de la Información por la Universidad Politécnica de Madrid
- Certificaciones: CISM, CISA, CDPP, ISO22301 Provisional Lead Implementer, ISO27001 Lead Auditor, ITIL Foundation v3, COBIT 5 Foundation.

Otros datos de interés profesional

- Inglés con nivel de competencia profesional
- Instructor en diversos cursos internos y externos de Deloitte

Principales proyectos

- Proyectos de Gestión de Oficinas Técnicas de Seguridad en diferentes ámbitos:
  - Adaptación a la Normativa de Seguridad de la Información.
  - Seguridad en Nuevas Iniciativas.
  - Adecuación al Reglamento General de Protección de Datos.
- Proyectos de evaluación de riesgos de terceras partes.
- Proyectos de adecuación de entidades al Reglamento General de Protección de Datos (GDPR).
- Adecuación a la Normativa de Seguridad de la Información bajo el marco regulatorio nacional e internacional.
- Asesoramiento especializado en el cumplimiento de normativa de seguridad, mediante el diseño de procedimientos y controles específicos en procesos, revisión e identificación de requisitos no funcionales de seguridad y riesgos en aplicaciones, etc.
- Consultorías y auditorías LOPD, en base al actual Reglamento de Desarrollo.
- Consultoría de protección de datos abordando aspectos asociados a calidad de la información, derechos ARCO, declaración de ficheros, etc.
- Auditorías informáticas de seguridad y confiabilidad de entornos en entidades del sector financiero y asegurador, tanto como proyectos completos como apoyo a las auditorías financieras, las cuales incluyen pruebas masivas de datos como parte de los trabajos de las auditorías financieras, y revisiones de las configuraciones de seguridad de diferentes entornos.

Principales clientes

Seguros

- MAPFRE
- HDI
- MetLife

Banca:

- Santander
- BBVA
- BMN

Otros:

- Inversis
- Cepsa
- Konecta
- Renault
- Rexam
- Vithas

Félix de Andrés
Senior Manager
11 años de experiencia
fdeandres@deloitte.es
91.157.85.19

Product Manager
Cyber Risk Management &
Compliance

Equipo de proyecto propuesto
Currículum

Por motivos de confidencialidad, no se muestra el nombre del candidato. En caso de resultar adjudicatarios, se asignará un consultor con un perfil similar al mostrado.

Descripción

Trayectoria profesional

- Se incorporó a Deloitte en 2018, al área de Strategy & Risk Advisory - Cyber.
- A lo largo de su trayectoria profesional, ha trabajado en Accenture como Consultor de Seguridad.
- Cuenta con más de 4 años de experiencia en temas de ciberseguridad y en particular, en gestión de Oficinas Técnicas de Seguridad.

Formación académica y titulaciones

- Licenciado en Ingeniería Superior Industrial por la Universidad de Sevilla (US - ESI).
- CISA (Certified Information Systems Auditor).
- SSCP (Systems Security Certified Practitioner).

Otros datos de interés

- Idiomas:
  - Castellano
  - Inglés
  - Alemán

Principales proyectos

- Definición de Planes Directores de Seguridad de la Información. Elaboración de estrategias en materia de seguridad de la información que aportan valor añadido para el negocio.
- Gestión, seguimiento y control sobre todas las actividades de ciberseguridad así como la coordinación y gestión de tareas dentro de una Oficina Técnica de Seguridad, en entidades financieras y del sector del juego privado.
- Realización de auditorías internas sobre el cumplimiento de la Ley SOx, LOPD, requisitos de la EBA y normas ISO, PCI-DSS, etc.
- Evaluación de nivel de madurez de las cibercapacidades de un framework de ciberseguridad y elaboración de un Plan Director de Seguridad en entidades públicas.
- Definición del marco normativo en Seguridad de la Información en entidades financieras, teniendo en cuenta la clasificación y tratamiento de la información, la gestión de servicios Cloud, las relaciones con terceros, etc.
- Colaboración en distintos proyectos de Seguridad de la Información y Continuidad de Negocio.
- Análisis y gestión de riesgos basados en metodología Magerit, CobIT 5, etc.
- Soporte a las áreas de auditoría en la identificación de riesgos TIC así como la definición y ejecución de planes de acción.
- Definición y gestión de una PMO Global mediante metodologías ágiles.
- Definición de indicadores y realización de cuadros de mando.

Principales clientes

BBVA
Codere
Triodos Bank
Santander
Canal Isabel II

Consultor senior
4 años de experiencia

Índice

Honorarios

Propuesta económica

De acuerdo con la planificación y equipo de trabajo, así como sobre la base de nuestra experiencia en proyectos similares, y considerando el enorme interés que tenemos en poder colaborar con CNP Assurances en este proyecto, hemos estimado los siguientes honorarios:

Tipo de servicio	Equipo propuesto	Precio mes	Precio con descuento para el periodo septiembre-diciembre 2022
CISOaaS	**0,3 FTE Cyber** • Perfil consultor de seguridad – Cyber Strategy (~30%)	2.700 €	**6.666 €**

En caso de ser necesarios desplazamientos fuera de Madrid Capital (máximo 20% del tiempo presencial), se facturarán los gastos a manutención y/o alojamiento.

La cifra de honorarios y gastos que se ha hecho constar en los puntos anteriores se incrementará con los tributos que resulten aplicables, usando el tipo impositivo vigente en cada momento.

Nuestros honorarios desglosados por medio de facturas mensuales distribuidas según el importe total indicado en cada opción.

Les informamos que nuestras facturas son pagaderas en el plazo máximo de treinta (30) días naturales a contar desde la fecha de su emisión.

Índice

Valor diferencial de Deloitte

Por qué Deloitte

01

Líder
Firma líder en Servicios de Seguridad en todas sus capacidades

02

Experiencia
Experiencia en proyectos relacionados con la función del CISO y PMO relacionadas con la gestión de la seguridad

03

Cualificación
La mayor red de profesionales cualificados, certificados y en continua formación en materia de seguridad

04

Sector
Conocimiento del sector, así como las necesidades que tiene una entidad para ser líder en el mismo.

05

Flexibilidad
Proactividad y flexibilidad en la gestión de servicios profesionales. Capacidad de adaptarse a la demanda requerida por el servicio

06

Conocimiento
Profundo conocimiento del funcionamiento de las entidades del sector, sus necesidades y su modelo de gestión

07

Automatización
Focalización en la sistematización de actividades y dotación al servicio de herramientas útiles y sencillas

08

Procesos y metodología
Experiencia en la definición, adaptación y mejora de procesos y metodologías

09

Compromiso
Responsabilidad asumida en dar a la entidad el mejor servicio posible y garantizar la no complacencia

Valor diferencial de Deloitte

Factores clave de éxito

VISIÓN GLOBAL

Adecuar los mecanismos de trabajo con un enfoque global destinado a ofrecer a CNP Assurances una visión independiente, así como aprovecharse del conocimiento adquirido por Deloitte en otros proyectos.

GESTIÓN DE LA DEMANDA

Monitorizar la capacidad del Servicio y la carga de trabajo, permitiendo reaccionar a tiempo frente a potenciales picos de carga que requieran activar los procedimientos acordados para absorber la demanda.

INTEGRACIÓN

Conocer la filosofía de CNP Assurances y hacerla propia para facilitar la consecución de los objetivos planteados para el servicio.

SEGUIMIENTO Y TRANSPARENCIA

Dotar a la entidad de herramientas que le permitan determinar la calidad del servicio recibido, así como elevar los indicadores a la Dirección.

MEJORA CONTINUA

Identificar aspectos que permitan mejorar el servicio permanentemente sin importar su estado, evitando complacencias en el mismo.

FLEXIBILIDAD

Disponer de capacidad de adaptación a la demanda por parte de un equipo multidisciplinar y coordinación entre los propios proyectos.

Valor diferencial de Deloitte
Aspectos clave

Además, Deloitte dispone de un conjunto de aspectos diferenciales en la ejecución de los servicios, los cuales se incluyen a continuación:

1

Flexibilidad

Deloitte facilita que en el Servicio, en caso de picos de trabajo, puedan distribuirse para tareas específicas en momentos concretos.

2

Innovación

Deloitte desarrollará los mecanismos para gestionar el Servicio conforme a los mejores estándares, realimentándose de los casos de éxito en la gestión realizados en otros servicios.

3

Conocimiento transversal

Deloitte dispone de expertos en todas las capacidades de ciberseguridad (gobierno, seguridad, vigilancia y resiliencia), que darán soporte al Servicio.

4

Mejora continua

El propio modelo de seguridad de Deloitte está en continua mejora, lo que facilitará al Servicio tener en cuenta todos los riesgos de ciberseguridad que aparezcan con motivo del desarrollo de nuevas tecnologías o modalidades de ataque.

Valor diferencial de Deloitte

Principios para asegurar un retorno del servicio ordenado, controlado y completo

CONOCIMIENTO

La información relevante debe ser documentada y compartida de manera permanente entre el equipo del servicio de Deloitte y CNP Assurances para asegurar una adecuada actualización del estado de situación de manera constante.

DOCUMENTACIÓN

Toda documentación generada por el servicio que se considere parte de un entregable o documentación de soporte para la gestión ha de estar accesible, organizada eficientemente y con capacidad de ser explotada.

Como parte de la documentación, es relevante proporcionar información de estado del servicio e indicadores de calidad.

COMUNICACIÓN

Se han de establecer mecanismos para garantizar que la información relevante es comunicada y conocida por todos los implicados.

La comunicación se considera un aspecto fundamental para garantizar la independencia del proveedor, facilitando a CNP Assurances el control final del servicio y la toma de decisiones relevantes.

HERRAMIENTAS

Tanto en el retorno como en la mejora en la eficiencia del servicio, éste debe proporcionar medios eficientes para facilitar la gestión y transferencia del conocimiento.

Desde Deloitte, se considera fundamental ayudar a CNP Assurances en la creación de herramientas que agilicen los tiempos de respuesta, calidad de reportes y transparencia.

DC

Valor diferencial de Deloitte

Equipo profesional altamente cualificado y amplia experiencia

Deloitte cuenta 14 socios en España en gestión de riesgo tecnológico y un equipo de **más de 700 especialistas en seguridad** y auditoría informática, la mitad de ellos dedicados específicamente a la Ciberseguridad, que atesoran **más de 500 certificaciones** en auditoría informática y seguridad de la información.

Los equipos de cibersegu s, siendo uno de ellos el vencedor global.

Valor diferencial de Deloitte
CyberSOC-CERT

Equipo de **alta calidad técnica** en constante **formación y con experiencia** en proyectos similares de seguridad. Cada servicio prestado desde el CyberSOC-CERT está estructurado en **tres niveles de especialización** y organizado en base a diferentes procedimientos de actuación, sometidos a procesos continuos de **madurez y optimización**, para ofrecer una máxima calidad.	**Equipo de trabajo** 	**Medidas de seguridad** 	Diversas medidas para **asegurar la prestación** de los servicios: • Protocolos de cifrado seguros. • Actividades de seguimiento de eventos en 24x7 del canal. • Creación de políticas de acceso. • Rotación de contraseñas. • Segregación de privilegios en la plataforma de conexión. • Registro de trazas para identificar a cada usuario. • Línea de backup.
El CyberSOC-CERT cuenta con **herramientas y plataformas de análisis a la vanguardia** del mercado y específicas para la prestación de los servicios. El CyberSOC-CERT Desk es la herramienta de gestión de tickets que soporta la operativa diaria en el CyberSOC-CERT para el **tratamiento de alertas e incidencias, monitorizada en 24x7**, y que posee una gran base de procedimientos para la gestión y soporte de incidentes de seguridad.	**Herramientas y plataformas especializadas** 	**Procedimientos** 	Se definirán por parte del equipo de trabajo de Deloitte, y una vez se hayan consensuado, todos los **procedimientos** (de escalado, de comunicación, de atención de casos, etc.) **para la correcta prestación del servicio**. Gracias a la experiencia en este tipo de proyectos, contamos con una **gran base de información y conocimiento** que nos permitirá asesorar en el ajuste y mejora de los procedimientos.
Asegurar la calidad del servicio que presta a todos sus clientes es una de las principales preocupaciones de Deloitte. La figura de **jefe de proyecto** se responsabilizará del buen funcionamiento y de la calidad del servicio, centralizando todas estas tareas: • Generación de **informes y métricas**. • **Gestión** del servicio, **supervisión y control** a distintos niveles. • **Control de cambios** en procedimiento y documentación del servicio. • **Reuniones** de supervisión y seguimiento, internas y con cliente. • Canalización de **solicitudes**.	**Gestión, supervisión y calidad** 	**Factores diferenciales y capacidades añadidas** 	El SOC de Deloitte ofrece una serie de factores y capacidades añadidas que incrementa las prestaciones de los servicios. Prueba de ello son: • **Soporte de la Red Global de Deloitte** para proporcionar alcance internacional a nuestros clientes así como acceso a una base de inteligencia (Casos de Uso). • **Acceso a múltiples fuentes de inteligencia** a través de acuerdos y alianzas nacionales e internacionales y pertenencia a **la red CERT**. • **Fuerte inversión en materia de seguridad** para la creación de laboratorios de análisis de amenazas y plataformas tecnológicas.

Valor diferencial de Deloitte

Líderes en ciberseguridad

Liderazgo de Deloitte en Cibersegruidad consolidado y reconocido por los analistas independientes en el mercado de global de la consultoría de riesgos tecnológicos, seguridad de la información y ciberseguridad tales como Forrester, Gartner, Kennedy e Hypatia.

Deloitte ha certificado su proceso de gestión de la seguridad y de continuidad de negocio según la **normas ISO-27001 e ISO-22301**. El alcance del sistema de gestión incluye todos los activos de información que son gestionados en el contexto de la prestación de los nuestros servicios profesionales a nuestros clientes y el CyberSOC-CERT, respectivamente.

El **centro de operaciones de seguridad de Deloitte** (CyberSOC-CERT) ha recibido la certificación **CERT** (Computer Emergency Response Team), concedida por la Universidad Carnegie-Mellon.

Deloitte es la única Big Four en el mundo que cuenta con el sello CERT.

Más de 700 profesionales en España dedicados a la gestión de riesgos tecnológicos, y más de 300 focalizados en ciberseguridad.

Más de 500 certificaciones en esta materia, desde certificaciones orientadas a la gestión hasta certificaciones técnicas de producto.

Deloitte vencedor de las Global Cyberlympics 2011, 2012, 2013, 2015 y 2016.

El **CyberSOC-CERT de Deloitte**, situado en España, ofrece a nuestros clientes capacidades únicas para la prevención, detección y respuesta frente a ciberataques.

Para ello, el CyberSOC-CERT de Deloitte dispone de capacidades de operación 24x7 soportadas entre otras, con tecnologías propietarias de Deloitte.

El **CyberLabs de Deloitte** es un centro con una infraestructura y un equipo de arquitectos de seguridad dedicado en exclusiva a la evaluación independiente de nuevas soluciones de seguridad, al diseño de *blueprints* de arquitecturas de seguridad y a la evaluación y análisis de nuevas amenazas de seguridad asociadas al uso de nuevas tecnologías emergentes.

Valor diferencial de Deloitte

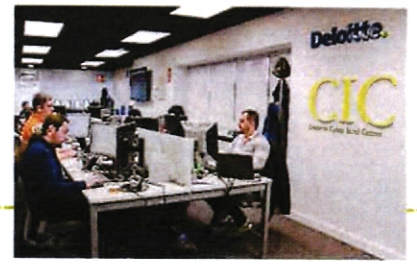
Liderazgo de Deloitte España en la estrategia global de Deloitte

- **Deloitte España** se posiciona como líder en Cyber con un **Centro Global de Operaciones de Ciberseguridad** (CyberSOC-CERT) para la región de **EMEA**, ubicado en Madrid, además, de **dos Centros de Ciber Inteligencia (CIC)**, ubicados en Madrid y Barcelona.
- De este modo, Deloitte ofrece una de las ofertas más completas e innovadoras a través de una amplia cartera de servicios de ciberseguridad de alto valor añadido, que presta a más 200 clientes alrededor del mundo a través de uno de los equipos más especializados del mercado conformado por más de 250 profesionales.

Cyber Intelligence Center (CIC) Madrid

Cyber Intelligence Center (CIC) Barcelona

CyberSOC-CERT: EMEA Delivery Center (EDC) Alcobendas (Madrid)



Valor diferencial de Deloitte

Nuestra Red de Inteligencia Global y CyberSOCs

Los **Centro de Excelencia en Ciberinteligencia CIC** (Cyber Intel Centre) de Deloitte se trata de centros avanzados y especializados en servicios de inteligencia y protección frente a ciberamenazas dirigidas contra organizaciones. La red de ciberinteligencia global de Deloitte está compuesta por diversos centros y nodos en diferentes países, ofreciendo una cobertura global e integral a sus clientes:

Deloitte cuenta con 53 laboratorios de seguridad (**Deloitte Data Forensics & eDiscovery Laboratories**) por todo el mundo, para recolectar, analizar, detectar y responder ante ciberataques.

Centro de Deloitte para la Ciberinnovación: más de 100 soluciones han sido testeadas en escenarios reales de ataque para mejorar sus capacidades de protección.

Valor diferencial de Deloitte

Nuestras capacidades en Ciberseguridad

Las capacidades de nuestro Centro europeo de Operaciones de Ciberseguridad fueron evaluadas en 2016 por Gartner, destacando su liderazgo como "**Centro de Detección y Respuesta gestionada de incidentes de Ciberseguridad**"

EMEA Delivery Center (EDC) ofrece una amplia gama de servicios de operaciones de alto valor añadido, actuando desde Madrid como proveedor de la red Deloitte para el mercado de Europa, Oriente Medio y África.

CERT

El EDC es un Centro de Respuesta a Incidentes de Ciberseguridad (CERT) certificado y parte de la Carnagie Mellon University CERT Network

ISO-22301

Certificado en ISO22301, el estándar para la gestión de la continuidad de negocio

ISO-27001

Certificado en ISO27001, el estándar para la gestión de la seguridad de la información

Equipo certificado

Finalmente, destacar que AENOR ha certificado conforme a las exigencias de la norma española UNE-EN **ISO 9001 el Sistema de Calidad exclusivamente para su uso en Sector Público de Deloitte Advisory, S.L.**

260 profesionales de Cyber en España y +1.200 distribuidos en 20 firmas de EMEA

Valor diferencial de Deloitte

Nuestros servicios de Ciberseguridad

Deloitte ofrece la oferta de servicios más completa del mercado a través de sus soluciones de Advisory, Seguridad Gestionada (SOC) y CyberAcademy. La complementariedad de estos servicios ofrece a todos nuestros clientes un amplio catálogo de soluciones de "extremo a extremo" y de alta diferenciación frente a nuestros competidores.

Seguridad "Extremo a Extremo"

Nuestros servicios de Ciberseguridad abarcan desde la capa estratégica hasta la operación de sistemas de seguridad 24x7x365, persiguiendo la protección integral de los activos críticos de la organización: personas, información, procesos e infraestructuras.

Estrategia

- **Cyber Risk Management and Compliance**
- **Cyber Training, Education and Awareness**
- **Cyber Strategy, Transformation and Assessments**

Protección

- **Infrastructure Protection**
- Vulnerability Management
- Application Protection
- Identity and Access Management
- Information Privacy and Protection

Vigilancia

- Advanced Threat Readiness and Preparation
- Cyber Risk Analytics
- Security Operations Centre
- Threat Intelligence and Analysis

Resiliencia

- Cyber Incident Response
- Cyber Wargaming

Modelos de entrega

Asesoramiento | Implementación | Operación | Formación

Índice

Responsabilidad, Indemnidad y Protección de Datos

Responsabilidad

La responsabilidad máxima de Deloitte, de sus socios y de su personal por daños, perjuicios o reclamaciones que se pudieran derivar de los servicios contemplados en esta propuesta estará limitada conjuntamente a una cantidad equivalente a los honorarios satisfechos por los concretos servicios prestados que den lugar a la reclamación, y en ningún caso podrán ser objeto de reclamación los daños o perjuicios indirectos, lucro cesante, daño emergente, o costes de oportunidad. Este límite no será de aplicación en el supuesto que Deloitte, sus socios o su personal haya incurrido, en la ejecución de los trabajos objeto de la presente propuesta, en dolo o negligencia grave declarada por sentencia firme o un incumplimiento de la cláusula de confidencialidad, de la normativa sobre protección de datos o propiedad intelectual e imputable a Deloitte.

Cualquier reclamación derivada o relacionada con los servicios contemplados en el marco de esta propuesta deberá presentarse en el plazo máximo de prescripción de las acciones.

Indemnidad

Salvo en los supuestos en que Deloitte haya incurrido en dolo o negligencia grave declarada por sentencia firme o resolución de una autoridad competente, el cliente mantendrá indemne en todo momento a Deloitte, sus socios y su personal frente a cualquier reclamación de terceros distintos de la propia sociedad, en relación o que traigan causa en un incumplimiento por parte del cliente de las condiciones establecidas en la presente propuesta, así como en un uso indebido de los resultados, debiendo indemnizar en su caso a Deloitte, sus socios y/o su personal por los daños y perjuicios, gastos y costes (incluyendo honorarios de asesoramiento, abogados y procuradores) en que pudiera incurrir por causa de dichas reclamaciones o por las actuaciones en las que deba intervenir.

Datos de contacto en relación a las obligaciones del Reglamento de Protección de Datos Personales

Datos de contacto		Datos de contacto en relación a las obligaciones con la RGPD	
Nombre	Araceli Benito	Notificación de violaciones de seguridad	dpd.es@cnppartners.eu
Dirección		Notificación de las peticiones de ejercicio de derechos	gdpr.es.peticion@cnppartners.eu
Teléfono	+34 91 524 31 61		
Correo electrónico	Araceli.benito@cnppartners.eu		

Deloitte informa a las personas de contacto del Cliente de que sus datos de carácter personal serán almacenados y tratados por aquella con la finalidad de gestionar la presente relación contractual, y que podrán ejercitar, en caso de estimarlo oportuno y conforme a los procedimientos legalmente previstos, sus derechos de acceso, rectificación, supresión, limitación del tratamiento, oposición o portabilidad dirigiéndose a la dirección que figura en el encabezamiento de esta carta propuesta o bien mediante el envío de un email a la dirección de correo electrónico lopd@deloitte.es.

DC

Índice

Condiciones Generales de Contratación

Deloitte Advisory, S.L. (en adelante Deloitte) prestará los servicios definidos en la Propuesta firmada por CNP Assurances SA, sucursal en España ("el Cliente") y Deloitte (la "Propuesta" y los "Servicios") de acuerdo con las siguientes Condiciones Generales de Contratación las cuales, junto con la Propuesta, constituyen el contrato completo entre ambos respecto a los Servicios (el "Contrato"), sustituyen cualquier comunicación oral o escrita intercambiada por el Cliente y Deloitte con anterioridad a la Propuesta, y pueden ser modificadas (incluyendo cambios al alcance o naturaleza de los Servicios) únicamente mediante acuerdo escrito de ambas partes de conformidad con lo que se establece en este Contrato y siguiendo el procedimiento de realización de cambios que, en su caso, se determine en la Propuesta. En caso de contradicción o conflicto entre estas Condiciones Generales y los términos de la Propuesta, prevalecerá la Propuesta.

Artículo 1 - Honorarios y Gastos.

El Cliente pagará a Deloitte Advisory, S.L. los honorarios y gastos aprobados previamente por escrito por el cliente correspondientes, de acuerdo con lo estipulado en la Propuesta.

Artículo 2 - Obligaciones de Deloitte Advisory, S.L.

Las obligaciones de Deloitte se determinan en la Propuesta y en estas Condiciones Generales.

Artículo 3 - Obligaciones del Cliente.

El Cliente es consciente de que un proyecto de consultoría como el que se aborda en este Contrato requiere, como elemento esencial del proyecto, el compromiso y la participación activos del propio Cliente, los cuales condicionan directamente las prestaciones y el cálculo de los honorarios del consultor. En este sentido, y sin perjuicio de que en la Propuesta y en estas Condiciones Generales se determinen con mayor detalle, amplitud o precisión las responsabilidades del Cliente en el marco de este Proyecto, el Cliente se compromete a llevar a cabo al menos las siguientes actividades esenciales:

a) ejecutar en los plazos establecidos y de forma adecuada sus responsabilidades, tal y como se determine en su caso en la Propuesta, y garantizar que las hipótesis de partida o factores de éxito identificados son correctos y adecuados;

b) proporcionar a Deloitte información fiable, correcta, actualizada y completa, según sea necesario para la realización de los Servicios;

c) adoptar decisiones dentro de los plazos establecidos y obtener toda aprobación necesaria de la Dirección o de los Órganos Sociales que resulten competentes para la contratación de estos servicios; en este sentido, las partes acuerdan que corresponderá a la Dirección o los Órganos Sociales del Cliente tomar toda decisión ejecutiva o estratégica relativa a este proyecto.

DC

(d) poner a disposición del personal de Deloitte, en su caso, un entorno de trabajo apropiado, así como recursos y material adecuados.

(e) Adicionalmente, Deloitte podrá confiar en toda decisión o aprobación efectuada por el Cliente independientemente de este Contrato y/o con anterioridad a la firma del mismo. Nada en este Contrato requerirá que Deloitte evalúe, aconseje sobre, modifique, confirme o rechace tales decisiones o aprobaciones, salvo que las partes establezcan lo contrario en el Contrato. El Cliente será responsable de cualquier retraso, coste adicional, u otras consecuencias negativas derivadas de o relacionadas con cualquier deficiencia en el cumplimiento por parte del Cliente de sus Obligaciones.

Artículo 4 - Confidencialidad.

Con relación a la información proporcionada en el marco de este Contrato y designada como confidencial por la parte que la proporcione, la parte que la reciba se compromete a: (i) proteger dicha información confidencial de forma razonable y adecuada y de acuerdo con los estándares profesionales aplicables, en su caso; (ii) utilizar la información confidencial únicamente con el fin de ejecutar sus obligaciones en el marco del Contrato; (iii) reproducir información confidencial únicamente en la medida necesaria para ejecutar sus obligaciones en el marco del Contrato. Este Artículo no se aplicará a información que: (i) sea del dominio público; (ii) sea ya conocida por la parte que la recibe; (iii) se haya proporcionado a un tercero sin restricciones; (iv) haya sido desarrollada independientemente; o (v) haya sido revelada por causa de requisitos legales. Sin perjuicio de lo anterior, Deloitte podrá comunicar información confidencial del Cliente a sus subcontratistas y a entidades miembro de la organización.

Artículo 5 - Resultados y Restricciones de Uso.

El Cliente podrá, únicamente para fines internos propios, usar, copiar, distribuir y modificar los resultados que se describen en la Propuesta (los "Resultados"). Dado que los Resultados se desarrollan únicamente para uso interno del Cliente, en el contexto preciso de este proyecto, el Cliente no comunicará los Resultados a terceros (las compañías del Grupo CNP no tendrán la consideración a efectos de esta cláusula como terceros), ni los citará públicamente, ni hará referencia a los mismos, sin el consentimiento previo escrito de Deloitte. Queda prohibido cualquier uso de los Resultados, diferente al que se indica en la Propuesta, sin la autorización previa y por escrito de Deloitte. Deloitte conserva todo derecho, título e interés en: (i) los Resultados, incluyendo a título ilustrativo, toda patente, derecho de autor, marca u otros derechos de propiedad intelectual relativos a los Resultados; y (ii) toda metodología, procedimiento, técnica, idea, concepto, secretos comerciales y knowhow incorporados o relativos a los Resultados o que Deloitte pueda desarrollar o aportar en relación con este Contrato (los "Conocimientos de Deloitte"). Sin perjuicio de las obligaciones de Confidencialidad que se establecen en la Cláusula 4, Deloitte podrá utilizar sin restricciones los Resultados y los Conocimientos de Deloitte.

Artículo 6 - Aceptación.

El Cliente aceptará los Resultados (i) que sean conformes a los requisitos o especificaciones que establezca la Propuesta; o (ii) que hayan superado el plan de pruebas de aceptación acordado específicamente para este proyecto, en su caso. Durante el proceso de aceptación, el Cliente notificará inmediatamente a Deloitte cualquier no-conformidad de los Resultados con tales requisitos o especificaciones ("No-Conformidad") y Deloitte dispondrá de un plazo de tiempo razonable, en función de la gravedad y de la complejidad de la No-conformidad, para rectificarla. Si el Cliente ha utilizado los Resultados antes de la aceptación, si no ha notificado a Deloitte inmediatamente la No-conformidad, o si retrasa de forma no razonable el inicio del plan de pruebas acordado, se considerará que el resultado en cuestión ha sido aceptado por el Cliente.

Artículo 7 - Manifestaciones y Compromisos.

(a) Deloitte prestará los Servicios con la diligencia debida y, una vez realizada la aceptación en los términos del Artículo 6, se compromete a corregir cualquier No-conformidad, siempre y cuando el Cliente notifique dicha No-conformidad a Deloitte por escrito en un plazo de treinta (30) días a partir de la aceptación tal y como se define en el mencionado Artículo 6. Transcurrido dicho plazo sin haber obtenido ninguna comunicación escrita por parte del Cliente, se considerará que el servicio ha sido prestado de acuerdo a las condiciones pactadas en la Propuesta.

(b) Deloitte no garantiza ni será responsable de productos o servicios de terceros. Toda reclamación del Cliente en este sentido, será frente a los terceros proveedores.

(c) Independientemente del alcance de los Servicios o Resultados, el Cliente manifiesta que es de su responsabilidad diseñar y mantener un sistema de control interno, y en particular de aquellos controles internos contables, que garantice suficientemente que: (i) las operaciones se realizan con autorización general o específica de la Dirección; (ii) las operaciones se registran de modo que permitan (a) preparar estados financieros y cuentas anuales de acuerdo con principios contables generalmente aceptados o con cualquier otro criterio que resultara aplicable a dichos estados financieros, y (b) mantener registros contables de los activos; (iii) el acceso a los activos se permite únicamente con autorización general o específica de la Dirección; y (iv) los registros contables de los activos se contrastan con los activos reales con una frecuencia adecuada y se emprenden acciones apropiadas en relación con cualquier diferencia que pudiera existir. El Cliente determinará la adecuación de sus controles contables internos y de sus sistemas de información financiera, sin basarse en los Servicios o Resultados como elemento principal de tal determinación, asumiendo, por tanto, la responsabilidad del sistema global de control interno. Finalmente, el Cliente manifiesta que es de su responsabilidad realizar las comunicaciones relativas a este proyecto que requiera la normativa aplicable.

DL

(d) El Cliente y Deloitte se comprometen a cumplir con las leyes y normativas aplicables, incluidas las relacionadas con la anticorrupción, manifestando asimismo su compromiso de actuar en todo momento de forma ética y profesional, y comprometiéndose a no realizar ninguna práctica que de alguna manera resulte o pueda resultar en una vulneración de leyes o normativas aplicables relacionadas con la corrupción en cualquier país cuya legislación sea aplicable al presente Contrato.

Artículo 8 - Personal.

(a) Deloitte será responsable de designar y asignar su propio personal, en el modo más adecuado según su criterio, para la realización de los Servicios, sin perjuicio de lo cual Deloitte tratará de responder a los requisitos o sugerencias del Cliente respecto a individuos determinados.

(b) Durante la vigencia de este Contrato, y durante un periodo de doce (12) meses a partir de la finalización o resolución del mismo, ninguna de las partes tratará de contratar, directa o indirectamente, personal de la otra que haya participado directamente en la prestación de los Servicios.

c) La naturaleza de este contrato es la propia de un arrendamiento de servicios de carácter exclusivamente mercantil. Por lo expuesto, no se deriva relación o vínculo laboral alguno entre las partes, ni entre el Cliente y el personal de Deloitte que, eventualmente, pudiera estar prestando alguno de los Servicios que constituye el objeto del presente contrato. Deloitte está obligado a cumplir con todas las obligaciones establecidas para con la Seguridad Social y Hacienda en relación a dicho personal y, específicamente, las relativas a la Seguridad Social e Higiene y Accidentes de trabajo. En este sentido, con la firma del presente contrato, Deloitte: i) certifica expresamente que cumple en todo momento con la totalidad de sus obligaciones en materia fiscal, laboral (en concreto pago de salarios) y de cotización respecto de sus empleados por cuenta ajena; ii) se obliga a aportar certificado de descubiertos emitido por la Seguridad Social así como un certificado de cumplimiento de sus obligaciones tributarias a la firma del presente Contrato.

Artículo 9 - Resolución.

(a) El presente Contrato podrá ser resuelto: (i) por cualquiera de las partes en caso de incumplimiento por la otra de los términos de este Contrato, siempre que tal incumplimiento no haya sido subsanado por la otra en un plazo de quince (15) días desde la fecha de recepción de la notificación de incumplimiento; y (ii) por Deloitte, en caso de incompatibilidad legal sobrevenida, con quince (15) días de preaviso.

(b) Salvo en caso de resolución por incumplimiento de Deloitte, el Cliente pagará a Deloitte todos los honorarios y gastos correspondientes a Servicios prestados hasta la fecha de la resolución.

(c) Deloitte deberá devolver el importe abonado en concepto de provisión de fondos si los honorarios exceden de los que debería haber cobrado Deloitte hasta la finalización del contrato.

c) Salvo en materias relativas a obligaciones de confidencialidad o derechos de propiedad intelectual, las partes se comprometen a tratar de resolver cualquier diferencia, disputa o posible incumplimiento, internamente, elevándolo a niveles de dirección competentes de sus respectivas organizaciones y, en general, a utilizar procedimientos alternativos de resolución de disputas que resulten mutuamente aceptables, antes de recurrir a procedimientos contenciosos.

Artículo 10 - Tratamiento de datos personales

Si como consecuencia de la prestación de los Servicios contratados, Deloitte tuviera acceso a datos de carácter personal que se encuentran bajo la responsabilidad del Cliente, Deloitte tendrá la condición de Encargado del tratamiento.

La naturaleza y finalidad de los tratamientos que Deloitte realizará por cuenta del Cliente será la derivada de la prestación del servicio objeto del Contrato, y en concreto consistirá en: recogida, procesamiento, conservación, consulta, cotejo, supresión, registro y destrucción.

Para la ejecución de los Servicios contenidos en el presente Acuerdo, el Cliente pone a disposición de Deloitte la siguiente información/datos personales:

*Marcar aquellas categorías de información o datos personales que se faciliten:

✖	Nombre		Datos de afiliación a entidades		DNI/Pasaporte		Orientación sexual
	Número de empleado/ID personal		Fotografía o videos donde aparezca el individuo		Estado civil		Códigos de cuentas financieras
	Dirección privada		Salario/Tipo de contrato		Datos de salud		Carnet de conducir
✖	Información de contacto privada		Evaluaciones		Etnia/Raza		Contraseñas
✖	Información de contacto de empresa		Registro de llamadas		Sexo		Certificado de penales
	Datos biométricos		Hojas de gastos		Creencias religiosas		Otros
	Estudios		Fecha de nacimiento		Orientación política		

3C

Habida cuenta del carácter reservado de los datos que obran en poder del Cliente, en caso de que éstos pudieran ser conocidos por Deloitte en virtud del presente Acuerdo, éste último se compromete a que permanezcan en secreto.

Esta obligación de Deloitte de guardar secreto permanecerá en vigor incluso después de cesar en su relación con el Cliente.

A estos efectos, Deloitte se compromete a tomar, respecto de sus empleados, todas las medidas necesarias para que resulten informados de la necesidad del cumplimiento de las obligaciones que le incumben como encargado del tratamiento de datos de carácter personal y que, en consecuencia, deben respetar.

Deloitte se compromete a tratar los datos personales a los que tenga acceso únicamente para el cumplimiento de los términos de este Acuerdo. Este compromiso se extenderá asimismo con respecto a las Transferencias Internacionales de Datos de carácter personal a un tercer país o una Organización internacional.

En consecuencia, los datos que se conozcan u obtengan en virtud de este Acuerdo, no podrán ser utilizados para ninguna otra finalidad distinta de la ejecución del mismo, tendrán carácter confidencial y no serán divulgados o puestos en conocimiento de terceros sin la previa autorización por escrito del Cliente salvo en los casos expresamente autorizados por la Ley.

En el caso de que Deloitte recurra a subcontratistas (subencargado) para llevar a cabo determinadas actividades de tratamiento de datos personales por cuenta del Cliente, Deloitte deberá obtener autorización previa del Cliente. A tal efecto, Deloitte informará por escrito al Cliente con carácter previo de las subcontrataciones previstas, facilitando los datos de los terceros a los que pretenda subcontratar. Si el Cliente no manifestara por escrito su oposición a dicha subcontratación en el plazo de quince días desde la recepción de la notificación correspondiente, se entenderá que no se opone a la misma. Los mismos términos y obligaciones resultarán aplicables en el supuesto de que Deloitte tuviera intención de sustituir a alguno o algunos de sus subencargados.

Adicionalmente, el Cliente acepta que Deloitte, actuando en nombre y por cuenta del Cliente, subcontrate los servicios de soporte informático con PM&S Recursos, S.L.U., así como otros servicios con cualquiera de las sociedades que formen parte de la Organización Deloitte en España (subencargados), todas ellas con domicilio social en Pza. de Pablo Ruiz Picasso nº 1, Torre Picasso, 28020-Madrid.

Deloitte impondrá por escrito al subencargado las mismas obligaciones de protección de datos recogidas en la presente cláusula. Dichas obligaciones serán igualmente extensibles para Deloitte en el supuesto de que el subencargado utilice otros terceros y en el caso de existir una cadena de subcontratistas, de tal modo que Deloitte y cualquiera de los sucesivos subcontratistas hasta llegar al último de la cadena queden sujetos a las mismas obligaciones.

Deloitte será plenamente responsable ante el Cliente y responderá del efectivo cumplimiento de las obligaciones en materia de protección de datos de los posibles subcontratistas que interviniesen en el tratamiento de los datos personales.

Deloitte se compromete a aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, habida cuenta del estado de la técnica, los costes de aplicación, la naturaleza de los datos almacenados, el alcance, contexto y fines del tratamiento, así como los riesgos a que estén expuestos y el impacto que esto pudiera tener sobre los derechos y libertades de las personas físicas.

En todo caso, Deloitte deberá implantar mecanismos para:

* Seudonimizar y cifrar los datos personales, en su caso.

* Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

* Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

* Verificar, evaluar y valorar regularmente la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

Asimismo, Deloitte estará obligado a cumplir con sus deberes respecto a la realización de cualesquiera evaluaciones de impacto en materia de protección de datos que estuviera obligado a llevar a cabo.

Deloitte deberá poner a disposición del Cliente la documentación justificativa correspondiente y permitir la realización de auditorías e inspecciones con el fin de comprobar los extremos indicados con anterioridad. Dichas auditorías serían realizadas por el Cliente, o por un tercero designado de mutuo acuerdo, siendo el coste de las mismas soportado por el Cliente.

Deloitte notificará al Cliente sin dilación indebida y el plazo máximo de 24 horas desde que fue conocida por Deloitte y a través del canal que facilite el Cliente a estos efectos, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia, salvo en aquellos supuestos en los que sea improbable que dicha violación de seguridad constituya un riesgo para los derechos y libertades de los interesados.

Si dispone de ella se facilitará, como mínimo, la información siguiente:

* Descripción de la naturaleza de la violación de la seguridad de los datos personales y, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

* El nombre y los datos del delegado de protección de datos.

* Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

* Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si en un primer momento Deloitte no pudiera informar de todas las cuestiones indicadas con anterioridad, las comunicará tan pronto tenga conocimiento de las mismas.

Deloitte asistirá al Cliente a través de medidas técnicas y organizativas apropiadas y siempre que sea posible, en relación con las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados.

En el caso de que las personas afectadas ejerzan los derechos mencionados en el apartado anterior ante Deloitte, ésta debe comunicarlo por correo electrónico al Cliente a la dirección que el cliente facilite a estos efectos. La comunicación deberá hacerse sin dilación indebida desde la recepción de la solicitud y en el plazo máximo de 5 días naturales desde que fue recibida por Deloitte, juntamente, en su caso, con cualquier otra información que pueda ser relevante para resolver la solicitud.

Asimismo, cualquier tipo de transferencia internacional deberá ser autorizada por el cliente y además deberá contar con las garantías precisas (binding corporate rules, modelo de clàusula aprobado por la UE) en caso contrario no podrá realizarse.

Una vez terminado por cualquier causa el Acuerdo y a elección del Cliente, Deloitte se compromete a devolver y/o destruir todos los datos personales a los que hubiera tenido o tenga acceso para la realización del objeto del Acuerdo, al igual que cualquier copia de los mismos en cualquier soporte, salvo en la medida en que sea necesaria su conservación en virtud del derecho comunitario o de los Estados miembros que resulte de aplicación, o para la formulación, ejercicio o defensa de reclamaciones relacionadas con el objeto del presente contrato.

Artículo 11 - Disposiciones Generales.

(a) Ninguna de las partes utilizará el nombre, marcas, logotipos, nombres comerciales y/o elementos publicitarios de la otra sin el consentimiento previo por escrito de aquélla. Sin perjuicio de lo anterior, Deloitte podrá citar en otras propuestas o contratos el nombre del Cliente y/ o realizar una descripción general de los Servicios/ del Proyecto, con fines de promoción. El Cliente acuerda igualmente que, mediando un preaviso razonable por parte de Deloitte, accederá a proporcionar a terceros referencias favorables a Deloitte (por ejemplo, en forma de llamadas telefónicas de clientes o analistas o presentaciones).

(b) No obstante lo indicado en el apartado (a), Deloitte podrá compartir con otras entidades de su organización el nombre del Cliente y/o realizar una descripción general de los servicios prestados, siendo dicha información para uso exclusivo de la organización Deloitte.

(c) Ninguna de las partes será responsable por retrasos o incumplimientos debidos a circunstancias que escapen a su control razonable.

(d) Este Contrato no podrá ser cedido en modo alguno, en todo o en parte, sin el acuerdo escrito previo de la otra parte, incluso cuando se trate de entidades de su organización internacional y además, deberá contar con las garantías adecuadas y cumplir con la cláusula y normativa sobre protección de datos incluida en la presente propuesta.

(e) Toda comunicación que se realice en el marco de este Contrato será escrita, se enviará a las direcciones indicadas en la Propuesta, y se considerará efectuada en el momento de su recepción por la parte destinataria.

(f) Toda renuncia a términos de este Contrato y toda excusa a un incumplimiento del mismo, deberán constar por escrito, firmado por la parte que consienta a dicha renuncia o excusa.

(g) En caso de que cualquier término o estipulación de este Contrato sea declarado ilegal, nulo o anulable, se considerará eliminado dicho término o estipulación, sobreviviendo el resto del Contrato.

(h) Este Contrato no convierte a ninguna de las partes en agente o representante legal de la otra, y no crea ningún tipo de asociación o empresa en común. Las partes actúan como contratistas independientes y asumen plenamente y en nombre propio sus respectivas obligaciones, derivadas de este Contrato.

(i) Los Artículos 4 a 13 de este Contrato sobrevivirán a la expiración o resolución del mismo por cualquier causa.

(j) El presente Contrato se somete a Ley española.

(k) El Cliente reconoce que: (i) Deloitte y el Cliente podrán comunicarse o enviarse documentación mediante correo electrónico/ Internet, salvo que el Cliente determine expresamente lo contrario; (ii) ninguna de las partes controla el funcionamiento, fiabilidad, disponibilidad o seguridad del correo electrónico/ Internet; y que (iii) Deloitte no será responsable de ninguna pérdida, daños, gastos, perjuicios o molestias que resulten de la pérdida, retraso, interceptación, corrupción, o alteración de cualquier correo electrónico o comunicación por Internet.

(l) Deloitte no asume responsabilidad por las prestaciones, fiabilidad, disponibilidad o seguridad de Internet, de sistemas o de hardware del Cliente o de terceros, que no estén comprendidos en el alcance de los Servicios de Deloitte en este proyecto.

Salvo que las partes acuerden por escrito lo contrario, el Cliente asume la responsabilidad de:

* determinar la existencia de, y cumplir con, los elementos siguientes, aplicables a transacciones, comercio, procesos electrónicos, o a actividades realizadas a través de Internet o de cualquier red electrónica ("Transacciones"): controles import/ export; requisitos para obtener y mantener licencias y otros permisos; requisitos para evaluar, pagar o retener impuestos, tasa de aduana u otras cargas o tributos; y cualesquiera otras leyes o reglamentos en cualquier jurisdicción competente;

* la seguridad de su red y de cualquier sistema relacionado con la misma, incluida la seguridad, privacidad y confidencialidad de cualquier dato, propiedad intelectual u otra información del Cliente o de terceros;

* establecer y determinar la validez y ejecutabilidad de los procesos de firma y realización de contratos, así como de cualquier otra documentación necesaria para o utilizada en el marco de las Transacciones;

* cualquier contenido aportado por el Cliente o por terceros en relación con este proyecto; y

* cualquier utilización de los Resultados por el Cliente, incluyendo, a título de ejemplo: inclusión por el Cliente en su website o transmisión a través de Internet, de texto, imágenes, software, música, videos u otra información; venta u oferta por el Cliente de bienes o servicios mediante su website o por Internet; y cualquier distribución de correo electrónico no solicitado en relación con el website del Cliente, que puedan resultar ilegales, molestos, que infrinjan derechos de propiedad intelectual de terceros, o que de cualquier otro modo constituyan abusos de la red ("Usos No Aceptables"), y el Cliente se compromete a indemnizar a Deloitte por toda responsabilidad, costes y gastos en que Deloitte pueda incurrir como consecuencia de Usos No Aceptables por el Cliente.

DC

(m) El Cliente reconoce que el Cliente y/o sus filiales y sucursales: (i) controlan cualquier dato y base de datos del Cliente, filiales, o de terceros, (los "Datos"), a los cuales tenga acceso Deloitte o que Deloitte deba procesar durante la prestación de los Servicios, y (ii) son los únicos responsables de los Datos frente a los terceros titulares de los mismos incluyendo, a título de ejemplo, empleados y clientes del Cliente. El Cliente garantiza a Deloitte que toda recogida, almacenamiento, proceso y transmisión de los Datos entre el Cliente y sus filiales, entre el Cliente y Deloitte y entre el Cliente y cualquier tercero, se ha realizado hasta la fecha de este Contrato y se realizará en lo sucesivo, en total conformidad con cualquier norma aplicable a la protección de datos. En el marco de este Contrato, Deloitte accederá a y procesará los Datos únicamente por cuenta del Cliente, bajo responsabilidad exclusiva del mismo, siempre de acuerdo con las instrucciones y procesos que el Cliente deberá establecer y comunicar a Deloitte, siendo igualmente responsabilidad del Cliente determinar la existencia y aplicabilidad de normas de protección de datos en cada momento.

(n) Deloitte no estará obligada a iniciar trabajo nuevo o diferente de los Servicios acordados en la Propuesta ("Cambio") en tanto no se haya acordado por escrito el impacto del Cambio sobre el precio y/o el calendario, en su caso. Cuando se produzca una solicitud de Cambio, bien sea a iniciativa del Cliente o de Deloitte, Deloitte presentará una propuesta al Cliente describiendo los Cambios y el impacto de éstos sobre el precio y/o el calendario, en su caso, pudiendo utilizar el documento de solicitud de cambios incluidos en la propuesta (si se hubiese incorporado a la misma). El Cliente comunicará por escrito a Deloitte su conformidad con la propuesta de Cambio, o bien indicará a Deloitte también por escrito que no deberá emprender los Cambios, en cuyo caso Deloitte continuará los Servicios inicialmente pactados.

Sin perjuicio de lo anterior, si a petición del Cliente o con el conocimiento del Cliente, Deloitte realizase trabajo no previsto en la Propuesta o que supere el alcance previsto en la Propuesta, se considerará dicho trabajo como Servicios realizados en el marco de este Contrato, que el Cliente vendrá obligado a pagar a las tarifas indicadas en la Propuesta o a las tarifas que se utilizaron para calcular los honorarios fijados en la Propuesta.

Artículo 12 - Propiedad intelectual y confidencialidad de la propuesta.

Queda prohibida la reproducción, comunicación pública, transformación, total o parcial, gratuita u onerosa, por cualquier medio o procedimiento, sin la autorización previa y por escrito de Deloitte. Esta propuesta es estrictamente confidencial. Si decidiesen no realizar este proyecto con Deloitte, seleccionar otra consultora o utilizar sus recursos internos para llevarlo a cabo, a nuestro requerimiento deberán devolvernos todas las copias de este documento.

Artículo 13 – Independencia de las Firmas

Deloitte se refiere a Deloitte Touche Tohmatsu Limited, (private company limited by guarantee, de acuerdo con la legislación del Reino Unido) y a su red de firmas miembro, cada una de las cuales es una entidad independiente. En www.deloitte.com/about se ofrece una descripción detallada de la estructura legal de Deloitte Touche Tohmatsu Limited y sus firmas miembro.

DC

Condiciones generales de contratación

Aceptación de la contratación

Este documento refleja enteramente el acuerdo entre CNP Assurances SA, sucursal en España y Deloitte Advisory, S.L. referente a los servicios indicados en el mismo y sustituye a cualquier propuesta previa, correspondencia o acuerdo verbal o escrito que pudiera existir.

En caso de conformidad con los términos aquí expuestos, les agradeceríamos que nos devolvieran debidamente firmadas las copias que les adjuntamos de la propuesta y de las Condiciones generales de contratación.

Estamos encantados de tener la oportunidad de prestarles nuestros servicios profesionales y les aseguramos que dedicaremos a este trabajo nuestra mayor atención.

Atentamente,

Deloitte Advisory, S.L.

Fdo.: Rubén Frieiro

En expresión de su consentimiento,

CNP Assurances SA, sucursal en España

Fdo.:

Deloitte.

ANEXO

A PROPUESTA DE COLABORACIÓN

(Oficina de seguridad para la externalización del CISO)

(Principios Éticos Grupo CNP)

ENTRE

CNP ASSURANCES, S.A. SUCURSAL EN ESPAÑA

Y

DELOITTE ADVISORY, S.L.

CNP assurances

ANEXO A PROPUESTA DE COLABORACIÓN

(Oficina de seguridad para la externalización del CISO)

Por medio del presente Anexo se incluye a la propuesta de colaboración (Oficina de seguridad para la externalización del CISO) de mayo de 2022 realizada por Deloitte Advisory, S.L. y debidamente aceptada por CNP ASSURANCES, S.A., Sucursal en España, carta con los principios éticos del Grupo CNP Assurances y cláusula financiera adicional.

Insuring
a more
open world

ÉTICA DE NEGOCIOS,
EL GRUPO CNP ASSURANCES SIGUE FIEL A SUS COMPROMISOS.

La ética es un elemento crucial de los principios corporativos del grupo CNP Assurances.

En un entorno cambiante, nuestro compromiso con valores fundamentales es una posición insoslayable.

La adhesión de CNP Assurances al Pacto Mundial de la ONU en el año 2003 es la prueba más fehaciente de este compromiso.

Fraude, corrupción, tráfico de influencias, conflicto de intereses, blanqueo de capitales son lacras contra las que el grupo CNP Assurances lucha y reafirma una tolerancia cero.
La implementación de medidas enérgicas guían nuestras acciones en nuestras relaciones comerciales, ya sea con nuestros clientes, proveedores o socios comerciales.

También seguiremos atentos al cumplimiento de prácticas comerciales justas.

Esperamos de cada colaborador del Grupo y de nuestros socios un comportamiento ejemplar y responsable.

La satisfacción de los clientes y de nuestros socios es nuestra máxima prioridad y, aunque valoramos el reconocimiento de la calidad del servicio prestado, no queremos recibir regalos, obsequios ni ningún otro beneficio.

De este modo, mantenemos una total imparcialidad en nuestra toma de decisiones y respetamos los principios de integridad y ética del grupo CNP Assurances.

You will find these principles in C@pEthic, our Group code of conduct, on our corporate site at www.cnp.fr and in our policies, available on request.

Stéphane DEDEYAN
Director General

Evelyn TORTOSA
Director Conformidad Grupo

ANEXO A PROPUESTA DE COLABORACIÓN

(Oficina de seguridad para la externalización del CISO)

La Entidad Aseguradora no realizará pago de cantidad alguna que le puedan exponer o impliquen cualquier sanción, prohibición o aplicación de medidas restrictivas, en virtud de resoluciones de cualquier organismo internacional, y en especial, aquéllas promulgadas por las Naciones Unidas, la Unión Europea, los Estados Unidos de América, los Gobiernos Francés o Español, así como cualquier autoridad que pertenezca a los anteriores.

La Entidad Aseguradora tendrá derecho a rescindir los acuerdos o contratos suscritos en el caso de que su contraparte adquiera la categoría de persona sancionada o se le aplique una medida restrictiva, en virtud de resoluciones de cualquier organismo internacional, y en especial, aquéllas promulgadas por las Naciones Unidas, la Unión Europea, los Estados Unidos de América, los Gobiernos Francés o Español, así como cualquier autoridad que pertenezca a los anteriores.

Y en prueba de conformidad ambas partes en el carácter con el que interviene, firman el presente anexo en Madrid a 30 de mayo de 2022

Por duplicado a un solo efecto.

Deloitte Advisory, S.L.	CNP ASSURANCES, S.A., Sucursal en España
Fdo.: Rubén Frieiro	Fdo: David Lattes

ANEXO

A PROPUESTA DE COLABORACIÓN

(Oficina de seguridad para la externalización del CISO)

(Principios Éticos Grupo CNP)

ENTRE

CNP ASSURANCES, S.A. SUCURSAL EN ESPAÑA

Y

DELOITTE ADVISORY, S.L.

CNP assurances

ANEXO A PROPUESTA DE COLABORACIÓN

(Oficina de seguridad para la externalización del CISO)

Por medio del presente Anexo se incluye a la propuesta de colaboración (Oficina de seguridad para la externalización del CISO) de mayo de 2022 realizada por Deloitte Advisory, S.L. y debidamente aceptada por CNP ASSURANCES, S.A., Sucursal en España, carta con los principios éticos del Grupo CNP Assurances y cláusula financiera adicional.

Insuring
a more
open world

ÉTICA DE NEGOCIOS,
EL GRUPO CNP ASSURANCES SIGUE FIEL A SUS COMPROMISOS.

La ética es un elemento crucial de los principios corporativos del grupo CNP Assurances.

En un entorno cambiante, nuestro compromiso con valores fundamentales es una posición insoslayable.

La adhesión de CNP Assurances al Pacto Mundial de la ONU en el año 2003 es la prueba más fehaciente de este compromiso.

Fraude, corrupción, tráfico de influencias, conflicto de intereses, blanqueo de capitales son lacras contra las que el grupo CNP Assurances lucha y reafirma una tolerancia cero.
La implementación de medidas enérgicas guían nuestras acciones en nuestras relaciones comerciales, ya sea con nuestros clientes, proveedores o socios comerciales.

También seguiremos atentos al cumplimiento de prácticas comerciales justas.

Esperamos de cada colaborador del Grupo y de nuestros socios un comportamiento ejemplar y responsable.

La satisfacción de los clientes y de nuestros socios es nuestra máxima prioridad y, aunque valoramos el reconocimiento de la calidad del servicio prestado, no queremos recibir regalos, obsequios ni ningún otro beneficio.

De este modo, mantenemos una total imparcialidad en nuestra toma de decisiones y respetamos los principios de integridad y ética del grupo CNP Assurances.

You will find these principles in C@pEthic, our Group code of conduct, on our corporate site at www.cnp.fr and in our policies, available on request.

Stéphane DEDEYAN
Director General

Evelyn TORTOSA
Director Conformidad Grupo

DC

ANEXO A PROPUESTA DE COLABORACIÓN

(Oficina de seguridad para la externalización del CISO)

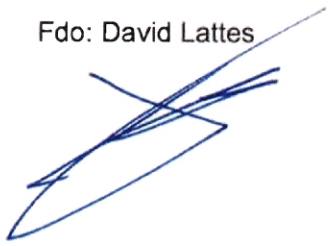
La Entidad Aseguradora no realizará pago de cantidad alguna que le puedan exponer o impliquen cualquier sanción, prohibición o aplicación de medidas restrictivas, en virtud de resoluciones de cualquier organismo internacional, y en especial, aquéllas promulgadas por las Naciones Unidas, la Unión Europea, los Estados Unidos de América, los Gobiernos Francés o Español, así como cualquier autoridad que pertenezca a los anteriores.

La Entidad Aseguradora tendrá derecho a rescindir los acuerdos o contratos suscritos en el caso de que su contraparte adquiera la categoría de persona sancionada o se le aplique una medida restrictiva, en virtud de resoluciones de cualquier organismo internacional, y en especial, aquéllas promulgadas por las Naciones Unidas, la Unión Europea, los Estados Unidos de América, los Gobiernos Francés o Español, así como cualquier autoridad que pertenezca a los anteriores.

Y en prueba de conformidad ambas partes en el carácter con el que interviene, firman el presente anexo en Madrid a 30 de mayo de 2022

Por duplicado a un solo efecto.

Deloitte Advisory, S.L.	CNP ASSURANCES, S.A., Sucursal en España
Fdo.: Rubén Frieiro	Fdo: David Lattes



ANEXO

A PROPUESTA DE COLABORACIÓN

(Oficina de seguridad para la externalización del CISO)

(Principios Éticos Grupo CNP)

ENTRE

CNP ASSURANCES, S.A. SUCURSAL EN ESPAÑA

Y

DELOITTE ADVISORY, S.L.

CNP assurances

ANEXO A PROPUESTA DE COLABORACIÓN

(Oficina de seguridad para la externalización del CISO)

Por medio del presente Anexo se incluye a la propuesta de colaboración (Oficina de seguridad para la externalización del CISO) de mayo de 2022 realizada por Deloitte Advisory, S.L. y debidamente aceptada por CNP ASSURANCES, S.A., Sucursal en España, carta con los principios éticos del Grupo CNP Assurances y cláusula financiera adicional.

Insuring
a more
open world

ÉTICA DE NEGOCIOS,
EL GRUPO CNP ASSURANCES SIGUE FIEL A SUS COMPROMISOS.

La ética es un elemento crucial de los principios corporativos del grupo CNP Assurances.

En un entorno cambiante, nuestro compromiso con valores fundamentales es una posición insoslayable.

La adhesión de CNP Assurances al Pacto Mundial de la ONU en el año 2003 es la prueba más fehaciente de este compromiso.

Fraude, corrupción, tráfico de influencias, conflicto de intereses, blanqueo de capitales son lacras contra las que el grupo CNP Assurances lucha y reafirma una tolerancia cero.
La implementación de medidas enérgicas guían nuestras acciones en nuestras relaciones comerciales, ya sea con nuestros clientes, proveedores o socios comerciales.

También seguiremos atentos al cumplimiento de prácticas comerciales justas.

Esperamos de cada colaborador del Grupo y de nuestros socios un comportamiento ejemplar y responsable.

La satisfacción de los clientes y de nuestros socios es nuestra máxima prioridad y, aunque valoramos el reconocimiento de la calidad del servicio prestado, no queremos recibir regalos, obsequios ni ningún otro beneficio.

De este modo, mantenemos una total imparcialidad en nuestra toma de decisiones y respetamos los principios de integridad y ética del grupo CNP Assurances.

You will find these principles in C@pEthic, our Group code of conduct, on our corporate site at www.cnp.fr and in our policies, available on request.

Stéphane DEDEYAN
Director General

Evelyn TORTOSA
Director Conformidad Grupo

ANEXO A PROPUESTA DE COLABORACIÓN

(Oficina de seguridad para la externalización del CISO)

Por medio del presente Anexo se incluye a la propuesta de colaboración (Oficina de seguridad para la externalización del CISO) de mayo de 2022 realizada por Deloitte Advisory, S.L. y debidamente aceptada por CNP ASSURANCES, S.A., Sucursal en España, carta con los principios éticos del Grupo CNP Assurances y cláusula financiera adicional.

Insuring
a more
open world

ÉTICA DE NEGOCIOS,
EL GRUPO CNP ASSURANCES SIGUE FIEL A SUS COMPROMISOS.

La ética es un elemento crucial de los principios corporativos del grupo CNP Assurances.

En un entorno cambiante, nuestro compromiso con valores fundamentales es una posición insoslayable.

La adhesión de CNP Assurances al Pacto Mundial de la ONU en el año 2003 es la prueba más fehaciente de este compromiso.

Fraude, corrupción, tráfico de influencias, conflicto de intereses, blanqueo de capitales son lacras contra las que el grupo CNP Assurances lucha y reafirma una tolerancia cero.
La implementación de medidas enérgicas guían nuestras acciones en nuestras relaciones comerciales, ya sea con nuestros clientes, proveedores o socios comerciales.

También seguiremos atentos al cumplimiento de prácticas comerciales justas.

Esperamos de cada colaborador del Grupo y de nuestros socios un comportamiento ejemplar y responsable.

La satisfacción de los clientes y de nuestros socios es nuestra máxima prioridad y, aunque valoramos el reconocimiento de la calidad del servicio prestado, no queremos recibir regalos, obsequios ni ningún otro beneficio.

De este modo, mantenemos una total imparcialidad en nuestra toma de decisiones y respetamos los principios de integridad y ética del grupo CNP Assurances.

You will find these principles in C@pEthic, our Group code of conduct, on our corporate site at www.cnp.fr and in our policies, available on request.

Stéphane DEDEYAN
Director General

Evelyn TORTOSA
Director Conformidad Grupo

ANEXO A PROPUESTA DE COLABORACIÓN

(Oficina de seguridad para la externalización del CISO)

La Entidad Aseguradora no realizará pago de cantidad alguna que le puedan exponer o impliquen cualquier sanción, prohibición o aplicación de medidas restrictivas, en virtud de resoluciones de cualquier organismo internacional, y en especial, aquéllas promulgadas por las Naciones Unidas, la Unión Europea, los Estados Unidos de América, los Gobiernos Francés o Español, así como cualquier autoridad que pertenezca a los anteriores.

La Enticad Aseguradora tendrá derecho a rescindir los acuerdos o contratos suscritos en el caso de que su contraparte adquiera la categoría de persona sancionada o se le aplique una medida restrictiva, en virtud de resoluciones de cualquier organismo internacional, y en especial, aquéllas promulgadas por las Naciones Unidas, la Unión Europea, los Estados Unidos de América, los Gobiernos Francés o Español, así como cualquier autoridad que pertenezca a los anteriores.

Y en prueba de conformidad ambas partes en el carácter con el que interviene, firman el presente anexo en Madrid a 30 de mayo de 2022

Por duplicado a un solo efecto.

Deloitte Advisory, S.L.

Fdo.: Rubén Freire

CNP ASSURANCES, S.A., Sucursal en España

Fdo: David Lattes

Hoja de Control: Documentación a Firmar

(Esta hoja deberá ser entregada junto con la Ficha de Selección de Proveedor)

Fecha:	Mayo de 2022						
Sociedad:	CNP ASSURANCES						
Tipo de documento:	Contrato /Anexos ☐	Presupuesto/ Proyecto ☐	Doc. Consejo ☐	Doc. Hacienda ☐	Doc. DGSFP ☐	Doc. Planes/EPSV ☐	Otro: PROPUESTA DE COLABORACION
Solicitado por: *(Director del CODIR)*	DAVID LATTES						
Contenido / Objetivo: Principal Acuerdo, entregables y descripción del servicio	DELOITTE: Oficina de seguridad para la externalización del CISO						

Cumplimentar en caso de contrato, presupuestos, proyectos, u obligaciones de pago

Denominación del Documento:	PROPUESTA DE COLABORACION		
Apoderado/s de CNP: *(según importe económico del contrato)*[1]	DAVID LATTES		
Contraparte: *(proveedor, o interviniente)*	DELOITTE: RUBEN FRIEIRO		
Fecha de inicio del contrato:	01.09.2022		
Fecha de vencimiento del contrato:	31.12.2022		
Transferencia de datos:	☐ S/N	Tipo de Tratamiento: Encargado ☐	Responsable ☐ Corresponsable ☐
Renovación Tácita:	☐ SI ☐ NO		
Preaviso Cancelación:	☐ SI ☐ NO	Especificar preaviso:	
Penalización por cancelación:	☐ SI ☐ NO	Importe:	
Actualización precio por IPC, etc.:	☐ SI ☐ NO		
Delegación actividades críticas:	☐ SI ☐ NO	Especificar:	
KPI / SLA:	☐ SI ☐ NO		
Presupuestado:	☐ SI ☐ NO	Importe (IVA incluido):	
Código CECO:			
Código PEP:			
Activable:	☐ SI ☐ NO		
Periodicidad del pago:	Mensual ☐	*Trimestral* ☐	*Anual* ☐ *Pago único* ☐

- OBLIGATORIO-

Responsable del Departamento y Director del CODIR correspondiente:	Fecha:	Firma:	Firma:
Verificación de Control Financiero: *En el caso de que el gasto sea activable.*	Fecha:	Firma:	
Verificación de Control de Gestión: *En el caso de que el gasto esté presupuestado y el pedido o la factura no superen el presupuesto, no será necesaria la firma del Control de Gestión.*	Fecha:	Firma:	
Revisión Asesoría Jurídica: *(persona del equipo legal que ha revisado el contrato y verificado que cumple con todos los requerimientos solicitados)*	Fecha: 30/05/2022	Firma:	
Comentarios Asesoría Jurídica:			
Verificación de Compras: TV	Fecha: 30 5.22	Firma:	
Director General o Directora Operativa o Directora Financiera:	Fecha:	Firma:	
Director General o Directora Operativa:	Fecha: 01.06.22	Firma:	

(1) Véase rangos de importes económicos según hoja de pedido.

Creación 17/02/2022

Deloitte.

Oficina de seguridad para la externalización del CISO

Propuesta de colaboración

Mayo de 2022

Los sectores en los que operan nuestros clientes son muy competitivos. La confidencialidad de la información es crítica. Deloitte protegerá la confidencialidad de la información de sus clientes.

Deloitte manifiesta explícitamente su compromiso con CNP Assurances de mantener estricta confidencialidad con respecto a este proceso y a cualquier información recibida durante el mismo.

Entendemos que nuestros análisis, técnicas, metodologías y herramientas expuestas en este documento son propiedad privada de Deloitte y esperamos que nuestros clientes también protejan su confidencialidad.

Bajo ninguna circunstancia deben compartirse con terceras personas ajenas a la Dirección de CNP Assurances sin el consentimiento expreso y por escrito de Deloitte.

Deloitte.

Deloitte Advisory, S.L.
Torre Picasso
Plaza Pablo Ruiz Picasso, 1 28020
Madrid, España
+34 915145000
www.deloitte.es

Oficina de ciberseguridad

Mayo de 2022

Estimados,

En respuesta a su solicitud, nos complace presentarle para su consideración nuestra propuesta de servicios profesionales relacionados con la puesta en marcha de un servicio de CISO as a Service que sirva de apoyo a CNP Assurances SA, sucursal en España para el liderazgo, coordinación, ejecución y gestión de las iniciativas de seguridad que sean necesarias durante la actividad de la entidad.

Siendo conscientes de la importancia que este trabajo tiene para ustedes, hemos elaborado esta propuesta considerando la participación de nuestras herramientas y personal más adecuado para este tipo de trabajo.

Los objetivos, alcance y descripción del servicio se exponen en la propuesta de servicios profesionales adjunta. El planteamiento descrito en ella es, a nuestro juicio, el que mejor responde a sus necesidades. Sin embargo, estamos a su entera disposición para estudiar cualquier otro enfoque alternativo que ustedes consideren más apropiado.

De acuerdo con nuestros procedimientos, les agradeceríamos nos remitiesen por escrito su aprobación a la presente propuesta en caso de conformidad con la misma.

Agradecemos muy sinceramente la oportunidad que nos brindan de ofrecerles nuestros servicios y les aseguramos nuestro mayor interés y dedicación en la realización del trabajo de esta propuesta, si nos fuera confirmada.

Sin otro particular, aprovechamos la ocasión para saludarle.

Rubén Frieiro

Socio

Daniel Hernández

Director

Índice


Si crees que la tecnología puede solventar tus problemas de seguridad, entonces no entiendes los problemas y no entiendes de tecnología
Bruce Schneier

Entendimiento de la problemática actual

¿Por qué una entidad no dispone de un CISO?

Sensación de ausencia de peligro

No somos un objetivo, no tenemos nada que le pueda importar a nadie

Sensación de impunidad

No tenemos una regulación ni un regulador que nos supervise o nos sancione

Ausencia de conocimiento experto

No tenemos recursos para contratar un CISO experimentado

Ausencia temporal del CISO

La entidad dispone de un CISO, pero durante un tiempo no podrá ejercer su función

¿Cuáles son las situaciones más comunes por las que una entidad no dispone de un CISO?

Entendimiento de la problemática actual

¿Por qué una entidad no dispone de un CISO?

Sensación de ausencia de peligro

No somos un objetivo, no tenemos nada que le pueda importar a nadie

Sensación de impunidad

No tenemos una regulación ni un regulador que nos supervise o nos sancione

Ausencia de conocimiento experto

No tenemos recursos para contratar un CISO experimentado

Ausencia temporal del CISO

La entidad dispone de un CISO, pero durante un tiempo no podrá ejercer su función

Si no tienes clientes, empleados, proveedores, inversores, competidores, propiedad intelectual, procesos de negocio..., efectivamente no serás un objetivo para ningún atacante potencial. Sin embargo, esto implicará que no tienes actividad, por lo que no tienes un negocio.

Recientes ataques de tipo *ransomware* demuestran que nadie está fuera del alcance de los ataques. La cada vez mayor interconexión de los negocios hace que un posible ataque a un proveedor pueda impactarnos significativamente, por lo que todas las entidades pueden verse afectadas. Es por esto por lo que debe existir una figura que gestione sus necesidades en ciberseguridad desde una perspectiva experta. Esta figura ayudará para la toma de decisiones en función del riesgo de la entidad.

Entendimiento de la problemática actual

¿Por qué una entidad no dispone de un CISO?

Sensación de ausencia de peligro

No somos un objetivo, no tenemos nada que le pueda importar a nadie

Sensación de impunidad

No tenemos una regulación ni un regulador que nos supervise o nos sancione

Ausencia de conocimiento experto

No tenemos recursos para contratar un CISO experimentado

Ausencia temporal del CISO

La entidad dispone de un CISO, pero durante un tiempo no podrá ejercer su función

El hecho de que las regulaciones que afectan a la entidad puedan no exigir explícitamente la figura de CISO no implica que la misma no deba ser tenida en cuenta. La gestión de los riesgos de ciberseguridad, mediante la definición, supervisión, implementación y operación de las medidas de ciberseguridad es responsabilidad del CISO, siendo necesaria una figura experta que las soporte.

Además de todo esto, son precisamente las regulaciones actuales (y sus correspondientes sanciones) las que suponen una palanca importante para abordar la mitigación de los riesgos de ciberseguridad (GDPR, Solvencia, EIOPA, PCI-DSS, PSD2, NIS, LPIC, etc.).

DL

Entendimiento de la problemática actual

¿Por qué una entidad no dispone de un CISO?

Sensación de ausencia de peligro

No somos un objetivo, no tenemos nada que le pueda importar a nadie

Sensación de impunidad

No tenemos una regulación ni un regulador que nos supervise o nos sancione

Ausencia de conocimiento experto

No tenemos recursos para contratar un CISO experimentado

Ausencia temporal del CISO

La entidad dispone de un CISO, pero durante un tiempo no podrá ejercer su función

Una de las tácticas a corto plazo utilizada en ocasiones por algunas entidades es que personas no expertas en ciberseguridad se hagan cargo de esta función. Sin embargo, la constante evolución de los ataques y las medidas de prevención requieren de un conocimiento experto específico que pueda proporcionar una visión de las necesidades en ciberseguridad ajustada a las necesidades de la entidad. De la misma manera, algunas entidades carecen de un atractivo real para un perfil experto que pueda actuar como CISO.

Evidentemente, no todas las entidades van a necesitar la misma dedicación, pero sí que la misma tenga un nivel de calidad que permita priorizar las iniciativas de seguridad a realizar por lo realmente importante, consiguiendo además que impacten lo menos posible en el negocio.

Entendimiento de la problemática actual

¿Por qué una entidad no dispone de un CISO?

Sensación de ausencia de peligro

No somos un objetivo, no tenemos nada que le pueda importar a nadie

Sensación de impunidad

No tenemos una regulación ni un regulador que nos supervise o nos sancione

Ausencia de conocimiento experto

No tenemos recursos para contratar un CISO experimentado

Ausencia temporal del CISO

La entidad dispone de un CISO, pero durante un tiempo no podrá ejercer su función

Ciertas circunstancias que puedan afectar a la entidad, como una eventual ausencia no programada del CISO, la salida del CISO de la organización, o un cambio de funciones del CISO, pueden implicar un periodo de falta de responsabilidades en materia de ciberseguridad.

Ya sea durante un tiempo corto o como una solución alternativa a la espera de contratación de un nuevo CISO, es necesario disponer de un experto en la materia que pueda liderar las iniciativas en materia de ciberseguridad e identificar nuevos riesgos que puedan afectar a la entidad.

Índice

Objetivos y alcance

Alcance

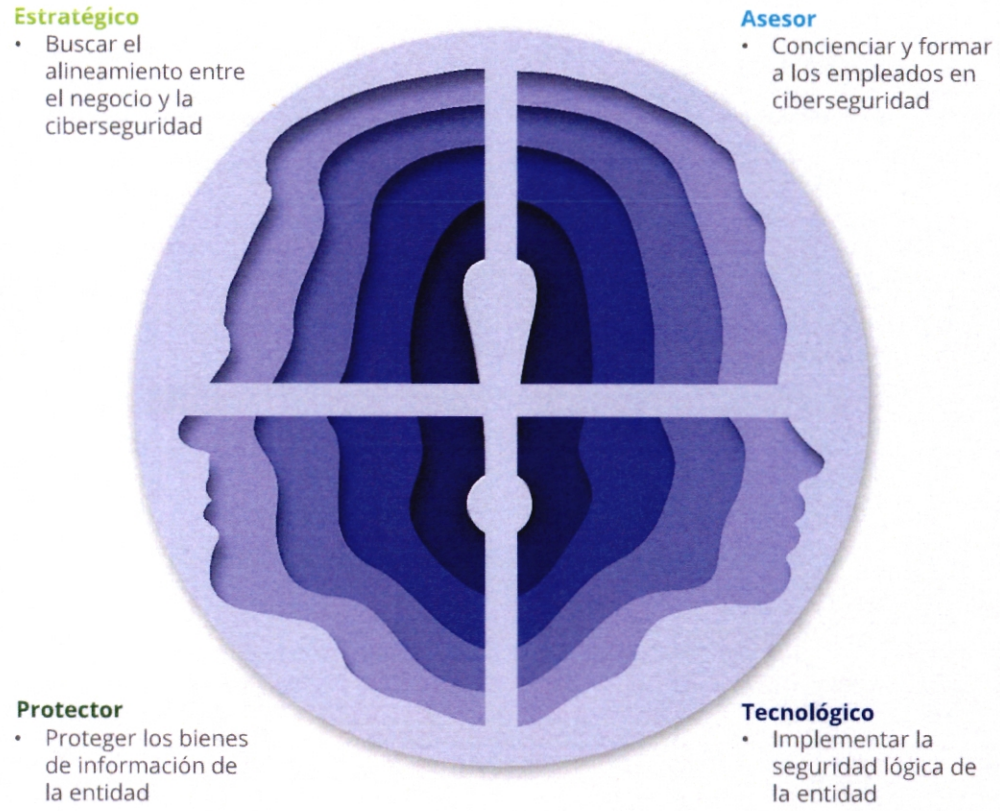
CNP Assurances, consciente de la importancia de la Ciberseguridad en la estrategia y operativa de sus diferentes líneas de negocio, ha acometido un plan de acción a corto plazo con acciones muy básicas que es necesario acometer, coordinados por un servicio de Oficina de ciberseguridad de una duración reducida que externalice ciertas funciones del CISO.

Una vez realizado, se hace necesario acometer un plan a largo plazo que permita a la entidad actualizar su función de seguridad y adecuarla a las amenazas y exigencias regulatorias actuales.

Todo esto hace que CNP Assurances considere necesario disponer de una Oficina de ciberseguridad que permita un adecuado liderazgo, coordinación y gestión de la ejecución de las iniciativas de seguridad de la entidad.

El enfoque de Deloitte propone un servicio que dé soporte en las acciones de seguridad englobando, entre otros proyectos, un análisis inicial que permita realizar dicha planificación y priorización a largo plazo de las diferentes acciones. Esto permitirá al servicio ejercer las labores de liderazgo, coordinación, ejecución y promoción de la ciberseguridad.

ROL DEL CISO



Índice

Referencias

Otras referencias en Oficinas Técnicas de Seguridad y externalización del CISO

A continuación se muestran las referencias permitidas más recientes de las Oficinas Técnicas de Seguridad para la Externalización del CISO (Ciso as a Service) realizadas por Deloitte Advisory, S.L. Las mismas son en gran parte adjudicaciones por tres años, pero se muestra el último año en el que las mismas han sido ejecutadas (la mayor parte con adjudicaciones por tres años).

Año	Proyecto	Cliente
2020	Oficina Técnica de Seguridad	Pelayo
2020	Oficina de SDLC	Banc Sabadell
2020	PMO Ciberseguridad	BBVA
2020	Oficina Técnica para la supervisión de PECA	MAPFRE
2020	Oficina de Lucha contra el fraude	MAPFRE
2020	CISO as a Service	TRIODOS Bank
2020	Oficina Técnica de Seguridad	Wizink
2020	Oficina Técnica de Seguridad Políticas y Normativas	Bankia
2020	Oficina Seguridad	Bankinter
2020	Oficina ciberseguridad Proyectos	Banco Santander
2020	Servicio de Seguridad en Nuevas Iniciativas	MAPFRE
2020	Oficina ciberseguridad	CLH

Año	Proyecto	Cliente
2020	Oficina Técnica de Seguridad	Viesgo
2020	Oficina Técnica de Seguridad	Inversis
2020	Oficina Técnica de Seguridad	Gurit
2020	Oficina de Gobierno y Cumplimiento	RACC
2020	Oficina Técnica de Seguridad	Bankia
2020	Oficina de SDLC	Ayuntamiento de Barcelona
2020	Oficina Ciberseguridad	Codere
2020	Servicio de Revisiones Técnicas	MAPFRE
2019	Asesoramiento en Oficina de Gobierno y Cumplimiento	Liberbank
2019	Oficina de Cumplimiento Normativo	Banca March
2019	Oficina de soporte al cumplimiento de LPIC	Entidad financiera
2019	Oficina Técnica de Seguridad Plan Transformación	Banco Santander
2019	Oficina Técnica de Seguridad Proyectos TyO	Airbus

Índice

Descripción de los servicios ofertados

Enfoque metodológico y aspectos clave de éxito en cada fase

- **Contacto constante durante todo el servicio, no solo en el retorno**
- **Gestión adecuada de la información y documentación**

- **Formalización de responsabilidades**
- **Definición del modelo de reporting del servicio**

Diseño

Conocer la actividad actual y determinar los requerimientos concretos de CNP Assurances para establecer las responsabilidades que asumirá el servicio, las tareas que realizará, y desarrollar el plan de transferencia y captura de conocimiento de áreas expertas de CNP Assurances.

- **Contacto desde el primer día con el responsable**
- **Recopilación de información disponible**
- **Evaluación de la situación y propuestas desde el principio**

Arranque

Puesta en marcha del Servicio: desarrollo de los procedimientos necesarios para su operación. Designación de comités de gobierno del servicio, modelo de relación con CNP Assurances. Inicio del proceso de transformación y madurez del servicio.

- **Reportes periódicos**
- **Comités de seguimiento**

Explotación

Operación normal del Servicio basado en una gestión de la demanda adecuada y de la realización de las actividades conforme a los parámetros de calidad establecidos y conforme a los acuerdos de nivel de servicio acordados en la organización.

Como parte de la explotación se contempla la mejora continua, identificando y gestionando las incidencias y desviaciones en relación al cumplimiento de los objetivos y puesta en marcha acciones correctivas. Mejorar y evolucionar el servicio, dotarlo de nuevas capacidades. Estandarización y automatización de actividades, evolucionar el modelo de madurez.

- **Gestión adecuada de la demanda**
- **Interlocución, coordinación y comunicación**
- **Seguimiento de la actividad e identificación de desviaciones**

Retorno

Asegurar que durante el transcurso del Servicio, se establece un modelo de gestión del conocimiento que permita poner a disposición de terceros o de otras áreas de CNP Assurances el control del Servicio en un plazo de tiempo determinado.

Establecer mecanismos de compartición del conocimiento.

Gestión del Servicio

Calidad y seguimiento

DC

Operación en modo BAU

Descripción de los servicios ofertados

Las labores de un CISO, de un vistazo

Mantenerse al día

- Observatorio de noticias de ciberseguridad y ataques
- Comunicación de tendencias en ciberseguridad
- Análisis de implicaciones de nuevas tendencias tecnológicas y de negocio
- Análisis temprano de impacto de nuevas regulaciones

Gestión

- Identificación de debilidades
- Resolución de dudas de seguridad
- Planificación, lanzamiento y gestión de iniciativas de seguridad
- Colaboración en la selección de proveedores
- Planificación y estimación de presupuestos de seguridad
- Contacto con áreas técnicas y de negocio
- Identificación de requisitos y riesgos asociados a seguridad
- Reporte a la Dirección
- Concienciación en seguridad

Problemas

- Punto de contacto ante problemas
- Comunicación a interlocutores
- Coordinación de involucrados
- Reporte a la Dirección

Descripción de los servicios ofertados

Las labores de un CISO, de un vistazo

Mantenerse al día

- Observatorio de noticias de ciberseguridad y ataques
- Comunicación de tendencias en ciberseguridad
- Análisis de implicaciones de nuevas tendencias tecnológicas y de negocio
- Análisis temprano de impacto de nuevas regulaciones

Aproximación Proactiva.

Screening continuo de noticias sobre nuevas tendencias, normativas y leyes

Aproximación Reactiva.

Requerimientos específicos (ad-hoc) en función de preguntas de la entidad

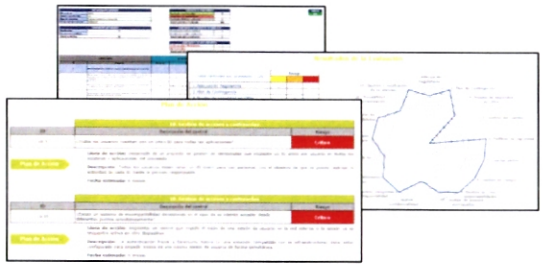
Red de Deloitte.

Presencia en más de 150 países

Ejemplos de reportes que mantendrán al día al CISO

Descripción de los servicios ofertados

Las labores de un CISO, de un vistazo



Selección de proveedores

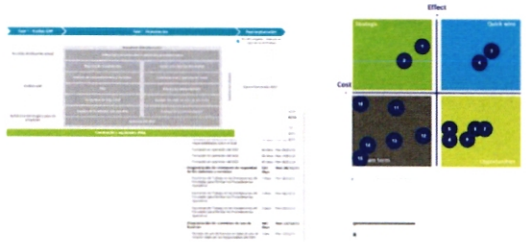
Cuadros de mando de ciberseguridad

Identificación de requisitos y controles

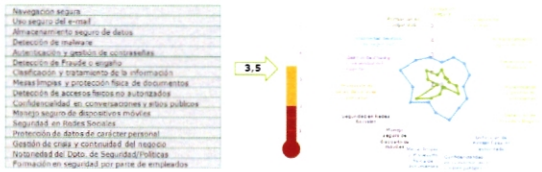
Gestión

- Identificación de debilidades
- Resolución de dudas de seguridad
- Planificación, lanzamiento y gestión de iniciativas de seguridad
- Colaboración en la selección de proveedores
- Planificación y estimación de presupuestos de seguridad
- Contacto con áreas técnicas y de negocio
- Identificación de requisitos y riesgos asociados a seguridad
- Reporte a la Dirección
- Concienciación en seguridad

Reporting a la Dirección



Planificación y gestión de iniciativas



Formación y concienciación en seguridad

Descripción de los servicios ofertados

Las labores de un CISO, de un vistazo

- Definición de canales de comunicación con el servicio de CISO
- Identificación de potenciales escenarios de emergencia
- Revisión, actualización y definición de mecanismos a seguir para la comunicación, tramitación y coordinación en situaciones de emergencias
- Coordinación con los distintos interlocutores según los mecanismos establecidos
- Evaluación del resultado de la gestión, y mejora continua de los mecanismos

El presente servicio no contempla un servicio de resolución de incidentes, sino una labor de liderazgo y comunicación en la coordinación de problemas que puedan surgir en materia de ciberseguridad.

Problemas

- Punto de contacto ante problemas
- Comunicación a interlocutores
- Coordinación de involucrados
- Reporte a la Dirección

Descripción del servicio
Actividades de la Oficina de ciberseguridad

Descripción del servicio

Oficina de Seguridad | Enfoque metodológico

La **metodología** propuesta para la gestión del servicio **se basa en las mejores prácticas y estándares** de referencia existentes en el mercado y **enriquecida con la experiencia adquirida** en proyectos de oficinas técnicas de seguridad e implantación de metodologías de seguridad. El modelo planteado garantiza un enfoque PDCA:

Etapas del ciclo del servicio

Establecimiento	Fase Estable	Retorno
Diseño del servicio	**Explotación del servicio**	**Retorno del servicio**
Conocer la actividad actual y determinar los requerimientos concretos de CNP Assurances para establecer las actividades a realizar y capturar el conocimiento de áreas de competencia del servicio.	Operación normal del servicio basado en una gestión de la demanda adecuada y de la realización de las actividades conforme a los parámetros de calidad establecidos. Como parte de la explotación se contempla la mejora continua del servicio, donde se identifican y gestionan las incidencias y desviaciones en relación al cumplimiento de los objetivos y se ponen en marcha las acciones correctivas. Mejorar y evolucionar el servicio, dotándolo de nuevas capacidades, objetivos y procesos formales. Estandarización y automatización de actividades, evolucionar el modelo de madurez.	Asegurar que durante el transcurso del proyecto, se establece un modelo de gestión del conocimiento que permita la devolución del control a CNP Assurances. Establecer mecanismos de compartición del conocimiento.

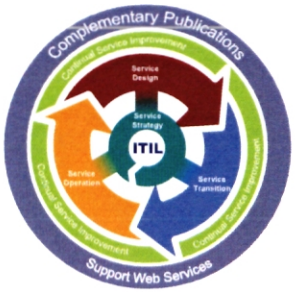
Gestión del servicio

Calidad y seguimiento

DL

Descripción del servicio

Oficina de Seguridad | Enfoque metodológico



Según la información trasladada por CNP Parnerts, la Oficina de cibeguridad de Deloitte estará focalizada en los siguientes ámbitos de trabajo:

- Definir normativa de Seguridad (políticas, procedimientos,) y velar por su cumplimiento.
- Gestión de auditorías. (se daría también el apoyo necesario)
- Gestión diaria del CISO.
- Alinear estrategia de Seguridad con los objetivos de la empresa.
- Interactuar con la alta Dirección en materia de Seguridad de la Información:
  - ✓ Organización de los comités
  - ✓ Participación activa en Comités de Seguridad (métricas, reporting de riesgos, planes de acción, amenazas e incidencias)
- Decisiones relacionadas con la seguridad.
- Soporte/Liderazgo en la implantación al SGSI.
- Marcar la estrategia relacionada con:
  - ✓ Concienciar y transmitir las políticas de seguridad al resto de áreas de IT de CNP
  - ✓ Formación y Concienciación tanto a la alta Dirección como al resto de los empleados.

Para ello se establecerá un equipo de trabajo experto del área de Risk Advisory – Cyber de Deloitte compuesto por un FTE durante 6 meses contando con dos perfiles:

- 1 Perfil consultor senior de la línea **Cyber Strategy**
- 1 Perfil consultor técnico de la línea **Cyber Infrastructure Protection**

Descripción del servicio
Oficina de Seguridad | Diseño del servicio

ANÁLISIS DE REQUISITOS

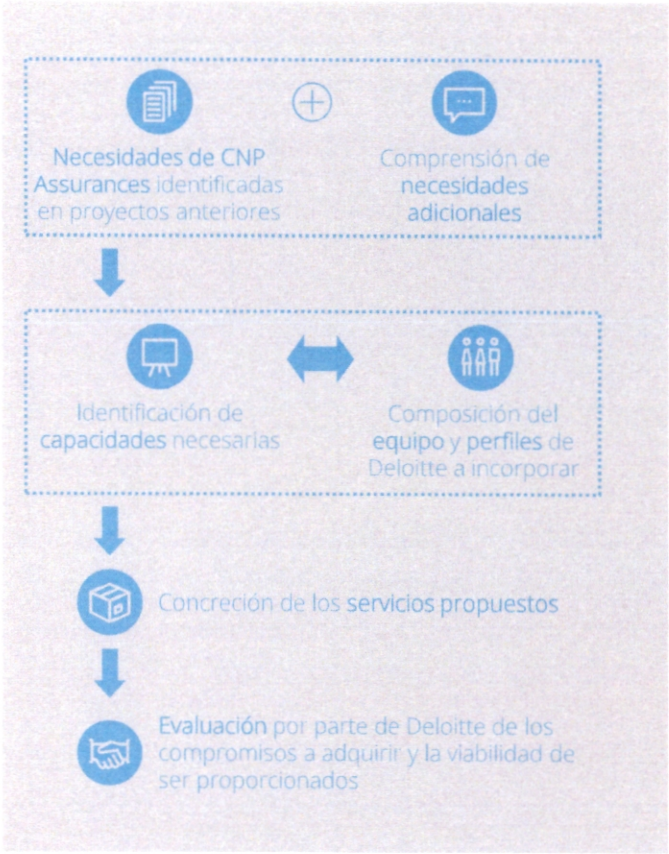
Una vez **analizadas las necesidades de CNP Assurances, se han establecido los servicios** a prestar por la Oficina Técnica de Seguridad. Se ha realizado una primera propuesta conforme a las necesidades comunicadas por CNP Assurances y el conocimiento que tiene Deloitte de la entidad, así como de las expectativas adicionales identificadas.

Los servicios identificados por Deloitte se muestran en la *fase de explotación*. Como parte de la planificación descrita en la propuesta, en la fase de diseño se podría llevar a cabo una **personalización** de dichos servicios conforme a las necesidades de CNP Assurances y la realidad existente.

ESTIMACIÓN DE CAPACIDADES

Conforme a los servicios a acometer, **se han estimado las capacidades necesarias**. Con base en dicho análisis, **Deloitte propone el equipo de trabajo** contenido en la presente oferta, el cual **se considera adecuado para garantizar la mejor prestación** del servicio solicitado.

El detalle de las capacidades solicitadas por CNP Assurances, así como las consideradas necesarias por Deloitte se detallan en el apartado *" Planificación y Equipo de trabajo"*.



Descripción del servicio
Oficina de Seguridad | Diseño del servicio

RESULTADOS ESPERADOS

Como resultado de la fase de diseño se deberá de haber obtenido un conocimiento adecuado de cómo CNP Assurances ejecuta actualmente las tareas a incluir en la Oficina Técnica de Seguridad, así como la especificación de nuevos requerimientos de CNP Assurances en relación al servicio a prestar.

Asimismo, fruto de esta fase se deberá de ser capaz de prestar el servicio actual de cara a su mejora progresiva en fases posteriores. Para ello se habrán documentado:

- **Requisitos cubiertos** por CNP Assurances actualmente que deberán ser asumidos y ejecutados por la Oficina Técnica de Seguridad.
- **Requisitos adicionales** propuestos en las actividades del servicio como parte de la propuesta y que deberán ser integrados en la Oficina Técnica de Seguridad. Para ello se definirán los modelos de integración junto con el equipo de CNP Assurances en la fase de arranque del servicio.
- **Transferencia del conocimiento** actual de CNP Assurances en la ejecución de tareas que pasarán a ser ejecutadas por Deloitte.

Deloitte ha evaluado su capacidad para poder ofrecer a CNP Assurances el servicio planteado, considerando que se dispone de los perfiles y capacidades idóneos para el mismo, así como de herramientas de valor añadido que se pondrán a disposición del Servicio.

En la fase de diseño, debe asegurarse la correcta adquisición del conocimiento técnico/funcional de las tareas ejecutadas actualmente por CNP Assurances, y el contraste de los requisitos demandados en relación a los identificados.

Descripción del servicio

Oficina de Seguridad | Explotación del servicio

Deloitte propone, como parte del servicio, establecer una Oficina Técnica de Seguridad que permita a la entidad disponer de un soporte en materia de Ciberseguridad y Seguridad de la Información

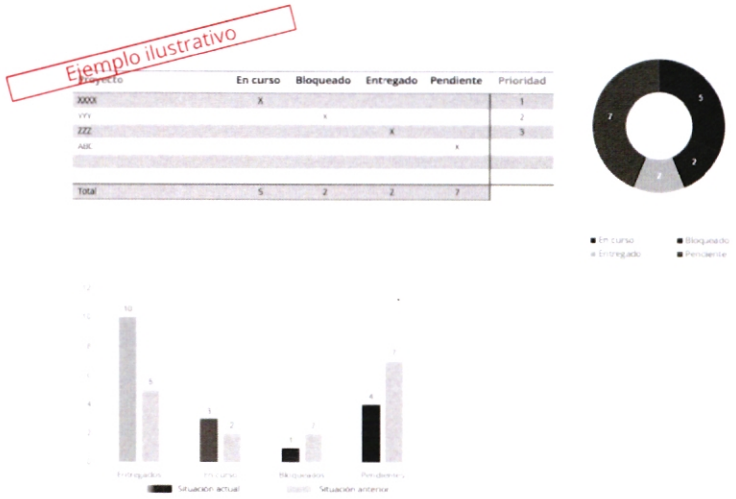
En base a este objetivo, se han definido un conjunto de tareas potenciales que se proponen a continuación, de forma que se pueda realizar el asesoramiento y colaboración circunscrito al ámbito de seguridad de la información.

Como parte del servicio se realizarán parte de estas tareas u otras similares que puedan acometerse dentro de la capacidad planificada para el servicio.

Ejemplos de potenciales tareas a realizar como parte de la colaboración

Seguimiento del cumplimiento Planes de Acción

- Elaboración de un documento ofimático para el seguimiento de los planes de acción que permita realizar un seguimiento adecuado sobre la evolución del cumplimiento.
- Elaboración de un cuadro de mando que permita realizar un adecuado reporting de la situación de los planes de acción (se propone utilizar la herramienta de Power BI Desktop).
- Seguimiento del cumplimiento de los planes y reporte periódico sobre el avance en la elaboración de acciones.



Descripción del servicio

Oficina de Seguridad | Explotación del servicio

Ejemplos de potenciales tareas a realizar como parte de la colaboración

Soporte en reuniones

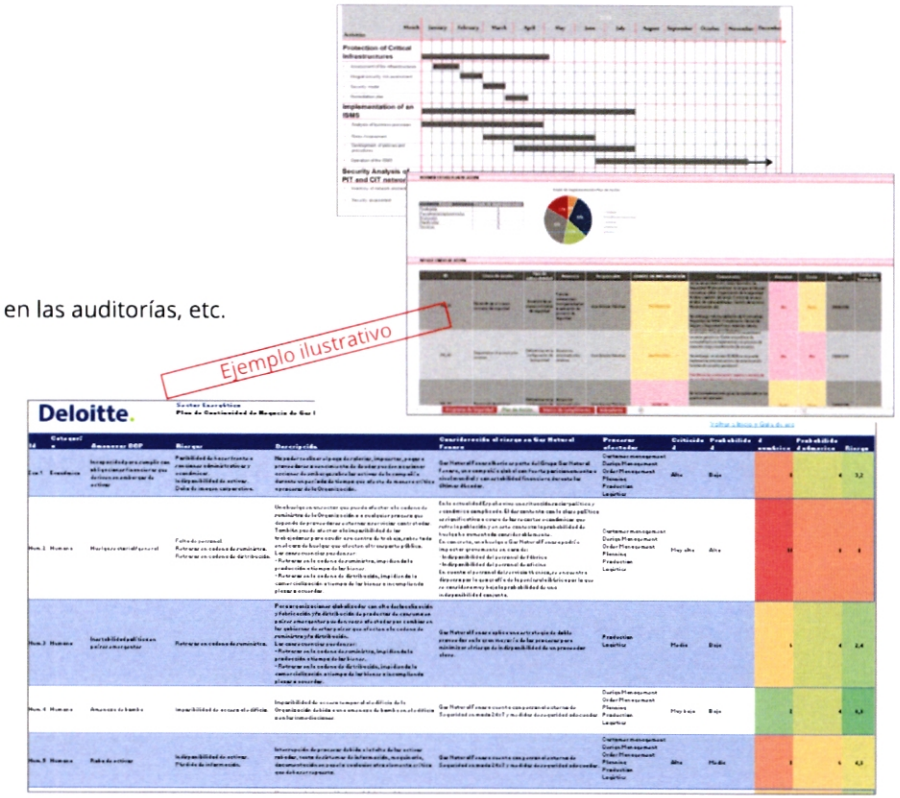
- Elaboración de presentaciones de seguimiento.
- Soporte en las reuniones a los Comités.

Actualización o correcciones referentes al SGSI y SGCN

- Soporte en la actualización del cuerpo normativo de seguridad
- Soporte en la medición de objetivos e indicadores propios de los sistemas de gestión
- Soporte en la elaboración y corrección de hallazgos y oportunidades de mejora detectadas en las auditorías, etc.
- ...

Soporte general

- Soporte adicional al Responsable de Seguridad en tareas asociadas al ámbito de Seguridad de la Información que deberán detallarse como parte del proyecto, como por ejemplo:
  - Asesoramiento sobre nuevas normativas de seguridad desde un punto de vista técnico.
  - Elaboración de presentaciones a demanda
  - Elaboración de documentos relativos a la seguridad de la información



Descripción del servicio

Oficina de Seguridad | Explotación del servicio | Aspectos clave de éxito

Uno de los aspectos de mayor importancia tenidos en cuenta por Deloitte es elaborar entregables que estén formal y correctamente realizados, de forma que el intercambio con los organismos oficiales o auditores sea lo más adecuado posible:

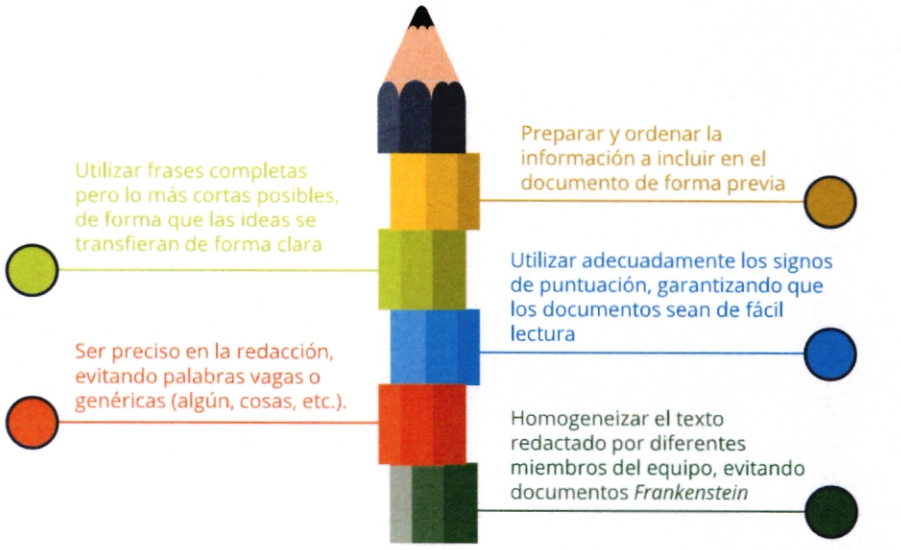
Formalización y revisión de entregables

Deloitte garantiza y pone hincapié en la relevancia de establecer mecanismos para garantizar una excelente redacción y sin errores.

Para ello, Deloitte utiliza los siguientes mecanismos

- Perfiles del área de *Cyber Strategy* encargados de la actualización de los documentos. Estos perfiles tienen un alto conocimiento técnico, pero disponen de unas habilidades muy avanzadas en redacción y elaboración de documentación.
- Los documentos serán realizados por estos perfiles, y serán revisados por parte de un equipo independiente, del gerente responsable y del gerente encargado de garantizar la calidad del trabajo. Los mismos serán:
  - Equipo independiente de revisión de los documentos.
  - Service Delivery Manager del área de *Cyber Strategy*, encargado de garantizar la calidad en los trabajos de ciberseguridad.

Claves de Deloitte en la redacción de los documentos por parte de los perfiles de *Cyber Strategy*



Descripción del servicio

Oficina de Seguridad | Retorno del servicio

CONOCIMIENTO

La información relevante debe ser documentada y compartida de manera permanente entre el equipo del servicio de Deloitte y CNP Assurances para asegurar una adecuada actualización del estado de situación de manera constante.

DOCUMENTACIÓN

Toda documentación generada por el servicio que se considere parte de un entregable o documentación de soporte para la gestión ha de estar accesible, organizada eficientemente y con capacidad de ser explotada.

COMUNICACIÓN

Se han de establecer mecanismos para garantizar que la información relevante es comunicada y conocida por todos los implicados.

La comunicación se considera un aspecto fundamental para garantizar la independencia del proveedor, facilitando a CNP Assurances el control final del servicio y la toma de decisiones relevantes.

HERRAMIENTAS

Tanto en el retorno como en la mejora en la eficiencia del servicio, éste debe proporcionar medios eficientes para facilitar la gestión y transferencia del conocimiento.

Desde Deloitte, se considera fundamental ayudar a CNP Assurances en la creación de herramientas que agilicen los tiempos de respuesta, calidad de reportes y transparencia. El compromiso de Deloitte con esta tarea será máximo para, en el retorno del servicio, facilitar a CNP Assurances estas herramientas.

Descripción del servicio

Oficina de Seguridad | Retorno del servicio

A lo largo del servicio, toda la información relevante deberá ser documentada y trasladada a CNP Assurances, bien en el momento, o bien empleando las herramientas acordadas para la gestión de la documentación y transferencia del conocimiento.

Descripción del servicio
Ejemplos de iniciativas

Descripción de los servicios ofertados

Revisión, mantenimiento y mejora continua de la ciberseguridad

Las siguientes actividades son ejemplos de acciones comúnmente realizadas en este tipo de servicios, si bien las mismas se concretarán como parte de la propia operación, quedando englobadas en actividades relacionadas con el alcance de los servicios definidos en la presente propuesta y de acuerdo al plan definido al comienzo del servicio

Objetivos

El objetivo de este proyecto es potenciar las capacidades de la entidad para dar respuesta a las actividades que permitan establecer una mejora continua de la ciberseguridad.

Esto facilitará al área el seguimiento de todos los proyectos de seguridad gestionados, identificando posibles desviaciones y oportunidades de mejora que faciliten cumplir con la estrategia de ciberseguridad.

Palancas de Deloitte

Conocimiento rápido de la organización gracias a la evaluación del diagnóstico de seguridad que se realizará inicialmente.

Experiencia en la gestión y seguimiento de proyectos de seguridad de las diferentes líneas en diferentes Oficinas Técnicas de Seguridad y PMOs.

Red internacional con un profundo conocimiento del sector, la normativa de seguridad, las últimas tendencias, etc.

Experiencia en proyectos de levantamiento de riesgos y definición de requisitos de seguridad de diferentes tipologías.

Ejemplos de tareas

- Identificar, en función del trabajo realizado, aquellos puntos que requieren un mantenimiento de la normativa de seguridad.
- Seguimiento de proyectos gestionados por el servicio e identificación de desviaciones.
- Seguimiento y dinamización de planes de acción de ciberseguridad y peticiones de otras áreas.
- Seguimiento y reporte de los indicadores de ciberseguridad (relacionado con la elaboración de cuadros de mando).
- Revisión de requisitos de seguridad definidos y adecuación a riesgos actuales de la compañía.
- Identificar oportunidades de mejora en materia de ciberseguridad.
- Revisar el nivel de madurez de la entidad en base al Plan Director de Ciberseguridad una vez esté definido.

Ejemplos de resultados

- Reportes periódicos de seguimiento de proyectos gestionados por el Servicio, y auditorías bajo el scope, junto a la identificación de desviaciones.
- Actualización periódica del nivel de madurez de seguridad en función de los proyectos ejecutados en el Servicio, lo que permitirá conocer el nivel de riesgo de la compañía.
- Reportes de indicadores, junto a oportunidades o acciones a acometer en función de los mismos.

Descripción de los servicios ofertados

Cuerpo normativo de seguridad

Las siguientes actividades son ejemplos de acciones comunmente realizadas en este tipo de servicios, si bien las mismas se concretarán como parte de la propia operación, quedando englobadas en actividades relacionadas con el alcance de los servicios definidos en la presente propuesta y de acuerdo al plan definido al comienzo del servicio

Objetivos

El objetivo de este proyecto es mantener un cuerpo normativo de seguridad completo para gestionar los procesos de ciberseguridad de la compañía.

Esto permitirá a la entidad disponer de unas directrices actualizadas a las últimas tendencias y requisitos regulatorios, asignando las responsabilidades correspondientes, y facilitando el reporting del nivel de cumplimiento de dicho Cuerpo Normativo.

Palancas de Deloitte

Conocimiento de la normativa de ciberseguridad aplicable a la entidad, así como la criticidad de algunas de ellas en el sector en el que ejecuta su actividad.

Red internacional con un profundo conocimiento de la normativa de seguridad, teniendo además a disposición herramientas colaborativas para la compartición de normativa e información de seguridad.

Experiencia en proyectos de adaptación y revisión de cuerpos normativos de seguridad, tanto a nivel proyecto independiente, como formando parte de Oficinas Técnicas de Seguridad.

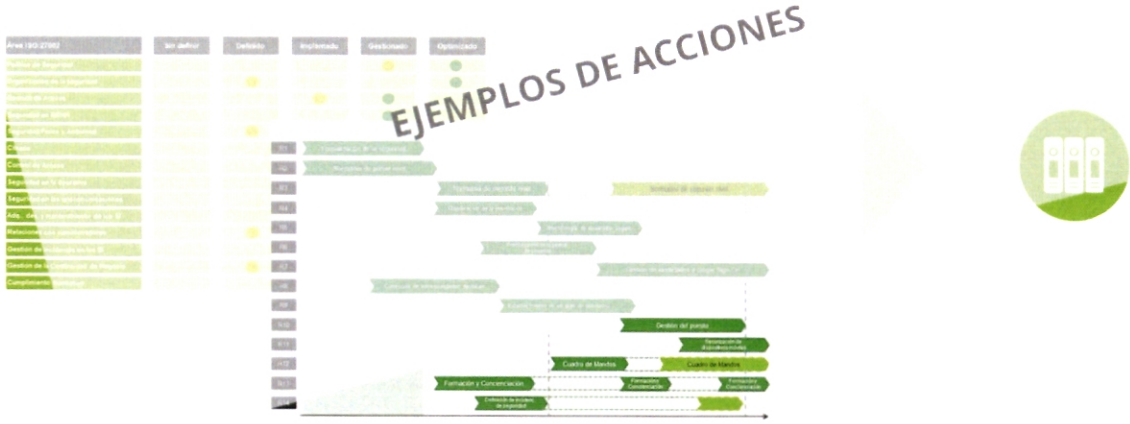
Expertos multidisciplinares en materia de normativa, tanto de Risk Advisory IT y Ciberseguridad, lo que facilita una visión transversal de dicho Cuerpo Normativo.

Ejemplos de tareas

- Revisar periódicamente el Cuerpo Normativo de Seguridad, e identificar aspectos a acometer para definir unos procedimientos que cumplan con los requisitos de seguridad y los procesos de la entidad, detallando, por ejemplo:
  - Descripción de actividades de ciberseguridad controles existentes para asegurar el cumplimiento de las directrices de la política
  - Mecanismos o herramientas de soporte utilizadas
  - Matriz RACI de cada una de las actividades contempladas
  - Listado de indicadores asociados al procedimiento.

Ejemplos de resultados

- Cuerpo Normativo de Seguridad actualizado, adaptado al entorno actual de la entidad y a la normative aplicable.
- Relación de indicadores asociados al Cuerpo Normativo de Seguridad que permitan medir el cumplimiento del mismo.



Descripción de los servicios ofertados

Cuadro de mando de seguridad

Las siguientes actividades son ejemplos de acciones comúnmente realizadas en este tipo de servicios, si bien las mismas se concretarán como parte de la propia operación, quedando englobadas en actividades relacionadas con el alcance de los servicios definidos en la presente propuesta y de acuerdo al plan definido al comienzo del servicio

Objetivos

El objetivo de este proyecto es reforzar el gobierno de la ciberseguridad en la entidad, haciendo más eficiente la identificación de información realmente importante para la organización en su toma de decisiones.

Para ello, Deloitte identificará aquellos indicadores más significativos para la entidad desde diferentes perspectivas (estratégica, económica, cumplimiento, etc.), y elaborará un cuadro de mando visual y fácil de gestionar.

Palancas de Deloitte

Experiencia en la elaboración de cuadros de mando interactivos en herramientas que permiten explotar la información de forma instantánea y visual (por ejemplo, Qlik Sense).

Profunda experiencia en el reporte a todos los niveles, desde la alta dirección a los operadores de seguridad, identificando la información necesaria para cada colectivo en diferentes perspectivas: estratégica, económica, de seguridad, normativa, externa e interna.

Conocimiento del las últimas tendencias en modelos de reporting, lo que facilita a Deloitte una adaptación progresiva con lo que en función de la situación actual de la entidad.

Ejemplos de tareas

- Definición y reporte periódico de un cuadro de mando que englobe todos los aspectos de la ciberseguridad en la entidad:
  - Elaboración de un catálogo de indicadores de cumplimiento que cubran todos los dominios descritos en la política de ciberseguridad, incluyendo los que ya se encuentran definidos.
  - Definición de criterios de medición, incluyendo la periodicidad, y cumplimiento objetivos para cada uno de los indicadores.
  - Establecimiento de responsabilidades de medición y revisión de cada uno de los indicadores.
  - Preparación de una herramienta de soporte para los indicadores que permita obtener el nivel de cumplimiento de cada uno de ellos.
  - Elaboración de una plantilla para el reporte periódico de cumplimiento de los indicadores.

Ejemplos de resultados

- Listado de indicadores a incorporar en el cuadro de mandos de ciberseguridad.
- Plantilla de cuadro de mando para facilitar el reporte periódico para el seguimiento de los indicadores.
- Propuesta de automatización de la generación de cuadro de mando interactivo (tipo Qlik Sense, o similar).
- Metodología y procedimientos para la extracción de información a incorporar en los cuadros de mando periódicos.
- Extracción de información y generación de indicadores periódicos en función de las necesidades de reporting a Comités.

Descripción de los servicios ofertados

Coordinación y reporte a Comités

Las siguientes actividades son ejemplos de acciones comúnmente realizadas en este tipo de servicios, si bien las mismas se concretarán como parte de la propia operación, quedando englobadas en actividades relacionadas con el alcance de los servicios definidos en la presente propuesta y de acuerdo al plan definido al comienzo del servicio

Objetivos

El objetivo de este proyecto es la formalización de un reporting a Comités en materia de ciberseguridad periódico que realice una revisión del estado de la ciberseguridad en la entidad.

En estos Comités, se deben tratar los diferentes aspectos relativos a ciberseguridad, y se apoyarán también en información proporcionada por el resto de proyectos gestionados por el Servicio.

Palancas de Deloitte

Experiencia en la adaptación de modelos de gobierno de seguridad, identificando las necesidades que deben ser implementadas y la forma en la que se debe realizar dicha adaptación.

Conocimiento de los mejores estándares en lo referente a reportes a Comités de Seguridad, de forma que pueda tomar como fuente de información los cuadros de mando para facilitar una toma de decisiones ágil.

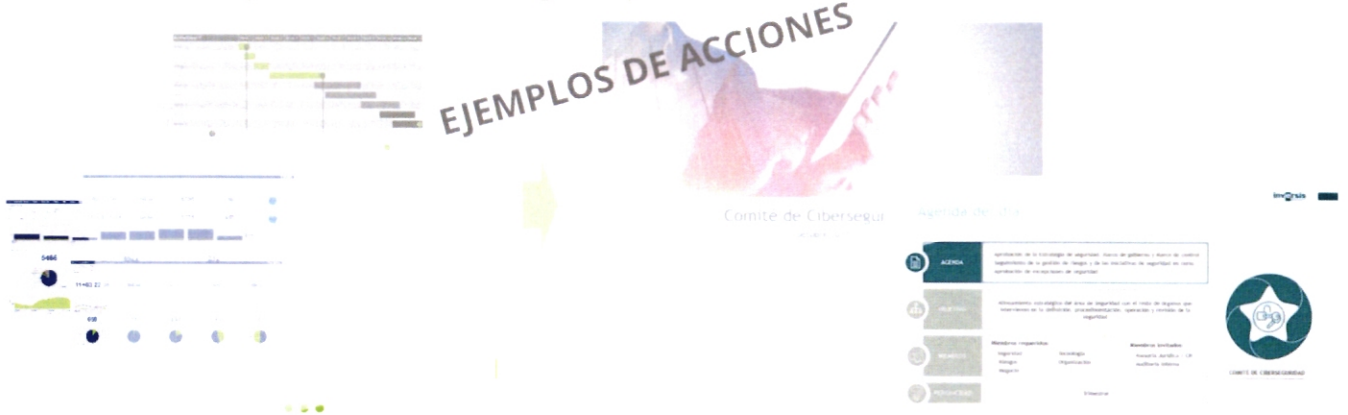
Adquisición rápida del conocimiento de la organización, lo que permite identificar aquellas figuras que son susceptibles de ser miembros (o participar ocasionalmente), en los Comités.

Ejemplos de tareas

- Ampliar las funciones y puntos de revisión de los Comités en materia de ciberseguridad, incluyendo temas como, por ejemplo:
  - Revisión de cambios en la organización o su entorno que afecten a la ciberseguridad
  - Aprobación y revisión de normativa de ciberseguridad así como autorización de excepciones a la misma
  - Estado de cumplimiento de indicadores y objetivos de ciberseguridad
  - Seguimiento de planes de acción y proyectos de ciberseguridad
  - Resultados del análisis de riesgos de ciberseguridad
  - Estado de las diferentes acciones formativas en materia de ciberseguridad
- Establecer los modelos de presentación y documentación soporte a utilizar en los Comités en materia de ciberseguridad.
- Recopilar la información necesaria a incluir en cada Comité en materia de ciberseguridad.
- Elaborar los contenidos de ciberseguridad a incluir en las presentaciones a utilizar en cada Comité.

Ejemplos de resultados

- Modelos de presentación adaptados en materia de ciberseguridad para los Comités.
- Información recopilada a tratar en cada Comité.
- Presentaciones de soporte en materia de ciberseguridad para cada Comité.



Descripción de los servicios ofertados

Soporte normativa de seguridad y estándares

Las siguientes actividades son ejemplos de acciones comúnmente realizadas en este tipo de servicios, si bien las mismas se concretarán como parte de la propia operación, quedando englobadas en actividades relacionadas con el alcance de los servicios definidos en la presente propuesta y de acuerdo al plan definido al comienzo del servicio

Objetivos

El objetivo de esta actividad es potenciar las capacidades de la entidad para la supervisión y seguimiento de las acciones de seguridad relativas a normativas y estándares

Esto facilitará a la entidad tener un control sobre el cumplimiento de ambas normativas, identificando potenciales desviaciones respecto al mismo y definiendo acciones que será necesario acometer.

Palancas de Deloitte

Conocimiento multidisciplinar en Deloitte, que dispone de perfiles de Risk Advisory que también podrán servir de apoyo y consulta por parte del equipo para la resolución de aspectos más relacionados con requisitos regulatorios no de seguridad.

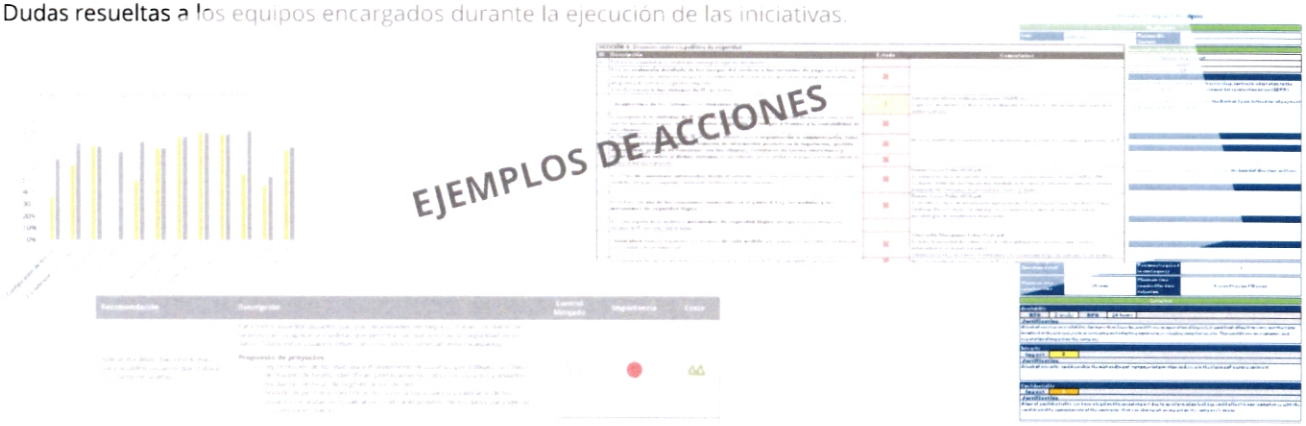
Experiencia en proyectos de adaptación de medidas de seguridad asociadas a normativas, que nos permiten conocer las dificultades a las que se enfrentan las entidades.

Ejemplos de tareas

- Identificar las acciones actualmente definidas en la entidad para la adaptación, y el seguimiento del nivel de cumplimiento en materia de seguridad en lo referente a las normativas como GDPR o estándares como NIST o ISO 27001.
- Dar seguimiento en la ejecución de acciones planificadas a corto plazo.
- Propuesta de ajuste de acciones a realizar a medio-largo plazo.
- Liderazgo de las mismas, identificando acciones e iniciativas que deban ejecutarse en la entidad para adecuarse a las normativas.
- Seguimiento de las iniciativas lanzadas, identificando potenciales desviaciones sobre el plan.
- Asesoramiento específico en materia de seguridad en la ejecución de las iniciativas por parte de los equipos asignados.

Ejemplos de resultados

- Planificación de acciones a realizar para dar seguimiento, e incrementar, el nivel de cumplimiento de GDPR o ISO27001
- Desviaciones identificadas sobre las planificaciones estimadas de iniciativas para la adaptación.
- Dudas resueltas a los equipos encargados durante la ejecución de las iniciativas.



Descripción de los servicios ofertados

Gestión de incidentes de seguridad

Las siguientes actividades son ejemplos de acciones comunmente realizadas en este tipo de servicios, si bien las mismas se concretarán como parte de la propia operación, quedando englobadas en actividades relacionadas con el alcance de los servicios definidos en la presente propuesta y de acuerdo al plan definido al comienzo del servicio

Objetivos

El objetivo de esta actividad es coordinar las acciones a realizar por parte de la entidad en caso de incidente de seguridad.

Esta tarea facilitará una rápida gestión de las acciones y anticiparse a las mismas de cara a que puedan realizarse las acciones más prioritarias que controlen el impacto del incidente.

Ejemplos de tareas

- Identificar el procedimiento de gestión de incidentes de seguridad.
- Mantener actualizado el mismo en función de la situación actual y los pasos que deben darse.
- Coordinar las acciones de acuerdo al procedimiento en función del procedimiento definido.
- Dar seguimiento a las acciones que deben realizarse por parte de cada uno de los involucrados en la entidad.
- Reportar el seguimiento de las acciones a realizar para controlar el incidente.
- Realizar un informe de los resultados producidos por el incidente.

Palancas de Deloitte

Experiencia en la definición de procedimientos para gestión de incidentes de seguridad.

Experiencia en la gestión de incidentes desde un punto de coordinación y también desde la propia **resolución de los mismos,** lo que nos hace conocedores de las principales dificultades a las que se enfrenta la entidad.

Amplia experiencia en ejecución de proyectos de simulaciones de crisis, lo que nos permite conocer de primera mano las reacciones de la alta dirección frente a un ciberincidente, sabiendo identificar los reportes que es necesario realizar y la gestión de los comunicados.

Ejemplos de resultados

- Procedimiento de gestión de incidentes actualizado.
- Seguimiento de acciones en caso de incidentes.
- Informe de resultados y lecciones aprendidas tras la ejecución del incidente.

EJEMPLOS DE ACCIONES

Prevención

Coordinación en época de incidentes

Cierre, resumen y aprendizaje

Descripción de los servicios ofertados

Soporte y supervisión de vulnerabilidades e incidencias SOC

Las siguientes actividades son ejemplos de acciones comúnmente realizadas en este tipo de servicios, si bien las mismas se concretarán como parte de la propia operación, quedando englobadas en actividades relacionadas con el alcance de los servicios definidos en la presente propuesta y de acuerdo al plan definido al comienzo del servicio

Objetivos

El objetivo de esta actividad es dar soporte a la entidad en la supervisión de los proyectos y servicios que actualmente tiene la entidad de análisis de vulnerabilidades e incidencias SOC

Esto permitirá a la entidad interpretar los resultados de los trabajos desde una perspectiva estratégica que facilite la toma de decisiones sobre las acciones a tomar para solucionar potenciales vulnerabilidades, interpretar posibles anomalías en los sistemas, etc.

Palancas de Deloitte

Conocimiento rápido de la organización gracias a que ya tenemos proyectos de hacking en la propia entidad.

Experiencia en la gestión y seguimiento de acciones de forma proactiva.

Capacidad de interlocución en el ámbito técnico y de negocio que facilita ser la interfaz entre los equipos encargados de los aspectos técnicos y las áreas de negocio.

Experiencia en proyectos técnicos de hacking y SIEM dentro de Deloitte que nos permite disponer de expertos que actuarán como soporte para facilitar que el equipo conozca las últimas novedades y tendencias en la materia.

Ejemplos de tareas

- Identificar la planificación de análisis de vulnerabilidades a realizar.
- Dar seguimiento al cumplimiento de la planificación definida.
- Recopilar los resultados de los informes de realizados e interpretación de los mismos.
- Interpretación de los informes y diálogo con los equipos ejecutores para conocer las consecuencias de los resultados.
- Acciones de liderazgo para la solución de las vulnerabilidades identificadas.
- Recopilar los informes sobre eventos destacados realizados a partir del servicio de incidencias SOC.
- Interpretación de los resultados y diálogo con los equipos dedicados al manejo del SOC de cara a profundizar en las consecuencias.
- Seguimiento de la resolución de eventos, incidencias y vulnerabilidades.
- Reporting sobre aquellas incidencias destacables y lanzamiento/seguimiento de acciones para solucionar las mismas.

Ejemplos de resultados

- Interpretaciones de los informes sobre análisis realizados.
- Interpretaciones de los resultados derivados de los eventos identificados por parte del servicio de SIEM.
- Levantamiento y reporting de vulnerabilidades y eventos críticos que sea necesario elevar en la propia entidad.
- Liderazgo y seguimiento de acciones para solucionar las vulnerabilidades y eventos detectados.

Descripción de los servicios ofertados

Seguridad en Proyectos

Las siguientes actividades son ejemplos de acciones comúnmente realizadas en este tipo de servicios, si bien las mismas se concretarán como parte de la propia operación, quedando englobadas en actividades relacionadas con el alcance de los servicios definidos en la presente propuesta y de acuerdo al plan definido al comienzo del servicio

Objetivos

El objetivo de esta actividad es incorporar la seguridad desde una fase temprana de los proyectos, suponiendo un ahorro de costes al minimizar el riesgo y la necesidad de correcciones de vulnerabilidades de los productos en producción.

Esto facilitará a la entidad la reducción de vulnerabilidades y contribuye a generar, fomentar y mantener una buena imagen corporativa, incrementando incluso la reputación de la propia función de TI y Seguridad de cara al resto de Áreas de Negocio.

Palancas de Deloitte

Experiencia en proyectos de establecimiento de enfoques metodológicos para el análisis de riesgos en nuevas iniciativas/soluciones y servicios que forman parte de la estrategia de transformación digital de clientes del sector financiero.

Experiencia en proyectos de levantamiento de riesgos y definición de requisitos de seguridad en **tecnología cloud, aplicaciones móviles, externalización de servicios, servicios como producto, etc.**

Experiencia en el desarrollo, implantación y uso de **herramientas de automatización** de procesos y ejecución de controles.

Catálogos de riesgos y requisitos maduros que facilitan una adaptación rápida a la casuística particular de la entidad.

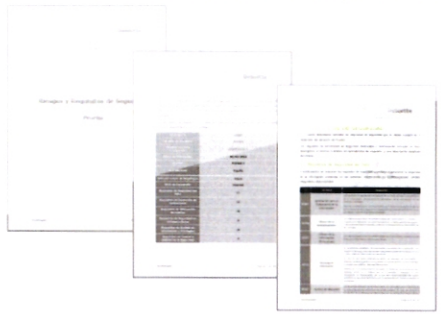
Ejemplos de tareas

- Identificar la metodología de análisis de riesgos y de definición de requisitos actualmente utilizada.
- Identificación, análisis y actualización del catálogo de riesgos y requisitos de seguridad.
- Definición de requisitos de seguridad y/o análisis de riesgos en iniciativas de la entidad que surjan desde el ámbito técnico o relacionados con el propio negocio de la entidad.
- Soporte y seguimiento relativo a la mitigación de los riesgos detectados durante el análisis de viabilidad de la solución.
- Asesorías y consultas en materia de seguridad durante todo el ciclo de vida (relativas a implementación de requerimientos, al respecto de las guías de buenas prácticas, etc.).
- Elaboración de entregables de acuerdo a las metodologías de la entidad y actualización del inventario de iniciativas junto a los parámetros del mismo.
- Identificar posibilidades para automatizar el proceso en función del nivel de madurez de la entidad.

Ejemplos de resultados

- Propuestas de ajustes de la metodología de análisis de riesgos y de definición de requisitos (en caso de que sea necesario).
- Análisis de riesgos e identificación de requisitos ad hoc para aquellas iniciativas que, debido a su criticidad, lo requieran.
- Entregables de las iniciativas según los estándares de la entidad, entre los que se encuentran:
  - Análisis de riesgos.
  - Requisitos de Seguridad.
- Garantía de la asimilación de las medidas de seguridad a implantar por parte de las áreas, mediante un seguimiento y asesoramiento que permita resolver las dudas asociadas a la implantación de los requisitos o a la mitigación de los riesgos detectados.
- Inventario de iniciativas actualizado.
- Identificación de posibilidades para automatizar el proceso.

EJEMPLOS DE ACCIONES



Descripción de los servicios ofertados

Marcos de control

Las siguientes actividades son ejemplos de acciones comúnmente realizadas en este tipo de servicios, si bien las mismas se concretarán como parte de la propia operación, quedando englobadas en actividades relacionadas con el alcance de los servicios definidos en la presente propuesta y de acuerdo al plan definido al comienzo del servicio

Objetivos

El incremento de la presión regulatoria a la que se está viendo sometido el entorno financiero, junto con el avance en la sofisticación de los ciberataques, hacen especialmente importante que las entidades cumplan (y vigilen el cumplimiento) de las regulaciones bajo las que están sometidas.

El objetivo de la presente actividad es mantener un marco de gobierno y control que le permita cubrir los distintos requisitos a los que se encuentra sometida.

Palancas de Deloitte

Red internacional con un profundo conocimiento del sector y la normativa de seguridad, teniendo además a disposición herramientas colaborativas para la compartición de normas e información de seguridad.

Experiencia en proyectos de definición de marcos de control, tanto a nivel proyecto, como formando parte de servicios.

Expertos multidisciplinares en materia de normativa, tanto de Risk Advisory IT y Ciberseguridad.

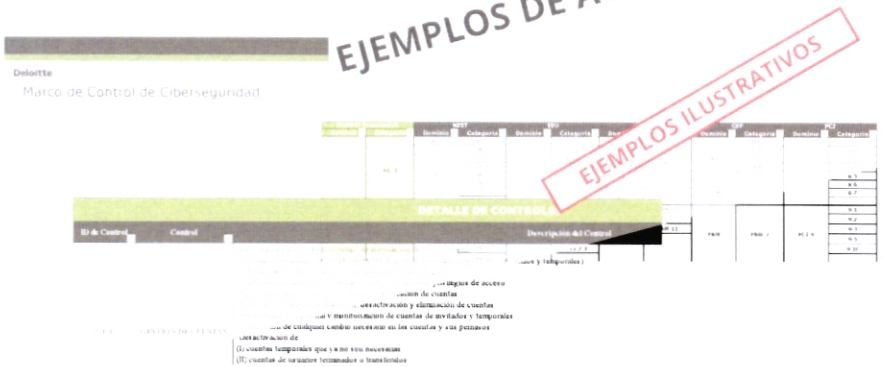
Conocimiento de las normativas aplicables a la entidad y su sector, al haber participado de forma activa en la definición y elaboración de marcos de controles en entidades del sector financiero, lo que facilita un rápido entendimiento de la casuística específica de cada uno de los controles.

Ejemplos de tareas

- Identificar el marco de control, incluyendo aquellos controles relativos a antivirus, firewall, revisión de usuarios, etc.
- Mantener actualizado el marco de control en función de nuevos requisitos regulatorios y normativos que aparezcan.
- Proponer modificaciones en los actuales, identificando aquellos indicadores que pueden ser de especial utilidad.
- Elaborar aquellos cuadros de mando que faciliten la visualización del cumplimiento del marco de gobierno y control de la seguridad.
- Comunicar a los responsables de subsanar las debilidades de control los plazos en los que las mismas deben estar solucionadas.
- Dar seguimiento a las acciones a realizar, comunicando aquellos casos en los que no se esté cumpliendo con los plazos.
- Dar soporte mediante la resolución de dudas en aquellos aspectos de seguridad de la información y riesgos tecnológicos gestionados.

Ejemplos de resultados

- Marco de gobierno y control actualizado.
- Actualización de indicadores y/o cuadros de mando que permitan conocer el nivel de cumplimiento del marco de control.
- Seguimiento de las debilidades.
- Resolución de dudas de los aspectos de seguridad de la información.



Descripción de los servicios ofertados

Coordinación y reporte

Las siguientes actividades son ejemplos de acciones comúnmente realizadas en este tipo de servicios, si bien las mismas se concretarán como parte de la propia operación, quedando englobadas en actividades relacionadas con el alcance de los servicios definidos en la presente propuesta y de acuerdo al plan definido al comienzo del servicio

Objetivos

El objetivo de esta actividad es la formalización del reporting periódico a Comités en materia de ciberseguridad que realice una revisión del estado de la ciberseguridad en la entidad, así como aquellos reportes mensuales que es necesario realizar a la matriz en Francia.

En estos Comités, se deben tratar los diferentes aspectos relativos a ciberseguridad, y se apoyarán también en información proporcionada por el resto de proyectos gestionados por el Servicio.

Palancas de Deloitte

Experiencia en la adaptación de modelos de gobierno de seguridad, identificando las necesidades que deben ser implementadas y la forma en la que se debe realizar dicha adaptación.

Conocimiento de los mejores estándares en lo referente a reportes a Comités de Seguridad, de forma que pueda tomar como fuente de información los cuadros de mando para facilitar una toma de decisiones ágil.

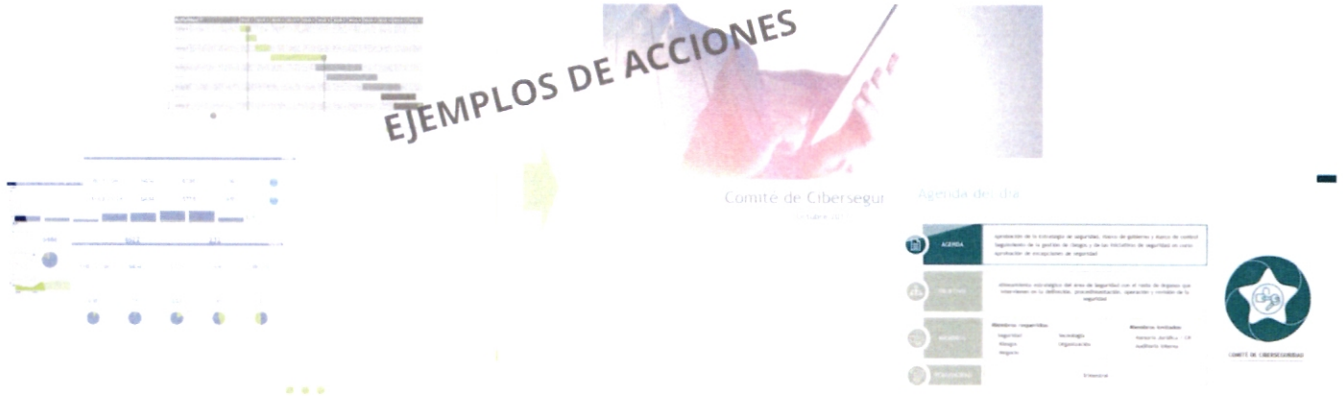
Adquisición rápida del conocimiento de la organización, lo que permite identificar aquellas figuras que son susceptibles de ser miembros (o participar ocasionalmente), en los Comités.

Ejemplos de tareas

- Identificar los reportes actualmente realizados en materia de ciberseguridad, incluidos aquellos realizados mensualmente a Francia.
- Ampliar las funciones y puntos de revisión de los reportes y Comités en materia de ciberseguridad, incluyendo temas como, por ejemplo:
  - Revisión de cambios en la organización o su entorno que afecten a la ciberseguridad
  - Aprobación y revisión de normativa de ciberseguridad así como autorización de excepciones a la misma
  - Estado de cumplimiento de indicadores y objetivos de ciberseguridad
  - Seguimiento de planes de acción y proyectos de ciberseguridad
  - Resultados del análisis de riesgos de ciberseguridad
  - Estado de las diferentes acciones formativas en materia de ciberseguridad
- Actualizar los modelos de presentación y documentación soporte a reportar en materia de ciberseguridad.
- Recopilar la información necesaria a incluir en cada reporte en materia de ciberseguridad.
- Elaborar los contenidos de ciberseguridad a incluir en las presentaciones a utilizar en cada reporte.

Ejemplos de resultados

- Modelos de presentación adaptados en materia de ciberseguridad para los distintos reportes.
- Información recopilada a tratar.
- Presentaciones de soporte en materia de ciberseguridad.



Descripción de los servicios ofertados

Concienciación de usuarios

Las siguientes actividades son ejemplos de acciones comúnmente realizadas en este tipo de servicios, si bien las mismas se concretarán como parte de la propia operación, quedando englobadas en actividades relacionadas con el alcance de los servicios definidos en la presente propuesta y de acuerdo al plan definido al comienzo del servicio

Objetivos

La estrategia de protección de la información de cualquier organización debe incluir la adecuada preparación de sus empleados y colaboradores con acceso a los sistemas de información ante las nuevas ciberamenazas que buscan explotar el eslabón más débil dentro de la cadena de la seguridad de la información: el factor humano.

Para ello, las actividades concienciación y divulgación se deben orientar para preparar a los diferentes colectivos de trabajadores respecto a los riesgos identificados.

Palancas de Deloitte

Metodología novedosa propia de concienciación y formación en seguridad basada en los siguientes principios:

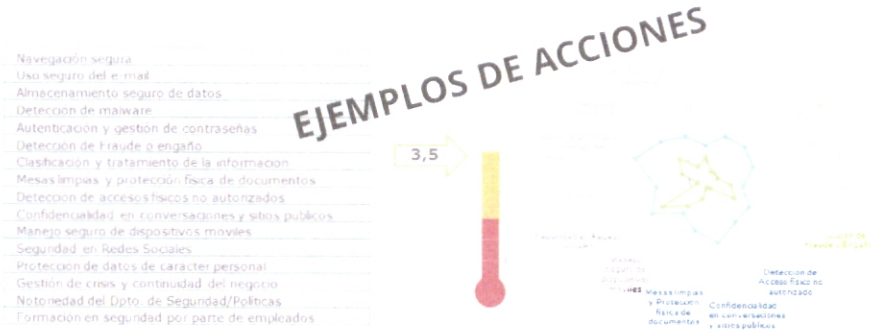
- **Medición del nivel de madurez en concienciación**. No se puede mejorar lo que no se puede medir.
- **Comparativa del nivel de madurez de la Compañía con otras compañías** similares, que ayudará a definir el nivel objetivo.
- Búsqueda de las motivaciones que hagan un cambio en el comportamiento de los empleados. Esto lo realizan perfiles especialistas en Marketing y Publicidad, mediante un **Mapa de Empatía**.
- Diseño del Plan de Concienciación incorporando **acciones eficaces en la concienciación**, y no basadas en la formación.

Ejemplos de tareas

- Identificación de colectivos para formación.
- Medición del AS-IS en concienciación, a través de cuestionarios, debilidades identificadas en las personas, etc.
- Definición de necesidades de formación y concienciación.
- Definición del TO-BE en concienciación
- Desarrollo y coordinación de material de formación y concienciación, recopilando el material que tenga actualmente la entidad y manteniéndolo actualizado.
- Ejecución y seguimiento de acciones formativas y de concienciación

Ejemplos de resultados

- Seguimiento y actualización del plan de concienciación, material asociado actualizado y ejecución de acciones de concienciación.



Ejemplo ilustrativa del nivel de madurez ***en concienciación de ciberseguridad***

Índice

Planificación

Calendario previsto para las fases de diseño y arranque

La **fase de explotación** contempla las actividades de asesoramiento descritas en la presente oferta, iniciándose desde el comienzo de la fase de diseño.

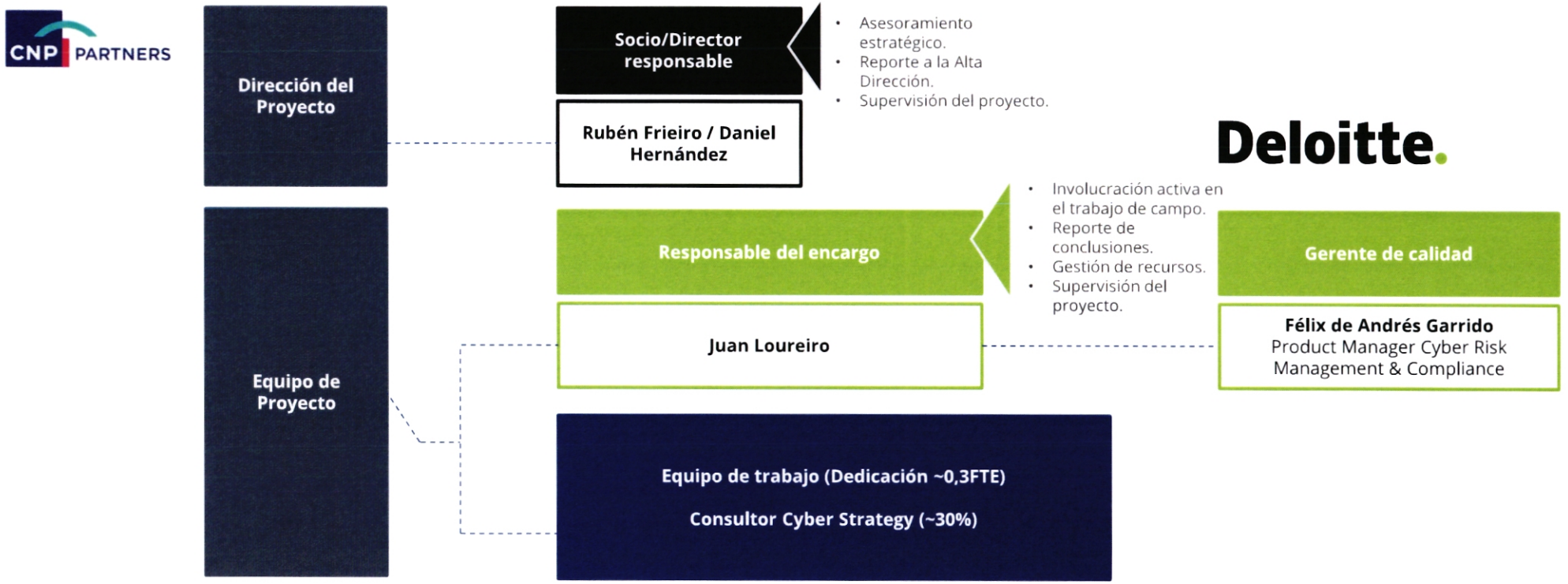
Durante la **fase de arranque** se irán produciendo modificaciones sobre la explotación del servicio conforme se acuerde entre Deloitte y CNP Assurances.

Índice

Equipo de proyecto propuesto

Modelo de relación

En base a nuestra experiencia proponemos un modelo de organización del proyecto basado en una asignación de responsabilidades y tareas de coordinación y cooperación de los equipos de trabajo de la siguiente forma:



Equipo de proyecto propuesto
Modelo de gobierno

Propuesta de establecimiento de responsabilidades

Rol	CNP Assurances	Deloitte	Descripción del rol
Responsable del contrato	Dirección de CNP Assurances	Equipo directivo Deloitte (Socio y Gerente)	CNP Assurances asume la dirección del servicio con el asesoramiento de Deloitte, tanto desde el punto de vista técnico como administrativo del contrato, con las actividades descritas en el pliego de contratación.
Gestor del Servicio	Responsable del Servicio	Gestor del servicio de Deloitte	Asumen la gestión operativa del servicio, de su seguimiento periódico y la mejora continua del mismo. Tiene por objeto evaluar la calidad del asesoramiento ofrecido.
Equipo de trabajo	Equipo de trabajo	Equipo de trabajo	Es el encargado de la prestación del servicio, de acuerdo a las actividades descritas.

Implicación

Se dispondrá de un equipo de trabajo, de los cuales uno de ellos realizará las tareas de gestión del servicio. Asimismo, el Responsable del Contrato y Deloitte se comprometen a implicarse en la correcta prestación del servicio, en la subsanación temprana de ineficiencias, y en la participación activa en comités y tareas que requiera y demande CNP Assurances.

Comités

Si bien se definirán comités periódicos, Deloitte se compromete a adaptarse a las necesidades concretas de CNP Assurances en la realización de Comités y reuniones.

Perfiles

Cada uno de los perfiles dispondrá de skills concretos potenciados en ciertas disciplinas como parte del servicio. Entre las habilidades identificadas se encuentran el conocimiento de la normativa, ciberriesgos, seguridad y modelos de gobierno. En este sentido, todos los miembros tendrán skills que permitan asumir el balanceo de carga en caso de necesidad, teniendo proactividad en la realización de las tareas y trato con los interlocutores de la entidad..

Procesos de gestión

Como parte del servicio, Deloitte hará un repaso a los procesos existentes de gestión del servicio y explotación de actividades para su adaptación a las actividades y necesidades de CNP Assurances.

Equipo de proyecto propuesto
Modelo de gobierno

Como parte del modelo de Gobierno, se contará Comités para asegurar el control y seguimiento del servicio de manera formalizada, donde se llevará a cabo el seguimiento de la actividad, indicadores, niveles de servicio establecidos, toma de decisiones asociadas a la gestión del servicio, etc.

Propuesta de comités internos del servicio

Comité	Asistentes	Descripción
Comité de dirección	Responsables del contrato y gestores del servicio	CNP Assurances coordina y desarrolla las actividades previstas para los responsables del contrato con el asesoramiento de Deloitte con la finalidad de analizar la calidad percibida del servicio, evaluar las necesidades de mejora en la prestación del mismo.
Comité operativo	Responsable del servicio de CNP Assurances, responsable de la ejecución de Deloitte, gerente responsable de Deloitte	En dicho Comité se abordará el estado actual de las acciones, el avance, los problemas existentes y la resolución de incidencias que pudieran ocurrir en las tareas.
Comité de calidad	Equipo directivo Deloitte y gestor del servicio	Coordinar y desarrollar de manera conjunta las actividades relacionadas con la gestión de la calidad del proyecto, teniendo en cuenta el manual de calidad de Deloitte. Este comité será interno del proveedor.

Equipo de proyecto propuesto

Roles y responsabilidades

Roles	Responsabilidades	Dedicación
Socio responsable	• Interlocución de Alto nivel, máximos responsables de la correcta ejecución del proyecto • Conocimiento de la cuenta y aportación de experiencia en proyectos similares • Revisión de calidad de los entregables de proyecto	Part Time
Responsable del encargo	• Gestión del equipo, distribución de tareas, reporte y revisión de la calidad de los entregables del proyecto • Soporte y seguimiento continuo de las necesidades	Part Time
Gerente de Calidad	• Aseguramiento de la calidad y provisión de recursos especializados • Gestión del equipo, distribución de tareas, reporte y revisión de la calidad de los entregables del proyecto • Soporte y seguimiento continuo de las necesidades	Part Time
Equipo de trabajo	• Llevar a cabo las tareas definidas en la presente propuesta.	Full time

Equipo de proyecto propuesto

Currículums | Socio del encargo

Rubén Frieiro Barros

Socio del proyecto

22 años de experiencia

rfrieiro@deloitte.es

Descripción

Trayectoria profesional

- Rubén se incorporó a Deloitte en 1999, como consultor del grupo de gestión de riesgos tecnológicos, encargado de la ejecución y dirección técnica de diferentes encargos de control interno y auditoría informática y consultoría sobre seguridad de la información.
- En 2005, es nombrado gerente del grupo Risk Advisory IT, con competencias en el desarrollo de servicios en el sector financiero (Seguros y Banca), experto en las áreas de Seguridad de la Información, Cumplimiento Normativo y Auditoría de Sistemas.
- En el 2015 es promocionado a Socio del grupo de Riesgos Tecnológicos, en las áreas de especialización de Auditoría Informática y Ciberseguridad.
- A lo largo de su trayectoria profesional ha colaborado en numerosas iniciativas sectoriales, como asesor del Centro Nacional de Protección de Infraestructuras Criticas para el desarrollo de los Planes Estratégicos Sectoriales de Protección de Infraestructuras Criticas.
- En la actualidad es miembro de la Comisión de Innovación y Tecnología del Instituto de Censores Jurados de Cuentas.

Formación académica y titulaciones

- Ingeniero de Telecomunicaciones por la Universidad de Vigo.
- Experto Universitario en Dirección de Seguridad por la UNED.
- CISA (Certified Information Systems Auditor).
- CISM (Certified Information Security Manager).
- CISSP (Certified Information Systems Security Professional).
- CSSLP (Certified Security Software Lifeclycle Professional).
- CRISC (Certified in Risk and Information Systems Control).
- ISO 27001 Lead Auditor.
- ITIL Foundations V3.

Otros datos de interés profesional

- Profesor en el Master de Auditoría Informática de la Universidad Politécnica de Madrid en los años, 2003, 2004, 2005, 2006, 2011, 2012.
- Profesor en el Master de Dirección y Gestión de la Seguridad de la Información de la Universidad Politécnica de Madrid en los años, 2012, 2013 y 2014.
- Profesor en el master de Ciberseguridad de la Universidad Carlos III de Madrid, año 2015.
- Experto colaborador en el diseño del plan de estudios del master de Ciberseguridad de la UC3M.
- Miembro del Colegio Oficial de Ingenieros de Telecomunicaciones.
- Idiomas: Español, Gallego, Inglés.

Principales proyectos

- Revisiones de controles generales del ordenador y de la realización de pruebas de datos.
- Servicios de riesgos tecnológicos en el sector servicios y medios de pago.
- Consultoría de seguridad de la información.
- Elaboración de planes directores de seguridad, adaptaciones a la LOPD, la implantación de planes de continuidad de negocio, revisiones de seguridad y hacking ético, planes de protección de la información, concienciación en seguridad o implementación de sistemas de gestión dela seguridad.
- Implantación de herramientas para la gestión del cumplimiento normativo, integridad de la información y calidad de datos.

Principales clientes

- MAPFRE
- Banco de España
- Inditex
- Arcelor Mittal
- Ferrovial

Equipo de proyecto propuesto

Currículums | Director de la práctica Cyber en sector asegurador

Descripción

Trayectoria profesional

- Director de IT Risk Advisory y Cyber Risk, se incorporó al grupo en el año 2019, aportando una gran especialización en proyectos de transformación, estrategia y ciberseguridad, principalmente en el sector financiero y asegurador.
- Director responsable de la práctica de ciberseguridad en el sector asegurador.

Formación académica y titulaciones

- Ingeniero Superior en Informática
- Licenciado en Administración y Dirección de Empresas
- Máster Executive en IT Governance & Audit
- Programa Experto en Planificación Financiera y Control de Gestión
- Programa Experto en Dirección Estratégica Aseguradora
- Certificaciones:
  - CISA
  - ITIL Foundation v3
  - ISO 22301 Lead Auditor

Otros datos de interés profesional

- Experiencia en dirección de proyectos internacionales con equipos multidisciplinares basados en diferentes países
- Experiencia en reporte a Comité de Dirección y Consejo de Administración
- Experiencia en Oficinas de Proyectos y de Transformación a nivel estratégico
- Colaborador habitual de ICEA
- Idiomas: castellano e inglés

Principales proyectos

- Elaboración de Planes Directores de Sistemas a 3 años en entornos internacionales
- Elaboración de Planes de Transformación Digital para el sector asegurador
- Elaboración de Planes Directores de Seguridad en baca y seguros
- Definición e implementación de modelos organizativos de TI
- Dirección de departamentos de Gobierno de TI en seguros
- Auditorías Financiera, SOX y de Sistemas en entidades cotizadas en Banca y Seguros
- Implantación y revisión de Sistemas de Gestión de la Continuidad de Negocio
- Adaptación y auditorías del cumplimiento por parte de proveedores y clientes del reglamento de medidas asociado a la Ley Orgánica de Protección de Datos (LOPD) y al GDPR.
- Dirección de Oficinas de Transformación y Oficinas de proyectos, tanto del Plan Estratégico Corporativo como de Proyectos de Tecnología
- Dirección de proyectos de integración de funciones de IT tras operaciones corporativas (M&A), tanto en Banca como en Seguros
- Diseño e implementación de cuadros de mando para la Función de TI
- Diseño e implementación del Modelo de Gobierno y Estructuras de Comités dentro de la función de TI
- Diseño funcional de herramientas PPM para la gestión del portfolio y optimización de los recursos
- Definición e implementación de Oficinas de Proveedores de TI
- Definición e implantación de Oficinas de Gestión Financiera de TI

Principales clientes

Seguros:

- Pelayo
- CNP
- Caser Seguros
- Catalana Occidente
- CNP Assurances
- AXA
- Ocaso
- MAPFRE
- SegurCaixa Adeslas
- Mutua Madrileña
- VidaCaixa
- BBVA Seguros
- ICEA

Banca:

- BBVA
- Banco Popular
- Banesto
- BMN
- Bancaja

Daniel Hernández Arroyo

Director Cyber en Seguros
17 años de experiencia

dhernandezarroyo@deloitte.es
+34 911 57 74 79

Director del encargo

Equipo de proyecto propuesto

Currículums | Account Manager responsable del encargo

Descripción

Trayectoria profesional

- Gerente de IT Risk Advisory y Cyber Risk, se incorporó al grupo en el año 2010, especializándose proyectos de adaptación regulatoria y en ciberseguridad, principalmente en el sector financiero y asegurador.
- Encargado de coordinar actividades de formación interna del Grupo en Continuidad de Negocio y de coordinación de iniciativas de gestión y captación del talento.

Formación académica y titulaciones

- Licenciado en Matemáticas (especialidad de Matemática Aplicada)
- Máster en Ingeniería Matemática orientada a finanzas por la Universidad de Santiago de Compostela.
- Certificaciones:
  - CISM
  - ISO 27032 Lead Cybersecurity Manager
  - CISA
  - ISO 22301 Lead Implementer
  - ITIL Foundation v3

Otros datos de interés profesional

- Idiomas: castellano, gallego, alemán, inglés.

Principales proyectos

- Liderazgo de Oficinas Técnicas de coordinación, seguimiento y reporte de actividades en el ámbito de la gestión de Riesgos Tecnológicos y Gobierno de la seguridad IT.
- Diagnósticos y Planes Directores de Ciberseguridad.
- Auditorías de ciberseguridad.
- Implantación y revisión de Sistemas de Gestión de la Continuidad de Negocio y desarrollo de material formativo.
- Implantación, revisión y mejora continua de Planes de Recuperación ante Desastres o DRP's.
- Implementación y revisión de Sistemas de Gestión de Seguridad de la Información.
- Adaptación y auditorías del cumplimiento por parte de proveedores y clientes del reglamento de medidas asociado a la Ley Orgánica de Protección de Datos (LOPD) y al GDPR.
- Auditoría de Sistemas de Información y revisión de aplicaciones de soporte al negocio.
- Adaptación a MiFID II y PRIIPs en Entidades Financieras a nivel europeo.
- Revisión de los procesos de generación del Transaction Reporting a CNMV en Entidades Financieras españolas.
- Análisis funcional de estrategias adoptadas motivadas por la Reforma del Sistema de Postcontratación español (liquidación, compensación y custodia)
- Elaboración de procedimientos de control y planes de auditoría IT asociados a Cámaras de Compensación del mercado de valores.

Principales clientes

Productos y Servicios:

- Estrella Galicia
- Grupo Orona
- Inditex
- Ecoembes
- Siemens-Gamesa
- Tetra Pak
- MAXAM

Banca:

- Abanca
- Laboral Kutxa
- Kutxabank
- Cecabank
- BBVA
- Unicaja
- Bankinter

Seguros:

- MAPFRE
- Pelayo
- Caser

Juan Loureiro Brañas

Senior Manager
12 años de experiencia

jloureirobranas@deloitte.es
+34 911 57 85 47

Account Manager responsable del encargo

Equipo de proyecto propuesto

Currículums | Product Manager Cyber Strategy

Descripción

Trayectoria profesional

- Se incorporó a Deloitte en 2010 en el área de Enterprise Risk – IT-ERS del área de Madrid.
- Como consultor ha desempeñado proyectos en diferentes clientes y sectores de actividad, principalmente en el sector asegurador y financiero.
- En 2017 fue promocionado a gerente como Product Manager la línea de Cyber Risk Management & Compliance dentro del área de Estrategia de ciberseguridad.

Formación académica y titulaciones

- Ingeniero Superior de Telecomunicación por la Universidad Politécnica de Madrid
- Máster en Dirección y Gestión de Seguridad de la Información por la Universidad Politécnica de Madrid
- Certificaciones: CISM, CISA, CDPP, ISO22301 Provisional Lead Implementer, ISO27001 Lead Auditor, ITIL Foundation v3, COBIT 5 Foundation.

Otros datos de interés profesional

- Inglés con nivel de competencia profesional
- Instructor en diversos cursos internos y externos de Deloitte

Principales proyectos

- Proyectos de Gestión de Oficinas Técnicas de Seguridad en diferentes ámbitos:
  - Adaptación a la Normativa de Seguridad de la Información.
  - Seguridad en Nuevas Iniciativas.
  - Adecuación al Reglamento General de Protección de Datos.
- Proyectos de evaluación de riesgos de terceras partes.
- Proyectos de adecuación de entidades al Reglamento General de Protección de Datos (GDPR).
- Adecuación a la Normativa de Seguridad de la Información bajo el marco regulatorio nacional e internacional.
- Asesoramiento especializado en el cumplimiento de normativa de seguridad, mediante el diseño de procedimientos y controles específicos en procesos, revisión e identificación de requisitos no funcionales de seguridad y riesgos en aplicaciones, etc.
- Consultorías y auditorías LOPD, en base al actual Reglamento de Desarrollo.
- Consultoría de protección de datos abordando aspectos asociados a calidad de la información, derechos ARCO, declaración de ficheros, etc.
- Auditorías informáticas de seguridad y confiabilidad de entornos en entidades del sector financiero y asegurador, tanto como proyectos completos como apoyo a las auditorías financieras, las cuales incluyen pruebas masivas de datos como parte de los trabajos de las auditorías financieras, y revisiones de las configuraciones de seguridad de diferentes entornos.

Principales clientes

Seguros

- MAPFRE
- HDI
- MetLife

Banca:

- Santander
- BBVA
- BMN

Otros:

- Inversis
- Cepsa
- Konecta
- Renault
- Rexam
- Vithas

Félix de Andrés
Senior Manager
11 años de experiencia
fdeandres@deloitte.es
91.157.85.19

Product Manager
Cyber Risk Management & Compliance

Equipo de proyecto propuesto
Currículum

Por motivos de confidencialidad, no se muestra el nombre del candidato. En caso de resultar adjudicatarios, se asignará un consultor con un perfil similar al mostrado

Descripción

Trayectoria profesional

- Se incorporó a Deloitte en 2018, al área de Strategy & Risk Advisory - Cyber.
- A lo largo de su trayectoria profesional, ha trabajado en Accenture como Consultor de Seguridad.
- Cuenta con más de 4 años de experiencia en temas de ciberseguridad y en particular, en gestión de Oficinas Técnicas de Seguridad.

Formación académica y titulaciones

- Licenciado en Ingeniería Superior Industrial por la Universidad de Sevilla (US - ESI).
- CISA (Certified Information Systems Auditor).
- SSCP (Systems Security Certified Practitioner).

Otros datos de interés

- Idiomas:
  - Castellano
  - Inglés
  - Alemán

Principales proyectos

- Definición de Planes Directores de Seguridad de la Información. Elaboración de estrategias en materia de seguridad de la información que aportan valor añadido para el negocio.
- Gestión, seguimiento y control sobre todas las actividades de ciberseguridad así como la coordinación y gestión de tareas dentro de una Oficina Técnica de Seguridad, en entidades financieras y del sector del juego privado.
- Realización de auditorías internas sobre el cumplimiento de la Ley SOx, LOPD, requisitos de la EBA y normas ISO, PCI-DSS, etc.
- Evaluación de nivel de madurez de las cibercapacidades de un framework de ciberseguridad y elaboración de un Plan Director de Seguridad en entidades públicas.
- Definición del marco normativo en Seguridad de la Información en entidades financieras, teniendo en cuenta la clasificación y tratamiento de la información, la gestión de servicios Cloud, las relaciones con terceros, etc.
- Colaboración en distintos proyectos de Seguridad de la Información y Continuidad de Negocio.
- Análisis y gestión de riesgos basados en metodología Magerit, CobIT 5, etc.
- Soporte a las áreas de auditoría en la identificación de riesgos TIC así como la definición y ejecución de planes de acción.
- Definición y gestión de una PMO Global mediante metodologías ágiles.
- Definición de indicadores y realización de cuadros de mando.

Principales clientes

BBVA
Codere
Triodos Bank
Santander
Canal Isabel II

Consultor senior
4 años de experiencia

Índice

DC

Honorarios

Propuesta económica

De acuerdo con la planificación y equipo de trabajo, así como sobre la base de nuestra experiencia en proyectos similares, y considerando el enorme interés que tenemos en poder colaborar con CNP Assurances en este proyecto, hemos estimado los siguientes honorarios:

Tipo de servicio	Equipo propuesto	Precio mes	Precio con descuento para el periodo septiembre-diciembre 2022
CISOaaS	**0,3 FTE Cyber** • Perfil consultor de seguridad – Cyber Strategy (~30%)	2.700 €	**6.666 €**

En caso de ser necesarios desplazamientos fuera de Madrid Capital (máximo 20% del tiempo presencial), se facturarán los gastos a manutención y/o alojamiento.

La cifra de honorarios y gastos que se ha hecho constar en los puntos anteriores se incrementará con los tributos que resulten aplicables, usando el tipo impositivo vigente en cada momento.

Nuestros honorarios desglosados por medio de facturas mensuales distribuidas según el importe total indicado en cada opción.

Les informamos que nuestras facturas son pagaderas en el plazo máximo de treinta (30) días naturales a contar desde la fecha de su emisión.

Índice

Valor diferencial de Deloitte

Por qué Deloitte

01 **Líder**
Firma líder en Servicios de Seguridad en todas sus capacidades

02 **Experiencia**
Experiencia en proyectos relacionados con la función del CISO y PMO relacionadas con la gestión de la seguridad

03 **Cualificación**
La mayor red de profesionales cualificados, certificados y en continua formación en materia de seguridad

04 **Sector**
Conocimiento del sector, así como las necesidades que tiene una entidad para ser líder en el mismo.

05 **Flexibilidad**
Proactividad y flexibilidad en la gestión de servicios profesionales. Capacidad de adaptarse a la demanda requerida por el servicio

06 **Conocimiento**
Profundo conocimiento del funcionamiento de las entidades del sector, sus necesidades y su modelo de gestión

07 **Automatización**
Focalización en la sistematización de actividades y dotación al servicio de herramientas útiles y sencillas

08 **Procesos y metodología**
Experiencia en la definición, adaptación y mejora de procesos y metodologías

09 **Compromiso**
Responsabilidad asumida en dar a la entidad el mejor servicio posible y garantizar la no complacencia

Valor diferencial de Deloitte

Factores clave de éxito

VISIÓN GLOBAL

Adecuar los mecanismos de trabajo con un enfoque global destinado a ofrecer a CNP Assurances una visión independiente, así como aprovecharse del conocimiento adquirido por Deloitte en otros proyectos.

GESTIÓN DE LA DEMANDA

Monitorizar la capacidad del Servicio y la carga de trabajo, permitiendo reaccionar a tiempo frente a potenciales picos de carga que requieran activar los procedimientos acordados para absorber la demanda.

INTEGRACIÓN

Conocer la filosofía de CNP Assurances y hacerla propia para facilitar la consecución de los objetivos planteados para el servicio.

SEGUIMIENTO Y TRANSPARENCIA

Dotar a la entidad de herramientas que le permitan determinar la calidad del servicio recibido, así como elevar los indicadores a la Dirección.

MEJORA CONTINUA

Identificar aspectos que permitan mejorar el servicio permanentemente sin importar su estado, evitando complacencias en el mismo.

FLEXIBILIDAD

Disponer de capacidad de adaptación a la demanda por parte de un equipo multidisciplinar y coordinación entre los propios proyectos.

Valor diferencial de Deloitte

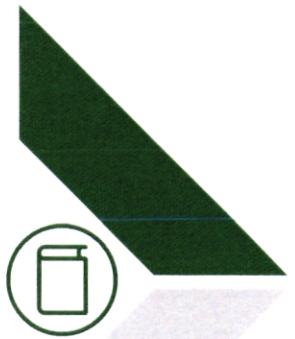
Aspectos clave

Además, Deloitte dispone de un conjunto de aspectos diferenciales en la ejecución de los servicios, los cuales se incluyen a continuación:

1

Flexibilidad

Deloitte facilita que en el Servicio, en caso de picos de trabajo, puedan distribuirse para tareas específicas en momentos concretos.



2

Innovación

Deloitte desarrollará los mecanismos para gestionar el Servicio conforme a los mejores estándares, realimentándose de los casos de éxito en la gestión realizados en otros servicios.

3

Conocimiento transversal

Deloitte dispone de expertos en todas las capacidades de ciberseguridad (gobierno, seguridad, vigilancia y resiliencia), que darán soporte al Servicio.

4

Mejora continua

El propio modelo de seguridad de Deloitte está en continua mejora, lo que facilitará al Servicio tener en cuenta todos los riesgos de ciberseguridad que aparezcan con motivo del desarrollo de nuevas tecnologías o modalidades de ataque.

Valor diferencial de Deloitte

Principios para asegurar un retorno del servicio ordenado, controlado y completo

CONOCIMIENTO

La información relevante debe ser documentada y compartida de manera permanente entre el equipo del servicio de Deloitte y CNP Assurances para asegurar una adecuada actualización del estado de situación de manera constante.

DOCUMENTACIÓN

Toda documentación generada por el servicio que se considere parte de un entregable o documentación de soporte para la gestión ha de estar accesible, organizada eficientemente y con capacidad de ser explotada.

Como parte de la documentación, es relevante proporcionar información de estado del servicio e indicadores de calidad.

COMUNICACIÓN

Se han de establecer mecanismos para garantizar que la información relevante es comunicada y conocida por todos los implicados.

La comunicación se considera un aspecto fundamental para garantizar la independencia del proveedor, facilitando a CNP Assurances el control final del servicio y la toma de decisiones relevantes.

HERRAMIENTAS

Tanto en el retorno como en la mejora en la eficiencia del servicio, éste debe proporcionar medios eficientes para facilitar la gestión y transferencia del conocimiento.

Desde Deloitte, se considera fundamental ayudar a CNP Assurances en la creación de herramientas que agilicen los tiempos de respuesta, calidad de reportes y transparencia.

DC

Valor diferencial de Deloitte

Equipo profesional altamente cualificado y amplia experiencia

Deloitte cuenta 14 socios en España en gestión de riesgo tecnológico y un equipo de **más de 700 especialistas en seguridad** y auditoría informática, la mitad de ellos dedicados específicamente a la Ciberseguridad, que atesoran **más de 500 certificaciones** en auditoría informática y seguridad de la información.

Los equipos de cibersegu s, siendo uno de ellos el vencedor global.

Valor diferencial de Deloitte

CyberSOC-CERT

Equipo de **alta calidad técnica** en constante **formación y con experiencia** en proyectos similares de seguridad. Cada servicio prestado desde el CyberSOC-CERT está estructurado en **tres niveles de especialización** y organizado en base a diferentes procedimientos de actuación, sometidos a procesos continuos de **madurez y optimización**, para ofrecer una máxima calidad.	**Equipo de trabajo**	**Medidas de seguridad**	Diversas medidas para **asegurar la prestación** de los servicios: • Protocolos de cifrado seguros. • Actividades de seguimiento de eventos en 24x7 del canal. • Creación de políticas de acceso. • Rotación de contraseñas. • Segregación de privilegios en la plataforma de conexión. • Registro de trazas para identificar a cada usuario. • Línea de backup.
El CyberSOC-CERT cuenta con **herramientas y plataformas de análisis a la vanguardia** del mercado y específicas para la prestación de los servicios. El CyberSOC-CERT Desk es la herramienta de gestión de tickets que soporta la operativa diaria en el CyberSOC-CERT para el **tratamiento de alertas e incidencias, monitorizada en 24x7**, y que posee una gran base de procedimientos para la gestión y soporte de incidentes de seguridad.	**Herramientas y plataformas especializadas**	**Procedimientos**	Se definirán por parte del equipo de trabajo de Deloitte, y una vez se hayan consensuado, todos los **procedimientos** (de escalado, de comunicación, de atención de casos, etc.) **para la correcta prestación del servicio**. Gracias a la experiencia en este tipo de proyectos, contamos con una **gran base de información y conocimiento** que nos permitirá asesorar en el ajuste y mejora de los procedimientos.
Asegurar la calidad del servicio que presta a todos sus clientes es una de las principales preocupaciones de Deloitte. La figura de **jefe de proyecto** se responsabilizará del buen funcionamiento y de la calidad del servicio, centralizando todas estas tareas: • Generación de **informes y métricas**. • **Gestión** del servicio, **supervisión y control** a distintos niveles. • **Control de cambios** en procedimiento y documentación del servicio. • **Reuniones** de supervisión y seguimiento, internas y con cliente. • Canalización de **solicitudes**.	**Gestión, supervisión y calidad**	**Factores diferenciales y capacidades añadidas**	El SOC de Deloitte ofrece una serie de factores y capacidades añadidas que incrementa las prestaciones de los servicios. Prueba de ello son: • **Soporte de la Red Global de Deloitte** para proporcionar alcance internacional a nuestros clientes así como acceso a una base de inteligencia (Casos de Uso). • **Acceso a múltiples fuentes de inteligencia** a través de acuerdos y alianzas nacionales e internacionales y pertenencia a **la red CERT**. • **Fuerte inversión en materia de seguridad** para la creación de laboratorios de análisis de amenazas y plataformas tecnológicas.

Valor diferencial de Deloitte

Líderes en ciberseguridad

Liderazgo de Deloitte en Cibersegruidad consolidado y reconocido por los analistas independientes en el mercado de global de la consultoría de riesgos tecnológicos, seguridad de la información y ciberseguridad tales como Forrester, Gartner, Kennedy e Hypatia.

Deloitte ha certificado su proceso de gestión de la seguridad y de continuidad de negocio según la **normas ISO-27001 e ISO-22301**. El alcance del sistema de gestión incluye todos los activos de información que son gestionados en el contexto de la prestación de los nuestros servicios profesionales a nuestros clientes y el CyberSOC-CERT, respectivamente.

El **centro de operaciones de seguridad de Deloitte** (CyberSOC-CERT) ha recibido la certificación **CERT** (Computer Emergency Response Team), concedida por la Universidad Carnegie-Mellon.

Deloitte es la única Big Four en el mundo que cuenta con el sello CERT.

Más de 700 profesionales en España dedicados a la gestión de riesgos tecnológicos, y más de 300 focalizados en ciberseguridad.

Más de 500 certificaciones en esta materia, desde certificaciones orientadas a la gestión hasta certificaciones técnicas de producto.

Deloitte vencedor de las Global Cyberlympics 2011, 2012, 2013, 2015 y 2016.

El **CyberSOC-CERT de Deloitte**, situado en España, ofrece a nuestros clientes capacidades únicas para la prevención, detección y respuesta frente a ciberataques.

Para ello, el CyberSOC-CERT de Deloitte dispone de capacidades de operación 24x7 soportadas entre otras, con tecnologías propietarias de Deloitte.

El **CyberLabs de Deloitte** es un centro con una infraestructura y un equipo de arquitectos de seguridad dedicado en exclusiva a la evaluación independiente de nuevas soluciones de seguridad, al diseño de *blueprints* de arquitecturas de seguridad y a la evaluación y análisis de nuevas amenazas de seguridad asociadas al uso de nuevas tecnologías emergentes.

Valor diferencial de Deloitte

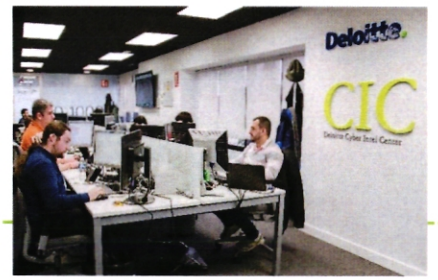
Liderazgo de Deloitte España en la estrategia global de Deloitte

- **Deloitte España** se posiciona como líder en Cyber con un **Centro Global de Operaciones de Ciberseguridad** (CyberSOC-CERT) para la región de **EMEA,** ubicado en Madrid, además, de **dos Centros de Ciber Inteligencia (CIC),** ubicados en Madrid y Barcelona.
- De este modo, Deloitte ofrece una de las ofertas más completas e innovadoras a través de una amplia cartera de servicios de ciberseguridad de alto valor añadido, que presta a **más** 200 clientes alrededor del mundo a través de uno de los equipos más especializados del mercado conformado por **más de 250 profesionales.**

Cyber Intelligence Center (CIC) Madrid

Cyber Intelligence Center (CIC) Barcelona

CyberSOC-CERT: EMEA Delivery Center (EDC) Alcobendas (Madrid)



Valor diferencial de Deloitte

Nuestra Red de Inteligencia Global y CyberSOCs

Los **Centro de Excelencia en Ciberinteligencia CIC** (Cyber Intel Centre) de Deloitte se trata de centros avanzados y especializados en servicios de inteligencia y protección frente a ciberamenazas dirigidas contra organizaciones. La red de ciberinteligencia global de Deloitte está compuesta por diversos centros y nodos en diferentes países, ofreciendo una cobertura global e integral a sus clientes:

Deloitte cuenta con 53 laboratorios de seguridad (**Deloitte Data Forensics & eDiscovery Laboratories**) por todo el mundo, para recolectar, analizar, detectar y responder ante ciberataques.

Centro de Deloitte para la Ciberinnovación: más de 100 soluciones han sido testeadas en escenarios reales de ataque para mejorar sus capacidades de protección.

Valor diferencial de Deloitte

Nuestras capacidades en Ciberseguridad

Las capacidades de nuestro Centro europeo de Operaciones de Ciberseguridad fueron evaluadas en 2016 por Gartner, destacando su liderazgo como "**Centro de Detección y Respuesta gestionada de incidentes de Ciberseguridad**"

EMEA Delivery Center (EDC) ofrece una amplia gama de servicios de operaciones de alto valor añadido, actuando desde Madrid como proveedor de la red Deloitte para el mercado de Europa, Oriente Medio y África.

CERT

El EDC es un Centro de Respuesta a Incidentes de Ciberseguridad (CERT) certificado y parte de la Carnagie Mellon University CERT Network

ISO-22301

Certificado en ISO22301, el estándar para la gestión de la continuidad de negocio

ISO-27001

Certificado en ISO27001, el estándar para la gestión de la seguridad de la información

Equipo certificado

Finalmente, destacar que AENOR ha certificado conforme a las exigencias de la norma española UNE-EN **ISO 9001 el Sistema de Calidad exclusivamente para su uso en Sector Público de Deloitte Advisory, S.L.**

260 profesionales de Cyber en España y +1.200 distribuidos en 20 firmas de EMEA

Valor diferencial de Deloitte

Nuestros servicios de Ciberseguridad

Deloitte ofrece la oferta de servicios más completa del mercado a través de sus soluciones de Advisory, Seguridad Gestionada (SOC) y CyberAcademy. La complementariedad de estos servicios ofrece a todos nuestros clientes un amplio catálogo de soluciones de "extremo a extremo" y de alta diferenciación frente a nuestros competidores.

Seguridad "Extremo a Extremo"

Nuestros servicios de Ciberseguridad abarcan desde la capa estratégica hasta la operación de sistemas de seguridad 24x7x365, persiguiendo la protección integral de los activos críticos de la organización: personas, información, procesos e infraestructuras.

Estrategia

- **Cyber Risk Management and Compliance**
- **Cyber Training, Education and Awareness**
- **Cyber Strategy, Transformation and Assessments**

Protección

- **Infrastructure Protection**
- Vulnerability Management
- Application Protection
- Identity and Access Management
- Information Privacy and Protection

Vigilancia

- Advanced Threat Readiness and Preparation
- Cyber Risk Analytics
- Security Operations Centre
- Threat Intelligence and Analysis

Resiliencia

- Cyber Incident Response
- Cyber Wargaming

Modelos de entrega

Asesoramiento | Implementación | Operación | Formación

Índice

Responsabilidad, Indemnidad y Protección de Datos

Responsabilidad

La responsabilidad máxima de Deloitte, de sus socios y de su personal por daños, perjuicios o reclamaciones que se pudieran derivar de los servicios contemplados en esta propuesta estará limitada conjuntamente a una cantidad equivalente a los honorarios satisfechos por los concretos servicios prestados que den lugar a la reclamación, y en ningún caso podrán ser objeto de reclamación los daños o perjuicios indirectos, lucro cesante, daño emergente, o costes de oportunidad. Este límite no será de aplicación en el supuesto que Deloitte, sus socios o su personal haya incurrido, en la ejecución de los trabajos objeto de la presente propuesta, en dolo o negligencia grave declarada por sentencia firme o un incumplimiento de la cláusula de confidencialidad, de la normativa sobre protección de datos o propiedad intelectual e imputable a Deloitte.

Cualquier reclamación derivada o relacionada con los servicios contemplados en el marco de esta propuesta deberá presentarse en el plazo máximo de prescripción de las acciones.

Indemnidad

Salvo en los supuestos en que Deloitte haya incurrido en dolo o negligencia grave declarada por sentencia firme o resolución de una autoridad competente, el cliente mantendrá indemne en todo momento a Deloitte, sus socios y su personal frente a cualquier reclamación de terceros distintos de la propia sociedad, en relación o que traigan causa en un incumplimiento por parte del cliente de las condiciones establecidas en la presente propuesta, así como en un uso indebido de los resultados, debiendo indemnizar en su caso a Deloitte, sus socios y/o su personal por los daños y perjuicios, gastos y costes (incluyendo honorarios de asesoramiento, abogados y procuradores) en que pudiera incurrir por causa de dichas reclamaciones o por las actuaciones en las que deba intervenir.

Datos de contacto en relación a las obligaciones del Reglamento de Protección de Datos Personales

Datos de contacto		Datos de contacto en relación a las obligaciones con la RGPD	
Nombre	Araceli Benito	**Notificación de violaciones de seguridad**	dpd.es@cnppartners.eu
Dirección		**Notificación de las peticiones de ejercicio de derechos**	gdpr.es.peticion@cnppartners.eu
Teléfono	+34 91 524 31 61		
Correo electrónico	Araceli.benito@cnppartners.eu		

Deloitte informa a las personas de contacto del Cliente de que sus datos de carácter personal serán almacenados y tratados por aquella con la finalidad de gestionar la presente relación contractual, y que podrán ejercitar, en caso de estimarlo oportuno y conforme a los procedimientos legalmente previstos, sus derechos de acceso, rectificación, supresión, limitación del tratamiento, oposición o portabilidad dirigiéndose a la dirección que figura en el encabezamiento de esta carta propuesta o bien mediante el envío de un email a la dirección de correo electrónico lopd@deloitte.es.

DC

Índice

Condiciones Generales de Contratación

Deloitte Advisory, S.L. (en adelante Deloitte) prestará los servicios definidos en la Propuesta firmada por CNP Assurances SA, sucursal en España ("el Cliente") y Deloitte (la "Propuesta" y los "Servicios") de acuerdo con las siguientes Condiciones Generales de Contratación las cuales, junto con la Propuesta, constituyen el contrato completo entre ambos respecto a los Servicios (el "Contrato"), sustituyen cualquier comunicación oral o escrita intercambiada por el Cliente y Deloitte con anterioridad a la Propuesta, y pueden ser modificadas (incluyendo cambios al alcance o naturaleza de los Servicios) únicamente mediante acuerdo escrito de ambas partes de conformidad con lo que se establece en este Contrato y siguiendo el procedimiento de realización de cambios que, en su caso, se determine en la Propuesta. En caso de contradicción o conflicto entre estas Condiciones Generales y los términos de la Propuesta, prevalecerá la Propuesta.

Artículo 1 - Honorarios y Gastos.

El Cliente pagará a Deloitte Advisory, S.L. los honorarios y gastos aprobados previamente por escrito por el cliente correspondientes, de acuerdo con lo estipulado en la Propuesta.

Artículo 2 - Obligaciones de Deloitte Advisory, S.L.

Las obligaciones de Deloitte se determinan en la Propuesta y en estas Condiciones Generales.

Artículo 3 - Obligaciones del Cliente.

El Cliente es consciente de que un proyecto de consultoría como el que se aborda en este Contrato requiere, como elemento esencial del proyecto, el compromiso y la participación activos del propio Cliente, los cuales condicionan directamente las prestaciones y el cálculo de los honorarios del consultor. En este sentido, y sin perjuicio de que en la Propuesta y en estas Condiciones Generales se determinen con mayor detalle, amplitud o precisión las responsabilidades del Cliente en el marco de este Proyecto, el Cliente se compromete a llevar a cabo al menos las siguientes actividades esenciales:

a) ejecutar en los plazos establecidos y de forma adecuada sus responsabilidades, tal y como se determine en su caso en la Propuesta, y garantizar que las hipótesis de partida o factores de éxito identificados son correctos y adecuados;

b) proporcionar a Deloitte información fiable, correcta, actualizada y completa, según sea necesario para la realización de los Servicios;

c) adoptar decisiones dentro de los plazos establecidos y obtener toda aprobación necesaria de la Dirección o de los Órganos Sociales que resulten competentes para la contratación de estos servicios; en este sentido, las partes acuerdan que corresponderá a la Dirección o los Órganos Sociales del Cliente tomar toda decisión ejecutiva o estratégica relativa a este proyecto.

(d) poner a disposición del personal de Deloitte, en su caso, un entorno de trabajo apropiado, así como recursos y material adecuados.

(e) Adicionalmente, Deloitte podrá confiar en toda decisión o aprobación efectuada por el Cliente independientemente de este Contrato y/o con anterioridad a la firma del mismo. Nada en este Contrato requerirá que Deloitte evalúe, aconseje sobre, modifique, confirme o rechace tales decisiones o aprobaciones, salvo que las partes establezcan lo contrario en el Contrato. El Cliente será responsable de cualquier retraso, coste adicional, u otras consecuencias negativas derivadas de o relacionadas con cualquier deficiencia en el cumplimiento por parte del Cliente de sus Obligaciones.

Artículo 4 - Confidencialidad.

Con relación a la información proporcionada en el marco de este Contrato y designada como confidencial por la parte que la proporcione, la parte que la reciba se compromete a: (i) proteger dicha información confidencial de forma razonable y adecuada y de acuerdo con los estándares profesionales aplicables, en su caso; (ii) utilizar la información confidencial únicamente con el fin de ejecutar sus obligaciones en el marco del Contrato; (iii) reproducir información confidencial únicamente en la medida necesaria para ejecutar sus obligaciones en el marco del Contrato. Este Artículo no se aplicará a información que: (i) sea del dominio público; (ii) sea ya conocida por la parte que la recibe; (iii) se haya proporcionado a un tercero sin restricciones; (iv) haya sido desarrollada independientemente; o (v) haya sido revelada por causa de requisitos legales. Sin perjuicio de lo anterior, Deloitte podrá comunicar información confidencial del Cliente a sus subcontratistas y a entidades miembro de la organización.

Artículo 5 - Resultados y Restricciones de Uso.

El Cliente podrá, únicamente para fines internos propios, usar, copiar, distribuir y modificar los resultados que se describen en la Propuesta (los "Resultados"). Dado que los Resultados se desarrollan únicamente para uso interno del Cliente, en el contexto preciso de este proyecto, el Cliente no comunicará los Resultados a terceros (las compañías del Grupo CNP no tendrán la consideración a efectos de esta cláusula como terceros), ni los citará públicamente, ni hará referencia a los mismos, sin el consentimiento previo escrito de Deloitte. Queda prohibido cualquier uso de los Resultados, diferente al que se indica en la Propuesta, sin la autorización previa y por escrito de Deloitte. Deloitte conserva todo derecho, título e interés en: (i) los Resultados, incluyendo a título ilustrativo, toda patente, derecho de autor, marca u otros derechos de propiedad intelectual relativos a los Resultados; y (ii) toda metodología, procedimiento, técnica, idea, concepto, secretos comerciales y knowhow incorporados o relativos a los Resultados o que Deloitte pueda desarrollar o aportar en relación con este Contrato (los "Conocimientos de Deloitte"). Sin perjuicio de las obligaciones de Confidencialidad que se establecen en la Cláusula 4, Deloitte podrá utilizar sin restricciones los Resultados y los Conocimientos de Deloitte.

Artículo 6 - Aceptación.

El Cliente aceptará los Resultados (i) que sean conformes a los requisitos o especificaciones que establezca la Propuesta; o (ii) que hayan superado el plan de pruebas de aceptación acordado específicamente para este proyecto, en su caso. Durante el proceso de aceptación, el Cliente notificará inmediatamente a Deloitte cualquier no-conformidad de los Resultados con tales requisitos o especificaciones ("No-Conformidad") y Deloitte dispondrá de un plazo de tiempo razonable, en función de la gravedad y de la complejidad de la No-conformidad, para rectificarla. Si el Cliente ha utilizado los Resultados antes de la aceptación, si no ha notificado a Deloitte inmediatamente la No-conformidad, o si retrasa de forma no razonable el inicio del plan de pruebas acordado, se considerará que el resultado en cuestión ha sido aceptado por el Cliente.

Artículo 7 - Manifestaciones y Compromisos.

(a) Deloitte prestará los Servicios con la diligencia debida y, una vez realizada la aceptación en los términos del Artículo 6, se compromete a corregir cualquier No-conformidad, siempre y cuando el Cliente notifique dicha No-conformidad a Deloitte por escrito en un plazo de treinta (30) días a partir de la aceptación tal y como se define en el mencionado Artículo 6. Transcurrido dicho plazo sin haber obtenido ninguna comunicación escrita por parte del Cliente, se considerará que el servicio ha sido prestado de acuerdo a las condiciones pactadas en la Propuesta.

(b) Deloitte no garantiza ni será responsable de productos o servicios de terceros. Toda reclamación del Cliente en este sentido, será frente a los terceros proveedores.

(c) Independientemente del alcance de los Servicios o Resultados, el Cliente manifiesta que es de su responsabilidad diseñar y mantener un sistema de control interno, y en particular de aquellos controles internos contables, que garantice suficientemente que: (i) las operaciones se realizan con autorización general o específica de la Dirección; (ii) las operaciones se registran de modo que permitan (a) preparar estados financieros y cuentas anuales de acuerdo con principios contables generalmente aceptados o con cualquier otro criterio que resultara aplicable a dichos estados financieros, y (b) mantener registros contables de los activos; (iii) el acceso a los activos se permite únicamente con autorización general o específica de la Dirección; y (iv) los registros contables de los activos se contrastan con los activos reales con una frecuencia adecuada y se emprenden acciones apropiadas en relación con cualquier diferencia que pudiera existir. El Cliente determinará la adecuación de sus controles contables internos y de sus sistemas de información financiera, sin basarse en los Servicios o Resultados como elemento principal de tal determinación, asumiendo, por tanto, la responsabilidad del sistema global de control interno. Finalmente, el Cliente manifiesta que es de su responsabilidad realizar las comunicaciones relativas a este proyecto que requiera la normativa aplicable.

DL

(d) El Cliente y Deloitte se comprometen a cumplir con las leyes y normativas aplicables, incluidas las relacionadas con la anticorrupción, manifestando asimismo su compromiso de actuar en todo momento de forma ética y profesional, y comprometiéndose a no realizar ninguna práctica que de alguna manera resulte o pueda resultar en una vulneración de leyes o normativas aplicables relacionadas con la corrupción en cualquier país cuya legislación sea aplicable al presente Contrato.

Artículo 8 - Personal.

(a) Deloitte será responsable de designar y asignar su propio personal, en el modo más adecuado según su criterio, para la realización de los Servicios, sin perjuicio de lo cual Deloitte tratará de responder a los requisitos o sugerencias del Cliente respecto a individuos determinados.

(b) Durante la vigencia de este Contrato, y durante un periodo de doce (12) meses a partir de la finalización o resolución del mismo, ninguna de las partes tratará de contratar, directa o indirectamente, personal de la otra que haya participado directamente en la prestación de los Servicios.

c) La naturaleza de este contrato es la propia de un arrendamiento de servicios de carácter exclusivamente mercantil. Por lo expuesto, no se deriva relación o vínculo laboral alguno entre las partes, ni entre el Cliente y el personal de Deloitte que, eventualmente, pudiera estar prestando alguno de los Servicios que constituye el objeto del presente contrato. Deloitte está obligado a cumplir con todas las obligaciones establecidas para con la Seguridad Social y Hacienda en relación a dicho personal y, específicamente, las relativas a la Seguridad Social e Higiene y Accidentes de trabajo. En este sentido, con la firma del presente contrato, Deloitte: i) certifica expresamente que cumple en todo momento con la totalidad de sus obligaciones en materia fiscal, laboral (en concreto pago de salarios) y de cotización respecto de sus empleados por cuenta ajena; ii) se obliga a aportar certificado de descubiertos emitido por la Seguridad Social así como un certificado de cumplimiento de sus obligaciones tributarias a la firma del presente Contrato.

Artículo 9 - Resolución.

(a) El presente Contrato podrá ser resuelto: (i) por cualquiera de las partes en caso de incumplimiento por la otra de los términos de este Contrato, siempre que tal incumplimiento no haya sido subsanado por la otra en un plazo de quince (15) días desde la fecha de recepción de la notificación de incumplimiento; y (ii) por Deloitte, en caso de incompatibilidad legal sobrevenida, con quince (15) días de preaviso.

(b) Salvo en caso de resolución por incumplimiento de Deloitte, el Cliente pagará a Deloitte todos los honorarios y gastos correspondientes a Servicios prestados hasta la fecha de la resolución.

(c) Deloitte deberá devolver el importe abonado en concepto de provisión de fondos si los honorarios exceden de los que debería haber cobrado Deloitte hasta la finalización del contrato.

c) Salvo en materias relativas a obligaciones de confidencialidad o derechos de propiedad intelectual, las partes se comprometen a tratar de resolver cualquier diferencia, disputa o posible incumplimiento, internamente, elevándolo a niveles de dirección competentes de sus respectivas organizaciones y, en general, a utilizar procedimientos alternativos de resolución de disputas que resulten mutuamente aceptables, antes de recurrir a procedimientos contenciosos.

Artículo 10 - Tratamiento de datos personales

Si como consecuencia de la prestación de los Servicios contratados, Deloitte tuviera acceso a datos de carácter personal que se encuentran bajo la responsabilidad del Cliente, Deloitte tendrá la condición de Encargado del tratamiento.

La naturaleza y finalidad de los tratamientos que Deloitte realizará por cuenta del Cliente será la derivada de la prestación del servicio objeto del Contrato, y en concreto consistirá en: recogida, procesamiento, conservación, consulta, cotejo, supresión, registro y destrucción.

Para la ejecución de los Servicios contenidos en el presente Acuerdo, el Cliente pone a disposición de Deloitte la siguiente información/datos personales:

*Marcar aquellas categorías de información o datos personales que se faciliten:

- [x] Nombre
- [ ] Número de empleado/ID personal
- [ ] Dirección privada
- [x] Información de contacto privada
- [x] Información de contacto de empresa
- [ ] Datos biométricos
- [ ] Estudios
- [ ] Datos de afiliación a entidades
- [ ] Fotografía o videos donde aparezca el individuo
- [ ] Salario/Tipo de contrato
- [ ] Evaluaciones
- [ ] Registro de llamadas
- [ ] Hojas de gastos
- [ ] Fecha de nacimiento
- [ ] DNI/Pasaporte
- [ ] Estado civil
- [ ] Datos de salud
- [ ] Etnia/Raza
- [ ] Sexo
- [ ] Creencias religiosas
- [ ] Orientación política
- [ ] Orientación sexual
- [ ] Códigos de cuentas financieras
- [ ] Carnet de conducir
- [ ] Contraseñas
- [ ] Certificado de penales
- [ ] Otros:

Habida cuenta del carácter reservado de los datos que obran en poder del Cliente, en caso de que éstos pudieran ser conocidos por Deloitte en virtud del presente Acuerdo, éste último se compromete a que permanezcan en secreto.

Esta obligación de Deloitte de guardar secreto permanecerá en vigor incluso después de cesar en su relación con el Cliente.

A estos efectos, Deloitte se compromete a tomar, respecto de sus empleados, todas las medidas necesarias para que resulten informados de la necesidad del cumplimiento de las obligaciones que le incumben como encargado del tratamiento de datos de carácter personal y que, en consecuencia, deben respetar.

Deloitte se compromete a tratar los datos personales a los que tenga acceso únicamente para el cumplimiento de los términos de este Acuerdo. Este compromiso se extenderá asimismo con respecto a las Transferencias Internacionales de Datos de carácter personal a un tercer país o una Organización internacional.

En consecuencia, los datos que se conozcan u obtengan en virtud de este Acuerdo, no podrán ser utilizados para ninguna otra finalidad distinta de la ejecución del mismo, tendrán carácter confidencial y no serán divulgados o puestos en conocimiento de terceros sin la previa autorización por escrito del Cliente salvo en los casos expresamente autorizados por la Ley.

En el caso de que Deloitte recurra a subcontratistas (subencargado) para llevar a cabo determinadas actividades de tratamiento de datos personales por cuenta del Cliente, Deloitte deberá obtener autorización previa del Cliente. A tal efecto, Deloitte informará por escrito al Cliente con carácter previo de las subcontrataciones previstas, facilitando los datos de los terceros a los que pretenda subcontratar. Si el Cliente no manifestara por escrito su oposición a dicha subcontratación en el plazo de quince días desde la recepción de la notificación correspondiente, se entenderá que no se opone a la misma. Los mismos términos y obligaciones resultarán aplicables en el supuesto de que Deloitte tuviera intención de sustituir a alguno o algunos de sus subencargados.

Adicionalmente, el Cliente acepta que Deloitte, actuando en nombre y por cuenta del Cliente, subcontrate los servicios de soporte informático con PM&S Recursos, S.L.U., así como otros servicios con cualquiera de las sociedades que formen parte de la Organización Deloitte en España (subencargados), todas ellas con domicilio social en Pza. de Pablo Ruiz Picasso nº 1, Torre Picasso, 28020-Madrid.

Deloitte impondrá por escrito al subencargado las mismas obligaciones de protección de datos recogidas en la presente cláusula. Dichas obligaciones serán igualmente extensibles para Deloitte en el supuesto de que el subencargado utilice otros terceros y en el caso de existir una cadena de subcontratistas, de tal modo que Deloitte y cualquiera de los sucesivos subcontratistas hasta llegar al último de la cadena queden sujetos a las mismas obligaciones.

Deloitte será plenamente responsable ante el Cliente y responderá del efectivo cumplimiento de las obligaciones en materia de protección de datos de los posibles subcontratistas que interviniesen en el tratamiento de los datos personales.

Deloitte se compromete a aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, habida cuenta del estado de la técnica, los costes de aplicación, la naturaleza de los datos almacenados, el alcance, contexto y fines del tratamiento, así como los riesgos a que estén expuestos y el impacto que esto pudiera tener sobre los derechos y libertades de las personas físicas.

En todo caso, Deloitte deberá implantar mecanismos para:

* Seudonimizar y cifrar los datos personales, en su caso.

* Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

* Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

* Verificar, evaluar y valorar regularmente la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

Asimismo, Deloitte estará obligado a cumplir con sus deberes respecto a la realización de cualesquiera evaluaciones de impacto en materia de protección de datos que estuviera obligado a llevar a cabo.

Deloitte deberá poner a disposición del Cliente la documentación justificativa correspondiente y permitir la realización de auditorías e inspecciones con el fin de comprobar los extremos indicados con anterioridad. Dichas auditorías serían realizadas por el Cliente, o por un tercero designado de mutuo acuerdo, siendo el coste de las mismas soportado por el Cliente.

Deloitte notificará al Cliente sin dilación indebida y el plazo máximo de 24 horas desde que fue conocida por Deloitte y a través del canal que facilite el Cliente a estos efectos, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia, salvo en aquellos supuestos en los que sea improbable que dicha violación de seguridad constituya un riesgo para los derechos y libertades de los interesados.

Si dispone de ella se facilitará, como mínimo, la información siguiente:

* Descripción de la naturaleza de la violación de la seguridad de los datos personales y, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

* El nombre y los datos del delegado de protección de datos.

* Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

* Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si en un primer momento Deloitte no pudiera informar de todas las cuestiones indicadas con anterioridad, las comunicará tan pronto tenga conocimiento de las mismas.

Deloitte asistirá al Cliente a través de medidas técnicas y organizativas apropiadas y siempre que sea posible, en relación con las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados.

En el caso de que las personas afectadas ejerzan los derechos mencionados en el apartado anterior ante Deloitte, ésta debe comunicarlo por correo electrónico al Cliente a la dirección que el cliente facilite a estos efectos. La comunicación deberá hacerse sin dilación indebida desde la recepción de la solicitud y en el plazo máximo de 5 días naturales desde que fue recibida por Deloitte, juntamente, en su caso, con cualquier otra información que pueda ser relevante para resolver la solicitud.

Asimismo, cualquier tipo de transferencia internacional deberá ser autorizada por el cliente y además deberá contar con las garantías precisas (binding corporate rules, modelo de clàusula aprobado por la UE) en caso contrario no podrá realizarse.

Una vez terminado por cualquier causa el Acuerdo y a elección del Cliente, Deloitte se compromete a devolver y/o destruir todos los datos personales a los que hubiera tenido o tenga acceso para la realización del objeto del Acuerdo, al igual que cualquier copia de los mismos en cualquier soporte, salvo en la medida en que sea necesaria su conservación en virtud del derecho comunitario o de los Estados miembros que resulte de aplicación, o para la formulación, ejercicio o defensa de reclamaciones relacionadas con el objeto del presente contrato.

Artículo 11 - Disposiciones Generales.

(a) Ninguna de las partes utilizará el nombre, marcas, logotipos, nombres comerciales y/o elementos publicitarios de la otra sin el consentimiento previo por escrito de aquélla. Sin perjuicio de lo anterior, Deloitte podrá citar en otras propuestas o contratos el nombre del Cliente y/ o realizar una descripción general de los Servicios/ del Proyecto, con fines de promoción. El Cliente acuerda igualmente que, mediando un preaviso razonable por parte de Deloitte, accederá a proporcionar a terceros referencias favorables a Deloitte (por ejemplo, en forma de llamadas telefónicas de clientes o analistas o presentaciones).

(b) No obstante lo indicado en el apartado (a), Deloitte podrá compartir con otras entidades de su organización el nombre del Cliente y/o realizar una descripción general de los servicios prestados, siendo dicha información para uso exclusivo de la organización Deloitte.

(c) Ninguna de las partes será responsable por retrasos o incumplimientos debidos a circunstancias que escapen a su control razonable.

(d) Este Contrato no podrá ser cedido en modo alguno, en todo o en parte, sin el acuerdo escrito previo de la otra parte, incluso cuando se trate de entidades de su organización internacional y además, deberá contar con las garantías adecuadas y cumplir con la cláusula y normativa sobre protección de datos incluida en la presente propuesta.

(e) Toda comunicación que se realice en el marco de este Contrato será escrita, se enviará a las direcciones indicadas en la Propuesta, y se considerará efectuada en el momento de su recepción por la parte destinataria.

(f) Toda renuncia a términos de este Contrato y toda excusa a un incumplimiento del mismo, deberán constar por escrito, firmado por la parte que consienta a dicha renuncia o excusa.

(g) En caso de que cualquier término o estipulación de este Contrato sea declarado ilegal, nulo o anulable, se considerará eliminado dicho término o estipulación, sobreviviendo el resto del Contrato.

(h) Este Contrato no convierte a ninguna de las partes en agente o representante legal de la otra, y no crea ningún tipo de asociación o empresa en común. Las partes actúan como contratistas independientes y asumen plenamente y en nombre propio sus respectivas obligaciones, derivadas de este Contrato.

(i) Los Artículos 4 a 13 de este Contrato sobrevivirán a la expiración o resolución del mismo por cualquier causa.

(j) El presente Contrato se somete a Ley española.

(k) El Cliente reconoce que: (i) Deloitte y el Cliente podrán comunicarse o enviarse documentación mediante correo electrónico/ Internet, salvo que el Cliente determine expresamente lo contrario; (ii) ninguna de las partes controla el funcionamiento, fiabilidad, disponibilidad o seguridad del correo electrónico/ Internet; y que (iii) Deloitte no será responsable de ninguna pérdida, daños, gastos, perjuicios o molestias que resulten de la pérdida, retraso, interceptación, corrupción, o alteración de cualquier correo electrónico o comunicación por Internet.

(l) Deloitte no asume responsabilidad por las prestaciones, fiabilidad, disponibilidad o seguridad de Internet, de sistemas o de hardware del Cliente o de terceros, que no estén comprendidos en el alcance de los Servicios de Deloitte en este proyecto.

Salvo que las partes acuerden por escrito lo contrario, el Cliente asume la responsabilidad de:

* determinar la existencia de, y cumplir con, los elementos siguientes, aplicables a transacciones, comercio, procesos electrónicos, o a actividades realizadas a través de Internet o de cualquier red electrónica ("Transacciones"): controles import/ export; requisitos para obtener y mantener licencias y otros permisos; requisitos para evaluar, pagar o retener impuestos, tasa de aduana u otras cargas o tributos; y cualesquiera otras leyes o reglamentos en cualquier jurisdicción competente;

* la seguridad de su red y de cualquier sistema relacionado con la misma, incluida la seguridad, privacidad y confidencialidad de cualquier dato, propiedad intelectual u otra información del Cliente o de terceros;

* establecer y determinar la validez y ejecutabilidad de los procesos de firma y realización de contratos, así como de cualquier otra documentación necesaria para o utilizada en el marco de las Transacciones;

* cualquier contenido aportado por el Cliente o por terceros en relación con este proyecto; y

* cualquier utilización de los Resultados por el Cliente, incluyendo, a título de ejemplo: inclusión por el Cliente en su website o transmisión a través de Internet, de texto, imágenes, software, música, videos u otra información; venta u oferta por el Cliente de bienes o servicios mediante su website o por Internet; y cualquier distribución de correo electrónico no solicitado en relación con el website del Cliente, que puedan resultar ilegales, molestos, que infrinjan derechos de propiedad intelectual de terceros, o que de cualquier otro modo constituyan abusos de la red ("Usos No Aceptables"), y el Cliente se compromete a indemnizar a Deloitte por toda responsabilidad, costes y gastos en que Deloitte pueda incurrir como consecuencia de Usos No Aceptables por el Cliente.

DC

(m) El Cliente reconoce que el Cliente y/o sus filiales y sucursales: (i) controlan cualquier dato y base de datos del Cliente, filiales, o de terceros, (los "Datos"), a los cuales tenga acceso Deloitte o que Deloitte deba procesar durante la prestación de los Servicios, y (ii) son los únicos responsables de los Datos frente a los terceros titulares de los mismos incluyendo, a título de ejemplo, empleados y clientes del Cliente. El Cliente garantiza a Deloitte que toda recogida, almacenamiento, proceso y transmisión de los Datos entre el Cliente y sus filiales, entre el Cliente y Deloitte y entre el Cliente y cualquier tercero, se ha realizado hasta la fecha de este Contrato y se realizará en lo sucesivo, en total conformidad con cualquier norma aplicable a la protección de datos. En el marco de este Contrato, Deloitte accederá a y procesará los Datos únicamente por cuenta del Cliente, bajo responsabilidad exclusiva del mismo, siempre de acuerdo con las instrucciones y procesos que el Cliente deberá establecer y comunicar a Deloitte, siendo igualmente responsabilidad del Cliente determinar la existencia y aplicabilidad de normas de protección de datos en cada momento.

(n) Deloitte no estará obligada a iniciar trabajo nuevo o diferente de los Servicios acordados en la Propuesta ("Cambio") en tanto no se haya acordado por escrito el impacto del Cambio sobre el precio y/o el calendario, en su caso. Cuando se produzca una solicitud de Cambio, bien sea a iniciativa del Cliente o de Deloitte, Deloitte presentará una propuesta al Cliente describiendo los Cambios y el impacto de éstos sobre el precio y/o el calendario, en su caso, pudiendo utilizar el documento de solicitud de cambios incluidos en la propuesta (si se hubiese incorporado a la misma). El Cliente comunicará por escrito a Deloitte su conformidad con la propuesta de Cambio, o bien indicará a Deloitte también por escrito que no deberá emprender los Cambios, en cuyo caso Deloitte continuará los Servicios inicialmente pactados.

Sin perjuicio de lo anterior, si a petición del Cliente o con el conocimiento del Cliente, Deloitte realizase trabajo no previsto en la Propuesta o que supere el alcance previsto en la Propuesta, se considerará dicho trabajo como Servicios realizados en el marco de este Contrato, que el Cliente vendrá obligado a pagar a las tarifas indicadas en la Propuesta o a las tarifas que se utilizaron para calcular los honorarios fijados en la Propuesta.

Artículo 12 - Propiedad intelectual y confidencialidad de la propuesta.

Queda prohibida la reproducción, comunicación pública, transformación, total o parcial, gratuita u onerosa, por cualquier medio o procedimiento, sin la autorización previa y por escrito de Deloitte. Esta propuesta es estrictamente confidencial. Si decidiesen no realizar este proyecto con Deloitte, seleccionar otra consultora o utilizar sus recursos internos para llevarlo a cabo, a nuestro requerimiento deberán devolvernos todas las copias de este documento.

Artículo 13 – Independencia de las Firmas

Deloitte se refiere a Deloitte Touche Tohmatsu Limited, (prívate company limited by guarantee, de acuerdo con la legislación del Reino Unido) y a su red de firmas miembro, cada una de las cuales es una entidad independiente. En www.deloitte.com/about se ofrece una descripción detallada de la estructura legal de Deloitte Touche Tohmatsu Limited y sus firmas miembro.

Condiciones generales de contratación

Aceptación de la contratación

Este documento refleja enteramente el acuerdo entre CNP Assurances SA, sucursal en España y Deloitte Advisory, S.L. referente a los servicios indicados en el mismo y sustituye a cualquier propuesta previa, correspondencia o acuerdo verbal o escrito que pudiera existir.

En caso de conformidad con los términos aquí expuestos, les agradeceríamos que nos devolvieran debidamente firmadas las copias que les adjuntamos de la propuesta y de las Condiciones generales de contratación.

Estamos encantados de tener la oportunidad de prestarles nuestros servicios profesionales y les aseguramos que dedicaremos a este trabajo nuestra mayor atención.

Atentamente,

Deloitte Advisory, S.L.

Fdo.: Rubén Frieiro

En expresión de su consentimiento,

CNP Assurances SA, sucursal en España

Fdo.:

Deloitte.

ANEXO

A PROPUESTA DE COLABORACIÓN

(Oficina de seguridad para la externalización del CISO)

(Principios Éticos Grupo CNP)

ENTRE

CNP ASSURANCES, S.A. SUCURSAL EN ESPAÑA

Y

DELOITTE ADVISORY, S.L.

CNP assurances

ANEXO A PROPUESTA DE COLABORACIÓN

(Oficina de seguridad para la externalización del CISO)

Por medio del presente Anexo se incluye a la propuesta de colaboración (Oficina de seguridad para la externalización del CISO) de mayo de 2022 realizada por Deloitte Advisory, S.L. y debidamente aceptada por CNP ASSURANCES, S.A., Sucursal en España, carta con los principios éticos del Grupo CNP Assurances y cláusula financiera adicional.

Insuring a more open world

ÉTICA DE NEGOCIOS,
EL GRUPO CNP ASSURANCES SIGUE FIEL A SUS COMPROMISOS.

La ética es un elemento crucial de los principios corporativos del grupo CNP Assurances.

En un entorno cambiante, nuestro compromiso con valores fundamentales es una posición insoslayable.

La adhesión de CNP Assurances al Pacto Mundial de la ONU en el año 2003 es la prueba más fehaciente de este compromiso.

Fraude, corrupción, tráfico de influencias, conflicto de intereses, blanqueo de capitales son lacras contra las que el grupo CNP Assurances lucha y reafirma una tolerancia cero.
La implementación de medidas enérgicas guían nuestras acciones en nuestras relaciones comerciales, ya sea con nuestros clientes, proveedores o socios comerciales.

También seguiremos atentos al cumplimiento de prácticas comerciales justas.

Esperamos de cada colaborador del Grupo y de nuestros socios un comportamiento ejemplar y responsable.

La satisfacción de los clientes y de nuestros socios es nuestra máxima prioridad y, aunque valoramos el reconocimiento de la calidad del servicio prestado, no queremos recibir regalos, obsequios ni ningún otro beneficio.

De este modo, mantenemos una total imparcialidad en nuestra toma de decisiones y respetamos los principios de integridad y ética del grupo CNP Assurances.

You will find these principles in C@pEthic, our Group code of conduct, on our corporate site at www.cnp.fr and in our policies, available on request.

Stéphane DEDEYAN
Director General

Evelyn TORTOSA
Director Conformidad Grupo

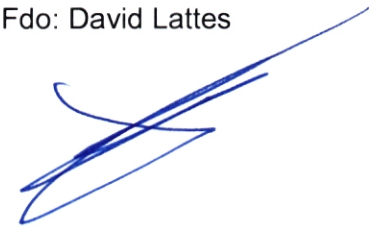
La Entidad Aseguradora no realizará pago de cantidad alguna que le puedan exponer o impliquen cualquier sanción, prohibición o aplicación de medidas restrictivas, en virtud de resoluciones de cualquier organismo internacional, y en especial, aquéllas promulgadas por las Naciones Unidas, la Unión Europea, los Estados Unidos de América, los Gobiernos Francés o Español, así como cualquier autoridad que pertenezca a los anteriores.

La Entidad Aseguradora tendrá derecho a rescindir los acuerdos o contratos suscritos en el caso de que su contraparte adquiera la categoría de persona sancionada o se le aplique una medida restrictiva, en virtud de resoluciones de cualquier organismo internacional, y en especial, aquéllas promulgadas por las Naciones Unidas, la Unión Europea, los Estados Unidos de América, los Gobiernos Francés o Español, así como cualquier autoridad que pertenezca a los anteriores.

Y en prueba de conformidad ambas partes en el carácter con el que interviene, firman el presente anexo en Madrid a 30 de mayo de 2022

Por duplicado a un solo efecto.

Deloitte Advisory, S.L.	CNP ASSURANCES, S.A., Sucursal en España
Fdo.: Rubén Frieiro	Fdo: David Lattes



ANEXO

A PROPUESTA DE COLABORACIÓN

(Oficina de seguridad para la externalización del CISO)

(Principios Éticos Grupo CNP)

ENTRE

CNP ASSURANCES, S.A. SUCURSAL EN ESPAÑA

Y

DELOITTE ADVISORY, S.L.

CNP assurances

ANEXO A PROPUESTA DE COLABORACIÓN

(Oficina de seguridad para la externalización del CISO)

Por medio del presente Anexo se incluye a la propuesta de colaboración (Oficina de seguridad para la externalización del CISO) de mayo de 2022 realizada por Deloitte Advisory, S.L. y debidamente aceptada por CNP ASSURANCES, S.A., Sucursal en España, carta con los principios éticos del Grupo CNP Assurances y cláusula financiera adicional.

Insuring a more open world

ÉTICA DE NEGOCIOS,
EL GRUPO CNP ASSURANCES SIGUE FIEL A SUS COMPROMISOS.

La ética es un elemento crucial de los principios corporativos del grupo CNP Assurances.

En un entorno cambiante, nuestro compromiso con valores fundamentales es una posición insoslayable.

La adhesión de CNP Assurances al Pacto Mundial de la ONU en el año 2003 es la prueba más fehaciente de este compromiso.

Fraude, corrupción, tráfico de influencias, conflicto de intereses, blanqueo de capitales son lacras contra las que el grupo CNP Assurances lucha y reafirma una tolerancia cero.
La implementación de medidas enérgicas guían nuestras acciones en nuestras relaciones comerciales, ya sea con nuestros clientes, proveedores o socios comerciales.

También seguiremos atentos al cumplimiento de prácticas comerciales justas.

Esperamos de cada colaborador del Grupo y de nuestros socios un comportamiento ejemplar y responsable.

La satisfacción de los clientes y de nuestros socios es nuestra máxima prioridad y, aunque valoramos el reconocimiento de la calidad del servicio prestado, no queremos recibir regalos, obsequios ni ningún otro beneficio.

De este modo, mantenemos una total imparcialidad en nuestra toma de decisiones y respetamos los principios de integridad y ética del grupo CNP Assurances.

You will find these principles in C@pEthic, our Group code of conduct, on our corporate site at www.cnp.fr and in our policies, available on request.

Stéphane DEDEYAN
Director General

Evelyn TORTOSA
Director Conformidad Grupo

La Entidad Aseguradora no realizará pago de cantidad alguna que le puedan exponer o impliquen cualquier sanción, prohibición o aplicación de medidas restrictivas, en virtud de resoluciones de cualquier organismo internacional, y en especial, aquéllas promulgadas por las Naciones Unidas, la Unión Europea, los Estados Unidos de América, los Gobiernos Francés o Español, así como cualquier autoridad que pertenezca a los anteriores.

La Entidad Aseguradora tendrá derecho a rescindir los acuerdos o contratos suscritos en el caso de que su contraparte adquiera la categoría de persona sancionada o se le aplique una medida restrictiva, en virtud de resoluciones de cualquier organismo internacional, y en especial, aquéllas promulgadas por las Naciones Unidas, la Unión Europea, los Estados Unidos de América, los Gobiernos Francés o Español, así como cualquier autoridad que pertenezca a los anteriores.

Y en prueba de conformidad ambas partes en el carácter con el que interviene, firman el presente anexo en Madrid a 30 de mayo de 2022

Por duplicado a un solo efecto.

Deloitte Advisory, S.L.	CNP ASSURANCES, S.A., Sucursal en España
Fdo.: Rubén Frieiro	Fdo: David Lattes