PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA CONTRATACION DE SERVICIOS DE CENTRO DE OPERACIONES DE SEGURIDAD PARA EL CONSORCIO DE AGUAS BILBAO BIZKAIA FINANCIADO CON FONDOS PROCEDENTES DEL MECANISMO PARA LA RECUPERACIÓN Y RESILENCIA – NEXT GENERATION EU EN EL MARCO DEL COMPONENTE 5 “PRESERVACIÓN DEL LITORAL Y RECURSOS HÍDRICOS” INVERSIÓN 1 (C5.I1) DENOMINADA «MATERIALIZACIÓN DE ACTUACIONES DE DEPURACIÓN, SANEAMIENTO, EFICIENCIA, AHORRO, REUTILIZACIÓN Y SEGURIDAD DE INFRAESTRUCTURAS (DSEAR)»

ÍNDICE

1 ANTECEDENTES

El Consorcio de Aguas Bilbao Bizkaia (en adelante CABB), junto con diferentes empresas especializadas, planifica, desarrolla y mantiene los servicios asociados al centro de operaciones de seguridad.

Dado el aumento y la complejidad de las amenazas y ataques, así como, el aumento en los incidentes a nivel nacional e internacional en materia de seguridad de la información y ciberseguridad, se hace necesario la contratación de servicios externos y especializados en estos, que aseguren una prevención de los riesgos y una respuesta adecuada ante un incidente.

2 OBJETO

El presente documento tiene por objetivo especificar las tareas y características que han de cumplir el servicio de SOC, de cara a su contratación en modalidad de servicio.

3 NORMATIVA ESPECÍFICA

A continuación, se recoge una relación no exhaustiva de normas y regulaciones que tienen relación con el objeto de la contratación:

- Real Decreto 43/2021.
- Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad.
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- “Guía Nacional de notificación y gestión de ciberincidentes”, publicada por el Ministerio del Interior.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos

personales y a la libre circulación de estos (Reglamento general de protección de datos).

- Ley Orgánica 3/2018 de Protección de Datos y Garantía de Derechos Digitales (LOPDGDD).
- Norma UNE-EN ISO/IEC 27001:2017 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. (y subsiguientes de la serie ISO/IEC 27000 relativas a los sistemas de gestión de seguridad de la información.
- Information Technology Infrastructure Library (ITIL)

4 DESCRIPCIÓN DE LOS SERVICIOS

El alcance de los trabajos a realizar por el adjudicatario en el ámbito del presente contrato será la prestación de servicios de seguridad de la información y ciberseguridad, como soporte al área de Seguridad Lógica del CABB. Para ello se contará con un Centro de Operaciones de la Seguridad (en adelante SOC).

A continuación, se describen en detalle los servicios que deberá prestar el adjudicatario. En el Anejo IV se recogen los estándares mínimos que el proveedor deberá cumplir (Acuerdos de Nivel de Servicio).

4.1 Centro de Operaciones de la Seguridad (SOC)

El SOC prestará un servicio permanente (24x7) de monitorización, supervisión, detección y gestión de incidentes de seguridad, esto es, su actividad se focalizará en la seguridad preventiva y reactiva.

Actuará en todo momento de acuerdo con los procedimientos establecidos en el CABB. El registro, control y seguimiento de la actividad se llevará a cabo utilizando la herramienta de gestión de incidencias ya disponible en CABB, así como las herramientas de notificación de ciberincidentes que se establezca por parte de las autoridades nacionales (LUCIA, del CCN-CERT u otras llegado el caso).

El Centro de Operaciones de Ciberseguridad que se despliegue en el ámbito del presente pliego formará parte de la Red Nacional de Centros de Operaciones de Ciberseguridad. La coordinación de los centros integrados en esta red nacional se llevará a cabo a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes, prevista en el artículo 11 del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

El SOC prestará como mínimo los servicios que se recogen a continuación, no constituyendo esta relación un listado exhaustivo. El ofertante podrá ampliar dicha relación tanto en contenido como en alcance.

4.1.1 Ciberinteligencia

El adjudicatario proveerá de un servicio de inteligencia digital para la recolección de datos e información a partir de diferentes fuentes, realizando su investigación y el análisis de los resultados con el fin de detectar precozmente posibles amenazas online que puedan afectar al CABB, como mínimo las siguientes:

- Fugas de información; presencia de datos personales (del personal propio o datos de terceros custodiados por el CABB), robo de Credenciales, robo o filtración de documentos confidenciales, presencia en Bases de Datos, información de sistemas comprometidos, etc.
- Protección de activos.
- Amenazas Avanzadas Persistentes (APTs).
- Movimientos sociales y hacktivistas.
- Protección VIP.
- Protección de marca, presencia y reputación online.

Las Fuentes que debe examinar deben ser, al menos:

- Webs convencionales, con independencia del idioma y la localización geográfica.

- Motores de búsqueda: Google, Bing, Altavista, Yahoo, entre otros.
- Foros.
- Bases de Datos públicas (BOE, OEPM, BOPI, etc.) y Bases de Datos Privadas (einforma, registradores, etc.).
- Información interna publicada en Internet: Casos de éxito de fabricantes, presentaciones públicas, metadatos publicados en los recursos del CABB, servidores de news, foros, etc.
- Redes Sociales (Facebook, Linkedin, Twitter, etc.).
- Bases de datos de Threat Intelligence.
- Listas negras de spam.
- Servidores DNS.
- Apropiación de dominios (Cybersquatting).
- Markets de aplicaciones móviles.
- Redes P2P (Emule, Bit Torrent, etc.).
- Red TOR y redes alternativas (I2P, Freenet, etc.).

- Canales y foros underground.
- Servicios de acortamiento de URL (Tiny URLs), listas de malware y de spam, registradores de dominios, etc.
- Online pastes (Pastebin y similares), IRCs, Botnets, Carding Markets, etc.
- Metadatos en los documentos recolectados en los ámbitos de búsqueda anteriores.

Este servicio proporcionará:

- Con carácter permanente, alertas tempranas para todos los incidentes y/o vulnerabilidades, incluso de día cero, que puedan poner en peligro la seguridad de CABB.
- De forma periódica:
  - Informe mensual elaborado por el analista de inteligencia, con el detalle de todas las alertas significativas generadas en el periodo.
  - Informe cuatrimestral de alto nivel detallando los hallazgos más relevantes en el periodo, aportando una visión de contexto global en el sector (en referencia a otras organizaciones similares en actividad, tamaño, localización geográfica… u otras características significativas).
- A demanda, informe de detalle sobre algún incidente concreto si así fuera requerido.

4.1.2 Monitorización de la seguridad

El adjudicatario supervisará permanentemente el estado de la infraestructura tecnológica de CABB, generando las alertas correspondientes en caso de eventos que puedan afectar a la seguridad de la compañía. Las principales tareas a realizar son:

- Monitorización y supervisión proactiva de los eventos de seguridad a través de un correlador de eventos de seguridad (SIEM). Esta herramienta deberá ser proporcionada por el adjudicatario como parte del servicio.
- Monitorización y supervisión proactiva de los eventos directamente sobre las propias herramientas de seguridad de CABB que se pongan a disposición del servicio y que no estén integradas en el SIEM.
- Procesamiento y correlación de los eventos recolectados en tiempo real para detección anticipada de sucesos relevantes que puedan ser indicativos de un ataque, así como análisis y verificación para desestimar falsos positivos.
- Elaboración de indicadores de cumplimiento y desempeño.

4.1.2.1 Plataforma de correlación de eventos de seguridad de la información.

El adjudicatario deberá proporcionar una plataforma para la recolección y análisis en tiempo real de las alertas de seguridad generadas por los componentes hardware o software que conforman los diferentes sistemas de información y telecomunicaciones de CABB. La citada plataforma se ofrecerá en la modalidad de SaaS (Software como Servicio), evitando la adquisición de hardware

o licencias por parte de CABB. El servicio incluirá la provisión de todo el hardware y el software necesarios para la prestación del servicio alojado en su propia infraestructura, las actualizaciones periódicas del mismo, la administración y la operación de la infraestructura en la modalidad 24x7 de acuerdo a lo especificado en este pliego. El personal de seguridad de CABB tendrá acceso a la plataforma a nivel totalmente funcional (creación de secuencias de búsqueda y correlación de eventos, elaboración de cuadros de mando, configuración y generación de alertas, etc.).

Dicha plataforma será aprovisionada, instalada, configurada, optimizada, operada y gestionada por el SOC. Recogerá y centralizará los registros y logs que contengan información y eventos de seguridad, normalizará, categorizará, agregará, correlacionará y almacenará dichos eventos por un período de retención inicial de 365 días, detectando incidentes de seguridad y generando alertas. Dispondrá de una herramienta de toma proactiva de decisiones y proporcionará una única consola web accesible, que permita a CABB realizar consultas y generar informes y cuadros de mando a partir de las políticas y métricas de riesgo definidas.

La explotación de este servicio deberá permitir mantener un equilibrio entre la detección de alertas de seguridad y el esfuerzo preciso para solucionarlas y documentarlas.

En general, deberá:

- Proporcionar un análisis de los eventos en tiempo casi real.
- Correlacionar y analizar información compleja procedente de diferentes fuentes y sistemas (entornos heterogéneos como activos de red, dispositivos de seguridad, sistemas operativos, aplicaciones, bases de datos y productos de gestión de accesos e identidades.).
- Permitir la creación de una línea base de actividades y detección de anomalías para identificar cambios en el comportamiento asociados a aplicaciones, hosts, usuarios, etc.
- Generar alertas basadas en anomalías observadas y en cambios en el comportamiento de los flujos de red y en los eventos de seguridad, así como poder añadir anomalías definidas por CABB.
- Proporcionar alertas en base a políticas establecidas (por ejemplo, tráfico de mensajería instantánea no permitido, almacenamiento en la nube no permitido, uso de protocolos no autorizados, etc.). y aplicaciones potencialmente peligrosas (file sharing, P2P, etc.).
- Configurar y transmitir alertas a través de diferentes mecanismos hacia otras soluciones de ticketing y herramientas de terceros.
- Establecer sinergias con herramientas de seguridad de terceros (feeds de inteligencia, plataformas de Cyber Threat Intelligence, etc.).
- Correlacionar resultados proporcionados por herramientas de escaneos de vulnerabilidades integradas o de terceros.
- Monitorizar y alertar cuando se produzca una interrupción en la recopilación de registros de una fuente o dispositivo supervisado.

- Descubrir y clasificar automáticamente los activos de la red mediante diferentes técnicas de escaneo (ping, fingerprinting de puertos y de sistemas operativos, etc.) y de consultar a repositorios de activos externos (como Directorio Activo, LDAP, CMDB, etc.).
- Soportar y mantener un histórico de la actividad de la autenticación de usuarios en función de cada activo, que permita la generación de informes de auditoría y trazabilidad.
- Permitir la correlación de valores añadidos en el tiempo (por ejemplo, enviar una alerta cuando una IP origen envía más de un volumen de datos configurado a un solo servicio publicado en una IP destino desde una ventana de tiempo configurada).
- Proveer información relacionada con los perfiles de tráfico en términos de número de bytes, frecuencia de paquetes, número de activos en comunicación por aplicación, puertos protocolos, amenazas u otros posibles puntos de monitorización en la red.
- Contar con módulos o herramientas avanzadas (Machine Learning, Big Data Analytics, IA, u otras) que permitan detectar eventos relacionado con amenazas de tipo “0-day”, amenazas desconocidas, APT, movimientos laterales, compromiso del endpoint, exfiltración de información, actividad sospechosa en general, etc.
- Auto-aprender dinámicamente de los patrones de comportamiento analizados (tanto eventos, como actividad de red) y alertar sobre actividad anómala que pudiera significar un incidente de seguridad.
- Ser capaz de detectar ataques de tipo DoS (Denial of Service) y DDoS (Distribute Denial of Service).
- Ser capaz de detectar y mostrar el tráfico relacionado con una amenaza específica observada en la red.
- Soportar la creación de perfiles de tráfico asociados con el diseño lógico de la red, tanto a nivel de dirección IP individual como de rango de redes (por ejemplo, subred/CIDR).
- Ser capaz de perfilar comunicaciones procedentes de, o dirigidas hacia internet por regiones geográficas y en tiempo real.
- Permitir la creación de perfiles claramente independientes y diferenciados del tráfico local y del tráfico con origen y destino a internet.
- Soportar la creación de perfiles de tráfico basados en direcciones IP, grupos de direcciones IP, parejas de direcciones IP origen/destino, etc.
- Permitir el acceso a los detalles de los eventos de seguridad y de los flujos de red almacenados, al menos durante 12 meses.

La solución SIEM incluirá todos los elementos y módulos necesarios para la prestación con garantía del servicio.

El SOC será responsable del análisis y asesoramiento continuo para la mejora de la madurez de la plataforma que presta el servicio de Monitorización de la Seguridad, proponiendo para ello un ciclo de mejora continua para la incorporación de nuevas fuentes, desarrollo de casos de uso, reglas de correlación y detección, objetos estándar y "ad hoc", filtros, informes estándar y "custom", alertas, listas, elementos de la base de datos de conocimiento con incidencias y las actuaciones realizadas para su resolución, etc. con el objeto de aprovechar al máximo la plataforma que presta dicho servicio.

Los logs, una vez configurados, estarán disponibles para realizar consultas y análisis forense para investigar incidentes de forma ágil, buscar indicadores de amenazas persistentes avanzadas (APT) y facilitar la superación de las debilidades detectadas por las auditorías de cumplimiento. Se combinará el acceso a datos históricos con la posibilidad de ver los detalles de cada evento específico.

La plataforma permitirá incluir las fuentes de información que CABB decida emplear para llevar a cabo la monitorización, de modo que sea sencilla y transparente la inclusión de nuevas fuentes como consecuencia de los cambios que se puedan producir en la infraestructura con el paso del tiempo. La incorporación de fuentes de información podrá realizarse en cualquier momento durante la prestación del servicio, habida cuenta que la infraestructura de CABB evoluciona y se desarrolla constantemente. El personal técnico del adjudicatario se encargará de incorporar las nuevas fuentes de información que CABB solicite, para lo que trabajará de forma coordinada con el personal técnico de CABB. La plataforma deberá ser compatible con amplia gama de dispositivos y productos de diferentes tipologías y fabricantes, así como soportar un volumen de al menos 1500 EPSs (40 GB/día).

4.1.3 Gestión de incidentes de seguridad

Una vez se detecte un incidente a través del servicio de monitorización, o bien este le sea comunicado por alguno de los canales establecidos, el SOC procederá a la gestión completa del incidente realizando, al menos, las siguientes actividades:

- Registrar, clasificar, valorar, priorizar y escalar los incidentes de seguridad que sean detectados a través del servicio de monitorización, que sean comunicados por el personal de Seguridad o TIC de CABB, o que sean notificados por parte los organismos nacionales, regionales o locales de respuesta a incidentes de ciberseguridad (CERTSIS).
- Emitir las alertas oportunas ante eventos de seguridad, tanto internas como a terceros (autoridades nacionales y/u otras organizaciones).
- Realizar la notificación y documentación de los incidentes de seguridad según la "Guía nacional de notificación y gestión de ciberincidentes" y los protocolos establecidos en CABB.
- Adoptar medidas de contención para los incidentes de seguridad, o dar indicaciones precisas para que estas sean implementadas por el personal del

área TIC de CABB, según los protocolos establecidos, así como verificar su eficacia.

- Investigar los incidentes de seguridad, localizando y recolectando evidencias sobre la infraestructura tecnológica de CABB cuyo acceso se haya autorizado, o bien solicitando la recolección de evidencias a la Oficina Técnica de Seguridad de la Información (en adelante OTSI) y al equipo TIC de CABB, y procediendo a su análisis posterior.
- Realizar el análisis de código malicioso.
- Investigación forense.
- Elaborar el informe de cierre del incidente, así como el informe post-incidente, con inclusión de lecciones aprendidas y propuestas de planes de acción para prevenir la reproducción futura de incidentes similares o para mejorar los mecanismos de respuesta y gestión de incidentes.
- Elaboración de informes periódicos sobre el servicio y actualización de las métricas e indicadores definidos.

El adjudicatario deberá disponer de las herramientas y capacidades necesarias para prestar los servicios de análisis de malware, investigación forense y recogida de evidencias digitales, como son:

- Sandboxes y herramientas de correlación de resultados para el análisis automatizado de muestras de código malicioso.
- Entorno para ingeniería inversa de código malicioso para realizar el análisis estático y dinámico, y para la generación de Indicadores de Compromiso (IOC - Indicator of Compromise) como firmas de detección de red o indicadores para ser usados en host
- Herramientas de análisis de forense de discos (recuperación de archivos borrados, indexador de datos)
- Material para la realización de intervenciones in-situ para la adquisición de evidencias (Kit de material para adquisiciones forense, clonadores de disco, dispositivos "writeblockers" para manipulación segura de evidencias, cámaras fotográficas con localización GPS para registro documental del proceso de adquisición forense, etc.).

El ciclo de vida del incidente se gestionará de acuerdo a los procedimientos establecidos en CABB. El adjudicatario propondrá los mecanismos y protocolos para dotar de plena garantía al proceso de peritaje, recolección, almacenamiento y cadena de custodia de las evidencias obtenidas para, llegado el caso, permitir su presentación, aceptación y validez plena en el ámbito legal y jurídico.

Adicionalmente el adjudicatario deberá mantener actualizados y probados los procedimientos de respuesta ante incidentes mediante las siguientes tareas:

- Revisión periódica de los procedimientos, manuales y herramientas definidos para la gestión de incidentes de seguridad.
- La preparación y ejecución de un ciberejercicio anual en la Organización.
- El soporte durante la participación de ciberejercicios, públicos o privados, en los que CABB decida participar

Para la atención al servicio de Gestión de Incidentes de Seguridad, el adjudicatario deberá contar al menos con:

- Punto Único de Contacto 24x7 (Service Desk); para la atención a incidencias, consultas, peticiones y gestión de notificaciones. El adjudicatario proporcionará un canal de comunicación seguro (cifrado, redundante).
- Equipo de Primera Intervención; para detección, identificación y valoración de incidentes, así como la emisión documentada de propuestas de solución y/o medidas de contención y/o medidas compensatorias que se identifiquen como necesarias.
- Gestor del servicio; encargado de la supervisión y seguimiento del servicio, presentación de informes y resultados.

4.1.4 Servicio de Auditorías de Seguridad y Análisis de Vulnerabilidades

El objetivo de este servicio es identificar vulnerabilidades o fallos de seguridad en las redes y sistemas de información de CABB frente a ataques externos e internos, cubriendo tanto los Sistemas de la información (IT) como los sistemas industriales (OT).

Las auditorías de seguridad y análisis de vulnerabilidades se realizarán utilizando como referencia metodologías de trabajo reconocidas internacionalmente como pueden ser OSSTMM, OWAS, WASC, etc. La valoración objetiva de las vulnerabilidades detectadas y verificadas se realizará empleando la metodología CVSS (Common Vulnerability Scoring System).

En los apartados siguientes se describe el alcance mínimo de los servicios requeridos.

4.1.4.1 Auditoría de seguridad Perimetral

Este servicio contempla la realización de una auditoría perimetral con carácter mensual, con el siguiente alcance mínimo:

- Recopilación de información pública desde diferentes fuentes (actividad realizada por el servicio de Ciberinteligencia, según se detalla en el apartado correspondiente).

- Enumeración de todos los activos y recursos de la organización expuestos hacia internet y que pueden ser objeto de un ciberataque (rangos IP, equipamiento, servicios activos, puertos abiertos, DNS, servidores de correo, etc.).
- Detección e identificación de vulnerabilidades, errores de configuración y fallos de seguridad en dichos activos, mediante el empleo de herramientas automatizadas y comprobación manual para descartar falsos positivos.
- Elaboración de un informe técnico donde se detallarán todas las vulnerabilidades encontradas con detalle de su identificación, descripción de la vulnerabilidad, activos afectados, nivel de riesgo, valoración CVSS si existe, evidencias, referencias documentales, planes de mitigación y recomendaciones.

- Elaboración de un informe ejecutivo.

El servicio estará previsto para 40 (sub)dominios diferentes.

4.1.4.2 Auditoría interna

4.1.4.2.1 Análisis de Vulnerabilidades

Durante la prestación del servicio el adjudicatario dotará de una herramienta para la identificación automática de vulnerabilidades en la red interna de CABB. Esta herramienta podrá ser alguna de las disponibles en el mercado (Nessus, Qualys, etc.) u Open Source (OpenVAS, etc.). Tanto la herramienta como el equipo sobre el que esta se ejecute serán aportados por el adjudicatario. La herramienta podrá quedar ubicada en las instalaciones de CABB durante la vigencia del contrato, para lo que el adjudicatario realizará los trabajos de instalación necesarios en coordinación con los técnicos de CABB, o bien estar alojada en las propias instalaciones del adjudicatario, realizando en este caso la tarea mediante conexión a través de una línea dedicada suministrada por CABB. En todo caso, los técnicos del área de Seguridad Lógica de CABB tendrán acceso a la consola de administración de la herramienta, con posibilidad de hacer uso de la misma, si fuera preciso.

Las pruebas se realizarán siempre de forma coordinada con el personal técnico de CABB y bajo estricto control para evitar situaciones que pudieran derivar en degradación de servicio.

El mantenimiento y actualización de la herramienta será realizado en su totalidad por el personal técnico del adjudicatario.

Como resultado de cada análisis de vulnerabilidades, el adjudicatario elaborará:

- Un informe técnico donde se detallarán todas las vulnerabilidades encontradas con detalle de su identificación, descripción de la vulnerabilidad, activos afectados, nivel

de riesgo, valoración CVSS si existe, evidencias, referencias documentales, planes de mitigación y recomendaciones.

- Un informe ejecutivo con el resumen, a alto nivel, de los principales hallazgos.

Se deberá llevar a cabo un análisis de vulnerabilidades completo (entorno corporativo e industrial), al menos, de forma trimestral. A este objeto, el adjudicatario elaborará una programación que deberá ser aprobada por el responsable del proyecto por parte de CABB.

4.1.4.2.1 Test de Seguridad (Hacking Ético).

Con carácter anual durante la prestación del servicio, el adjudicatario llevará a cabo un Test interno de Seguridad (Hacking Ético). Al principio del servicio se realizará el primer test de seguridad, del que se obtendrá una panorámica general de la situación en la organización que servirá como referencia para valorar la eficacia de las actuaciones de seguridad que se vayan realizando durante la prestación del contrato. Los Test de Seguridad incluirán en su alcance tanto los equipos, sistemas y redes del ámbito de las Tecnologías de la Información y las Comunicaciones (Sistemas y redes de telecomunicaciones corporativas) como los de las Tecnologías de la Operación (Redes y sistemas SCADA y de control de procesos industriales), para lo que el adjudicatario deberá disponer de personal debidamente cualificado en ambos campos.

Las pruebas de Hacking Ético consistirán en:

- Tests de tipo “caja negra”; el equipo auditor no dispondrá de información sobre los objetivos si bien podrá hacer uso de la aquella obtenida mediante el análisis de vulnerabilidades al entenderse que esta información podría estar en manos de un potencial atacante. Se realizarán análisis automatizados, complementados con el empleo de escáneres específicos y revisiones manuales al objeto de profundizar en los hallazgos y descartar falsos positivos.

- Tests de tipo “caja blanca”; partiendo de la información proporcionada por CABB, el equipo auditor analizará la arquitectura de las redes y sistemas de información de la compañía para detectar posibles debilidades o fallos de seguridad.

- Pruebas de Ingeniería social; se realizarán de diferente tipología, contemplándose como mínimo las siguientes:

  - Envío de correos electrónicos simulando ataques malintencionados (Phishing); con diferentes niveles de verosimilitud (con y sin suplantación de dominio del remitente, en castellano o en otro idioma, etc.).

- Realización de llamadas telefónicas para tratar de obtener información sensible de CABB (Vishing); dirigidas tanto a personal en plantilla como a personal de empresas proveedoras o terceros colaboradores de CABB.
- Intentos de acceso físico a oficinas de CABB mediante utilización de técnicas de engaño.

Estas pruebas serán previamente consensuadas con el responsable del proyecto por parte de CABB dado que afectan directamente personas físicas tales como empleados, proveedores, etc.

Se identificarán también aquellas debilidades que, aún sin tratarse de una vulnerabilidad en los sistemas, suponen un incumplimiento en la normativa de seguridad de CABB.

Como resultado de los test de Hacking Ético, el adjudicatario elaborará:

- Un informe técnico con el detalle de todos los fallos de seguridad encontrados con detalle de su identificación, descripción, activos afectados, nivel de riesgo, evidencias, referencias documentales, planes de mitigación y recomendaciones.

- Un informe ejecutivo con el resumen, a alto nivel, de los principales hallazgos.

4.1.4.3 Auditoría de código

El adjudicatario incluirá en su alcance la prestación de un servicio de auditorías de código sobre las aplicaciones que CABB solicite. Las aplicaciones a auditar se determinarán en las reuniones específicas que se realizarán al efecto entre CABB y el adjudicatario. Este servicio contemplará, como mínimo, la realización anual durante la duración del contrato de:

- Una auditoría de un servicio web completo
- Una auditoría de una aplicación para dispositivos móviles (Android e IOS, incluidos los servicios web vinculados, si los hubiera).

Las auditorías se basarán en estándares internacionalmente reconocidos como: CWE (Common Weakness Enumeration), Open Web Application Security Project (OWASP), Open Source Security Testing Methodology Manual (OSSTMM), etc.

La auditoría de código contemplará:

- Análisis inicial y revisión de documentación: con el objetivo de conocer y analizar cada aplicación y sus usos, así como los flujos de información presentes.
- Análisis estático: mediante herramientas automatizadas, suministradas por el adjudicatario para la prestación del servicio, se comprobará el código fuente en

busca de patrones que identifiquen vulnerabilidades típicas: Cross-Site Scripting (XSS), Inyecciones SQL, Inclusiones locales o remotas, ejecución de comandos, fugas de información, etc.

- Revisión manual de código fuente: como complemento al análisis estático, con objeto de eliminar falsos positivos o detectar vulnerabilidades o problemas potenciales fuera del alcance de las herramientas automatizadas.
- Análisis dinámico: con especial atención a los posibles puntos de entrada de la aplicación, generación de resultados de salidas, manipulación de errores, etc.
- Informe de resultados.

4.2 Medios técnicos y humanos

El Equipo Técnico de Seguridad lo constituirán los profesionales que, como equipo principal, sean responsables de la ejecución del trabajo del Centro de Operaciones de Ciberseguridad, siendo necesario un equipo multidisplicinar con formación y experiencia en seguridad técnica, organizativa y legal. Deberán disponer de la cualificación, conocimiento y experiencia adecuados a la naturaleza de los trabajos, tal y como se exige en este apartado.

Los recursos necesarios para la prestación de los servicios descritos en el presente documento serán los adecuados para realizar con garantía las tareas definidas, teniendo en cuenta los criterios que se detallan a continuación.

4.2.1 Jefe de Proyecto

- Titulación universitaria de grado superior en el ámbito de las Tecnologías de la Información, Computación, Telecomunicaciones o Industria.
- Contará con experiencia mínima de 6 años en actividades en gestión y coordinación de proyectos relativos a la Seguridad de los Sistemas de Información, Planes Directores de Seguridad, Oficinas Técnicas de Seguridad, Equipos de Respuesta ante ciber-incidentes, Planes Estratégicos de Seguridad de la Información, Plantes de Continuidad de Negocio, etc.
- Deberá haber dirigido, al menos, dos (2) proyectos similares o análogos a los del presente contrato en los últimos cinco (5) años.
- Deberá acreditar conocimiento en metodologías de gestión de proyectos (PMI u otras), mediante certificados de formación.
- Deberá estar en posesión de, al menos, dos (2) certificaciones de seguridad de las recogidas en el Anejo III “Certificaciones de Seguridad”.

4.2.2 Personal adscrito al Centro de Operaciones de Ciberseguridad (SOC)

4.2.2.1 Responsable del SOC

- Titulación universitaria de grado medio o superior en el ámbito de las Tecnologías de la Información, Computación, Telecomunicaciones o Industria.

- Contará con una experiencia mínima de 5 años en:

  - Gestión de equipos de Respuesta ante Incidentes informáticos (SOC, CERTSI)
  - Diseño, administración y operación de herramientas de seguridad (NGF, WAF, SIEM, MDM, Antimalware, Antispam, etc.).
  - Gestión y operación de sistemas y herramientas de alerta temprana.
  - Gestión de ciberincidentes.
  - Seguimiento y control de tickets de operaciones, informe y soporte a cliente.

  Además de contar con conocimientos generales sobre:

  - Realización de auditorías técnicas de Seguridad.
  - Análisis y gestión de vulnerabilidades
  - Administración y bastionado de equipos y sistemas operativos Windows y Linux.
  - Diseño seguro y administración de redes y hardware de comunicaciones.
  - Programación, administración y bastionado de portales web.
  - Análisis de malware y fraude electrónico.
  - Análisis forense.
  - Seguridad en dispositivos móviles (Android e IOS).

4.2.2.2 Técnicos del SOC

En el caso del equipo de técnicos que integran el SOC se deberá acreditar, para cada uno, una experiencia mínima de 1 año en:

- Pertenencia a equipos de Respuesta ante Incidentes informáticos (SOC, CERTSI)
- Diseño, administración y operación de herramientas de seguridad (NGF, WAF, SIEM, MDM, Antimalware, Antispam, etc.).
- Gestión y operación de sistemas y herramientas de alerta temprana.
- Gestión de ciberincidentes.

Las empresas licitantes desarrollarán en sus ofertas el equipo de trabajo propuesto para la asistencia remota y presencial (en caso de incidentes graves) garantizando las adecuadas condiciones laborales de los trabajadores (rotaciones, vacaciones, descansos, bajas, etc.).

4.2.2.3 Equipo Técnico de seguridad

Para el resto de tareas a realizar en el alcance del presente contrato (Hacking Ético, Análisis Forense, Recogida de Evidencias y atención "in situ" a ciberincidentes, etc.), el personal propuesto por el adjudicatario podrá formar, o no, parte del equipo de Técnicos del SOC, si bien y en todo caso, deberá contar con:

- Titulación universitaria de grado medio o superior en el ámbito de las Tecnologías de la Información, Computación, Telecomunicaciones o Industria.

- Contar con al menos dos años de experiencia en:

  - Realización de auditorías técnicas de Seguridad.
  - Análisis y gestión de vulnerabilidades
  - Administración y bastionado de equipos y sistemas operativos Windows y Linux.
  - Diseño seguro y administración de redes y hardware de comunicaciones.
  - Programación, administración y bastionado de portales web.
  - Análisis de malware y fraude electrónico.
  - Análisis forense.
  - Seguridad en dispositivos móviles (Android e IOS).
  - Desarrollo seguro de software.

Específicamente alguno de los perfiles propuestos para la realización de los Test de Seguridad (Hacking Ético), deberá contar con experiencia acreditada mínima de dos años en realización de auditorías técnicas de seguridad en entornos OT (Tecnologías de la Operación).

4.2.3 Consideraciones finales.

Los requerimientos indicados en la descripción de cada uno de los perfiles profesionales se consideran requerimientos mínimos, de manera que serán rechazadas las ofertas que no los acrediten, siendo una obligación contractual esencial la adscripción al contrato durante toda su duración de estos perfiles profesionales, por lo que el incumplimiento de esta obligación podrá conllevar la resolución anticipada del contrato.

Las empresas licitantes deberán especificar únicamente los nombres de los técnicos adscritos al proyecto en sus diferentes perfiles, absteniéndose de incluir cualquier otro que no lo sea. En caso de resultar adjudicataria, el equipo de personas que se incorporará para la ejecución de los trabajos tras la formalización del contrato deberá estar formado por los componentes relacionados en la oferta adjudicataria. El incumplimiento de esta obligación sin causa justificada podrá dar lugar a la resolución del contrato con pérdida de la fianza.

En el Anejo I se incluyen las plantillas a utilizar para aportar la información del personal adscrito al proyecto, así como la de la empresa licitadora. Cabe señalar que los perfiles profesionales presentados en la oferta, con sus cualificaciones, serán vinculantes para el ofertante en caso de resultar adjudicatario de la oferta. Asimismo, deberán incluir la documentación que acredite la experiencia y formación exigidas y también su pertenencia a la plantilla del licitador mediante copia del último TC2, donde deberán remarcarse los datos de las personas propuestas en la oferta para facilitar su localización. CABB se reserva el derecho de comprobar el cumplimiento de estos requerimientos de cualificación y experiencia. Se rechazarán aquellas ofertas que no acrediten el mínimo exigido y no se tendrán en cuenta aquellos aspectos que no estén acreditados. CABB se reserva el derecho de requerir al licitador otras pruebas si no considerara suficientes las aportadas. En el Anexo 1 del Pliego de Cláusulas Administrativas Particulares se indica en qué momento ha de aportarse esta información.

En el caso de que alguna de las personas que se pretende adscribir al contrato no figure en la plantilla del licitador en el momento de presentar la oferta, se deberá adjuntar un documento firmado por el licitador y el trabajador o trabajadora propuesta en el que ambos se comprometan a que en caso de que la oferta resulte adjudicataria, esa persona será dada de alta en la plantilla como condición previa a la formalización del contrato. De no acreditarlo, la adjudicación será revocada.

CABB considera un factor clave para el éxito del proyecto la continuidad en el equipo de trabajo asignado al proyecto, por lo que, si bien entiende que la gestión de su personal es responsabilidad del adjudicatario, es deseable un nivel de rotación del personal limitado, lo que será tenido en cuenta en los ANS referidos al personal.

La composición del equipo de trabajo no podrá ser modificada sin el consentimiento expreso de CABB, que lo otorgará siempre que se acredite que el sustituto o sustitutos propuestos cuenta con una cualificación técnica y experiencia igual o superior al del componente del equipo que se pretende sustituir. En su caso, cualquier modificación deberá solicitada por escrito con al menos 15 días naturales de preaviso.

Los posibles inconvenientes de adaptación al entorno de trabajo y al proyecto debidos a las sustituciones en los componentes del equipo, deberán subsanarse mediante periodos de solapamiento sin coste adicional y durante el tiempo necesario para garantizar una transición sin afección al servicio. El adjudicatario deberá asegurar la transferencia de conocimiento del recurso sustituido hacia el resto del equipo de trabajo.

La modificación de alguno de los componentes del equipo adscrito a la ejecución de los trabajos, sin observar el procedimiento y los requisitos anteriores, facultará a CABB para calificar dicha modificación como una rotación no planificada.

4.3 Supervisión y control

A los efectos de la Disposición Adicional Primera del RD 20/2012, de 13 de julio, se recuerda que la contratación para los servicios de soporte y mantenimiento de las aplicaciones de los sistemas de control para CABB, comporta únicamente el nacimiento de una relación mercantil entre CABB y la adjudicataria, la cual desarrollará los servicios contratados con plena independencia y autonomía en la organización de los recursos humanos y materiales para la ejecución de los mismos, sin que de ella se derive nacimiento de relación laboral alguna entre los trabajadores de la contratista y CABB.

A tales efectos, el supervisor designado por CABB para el control de la calidad y adecuación de los servicios contratados, no ostentará ninguna facultad de organización, control o asignación de funciones sobre los trabajos desarrollados por los trabajadores de la contratista, limitando su interlocución al reporte de las necesidades del servicio y el ajuste de los mismos en los términos acordados, a la persona designada por la adjudicataria como interlocutora, sin suponer injerencia alguna en el servicio contratado.

Se establecen las siguientes figuras y órganos de dirección del proyecto:

- Supervisor del contrato (Responsable por parte de CABB).
- Jefe del Proyecto (Responsable del Contrato por parte del adjudicatario).

El Supervisor del contrato será un técnico designado por CABB que realizará las siguientes funciones principales:

- Dirigir, supervisar y coordinar la realización y desarrollo de los trabajos, velando por su nivel de eficiencia y calidad.
- Hacer cumplir las normas de funcionamiento y las condiciones estipuladas en este Documento.
- Aprobar las planificaciones de realización de los trabajos.
- Decidir sobre la aceptación de las propuestas técnicas realizadas por el Jefe del Proyecto a lo largo del desarrollo de los trabajos.
- Asegurar el seguimiento del programa de realización de los trabajos.
- Autorizar cualquier alteración de la metodología o procedimientos empleados en la realización de las actividades y tareas encomendadas al servicio.
- Revisar y validar los informes de actividad.
- Velar por el cumplimiento de los Acuerdos de Nivel de Servicio establecidos y aplicar las sanciones que correspondan en casos de incumplimiento.
- Controlar económicamente la ejecución del proyecto y aprobar los pagos.

El adjudicatario nombrará un Jefe de Proyecto, cuyas funciones principales serán las siguientes:

- Dirigir a los medios personales que presten los servicios impartiendo al efecto las órdenes e instrucciones necesarias para su ejecución.

- Realizar las funciones de contacto directo de los medios personales que presten los servicios con CABB.
- Proponer al Responsable del Proyecto de CABB las modificaciones o mejoras que estime necesarias para la optimización de los sistemas de seguridad de CABB.
- Asegurar el nivel de calidad de los trabajos.
- Actuar como interlocutor con otros equipos de trabajo y coordinar los mismos cuando tengan que intervenir en actividades planificadas.

4.3.1 Obligación de información

Durante la ejecución de los trabajos objeto del contrato, el adjudicatario deberá facilitar al técnico supervisor del proyecto designado por CABB la información y documentación que éste solicite para disponer de un pleno conocimiento de las circunstancias en las que se desarrollan los mismos, así como de los eventuales problemas que puedan plantearse y los recursos utilizados para resolverlos.

Será necesario presentar un informe mensual de seguimiento de la actividad que recoja, entre otras cuestiones, las siguientes:

- Informe de incidentes de seguridad atendidos
- Trabajos realizados y resultados obtenidos en el período en curso.
- Trabajos planificados para el siguiente período.
- Incidencias tanto técnicas, como del equipo de trabajo, que afecten a la ejecución de las tareas asignadas, así como propuestas o alternativas para su resolución.

Asimismo, el Jefe de Proyecto del adjudicatario estará obligado a asistir a las reuniones de seguimiento del proyecto que se establezcan por parte de CABB, quién se compromete a citar con la debida antelación al adjudicatario.

4.3.2 Niveles de prestación del servicio

La atención (clasificación, priorización, escalado y gestión) a las comunicaciones de incidentes de seguridad notificados a través de los canales establecidos procedimentalmente, por parte de los interlocutores de CABB, se realizará diligentemente y conforme a los niveles de servicio que se recogen en el Anejo IV. No se contabilizarán en los tiempos de respuesta del adjudicatario aquellos imputables a terceros y que impidan las actuaciones a realizar. A modo indicativo, se considerarán incidentes críticos aquellos que:

- Afecten, o supongan un riesgo elevado de afección, a los sistemas críticos de la compañía establecidos de acuerdo a los procedimientos internos.

- Supongan un impacto significativo sobre un elevado número de sistemas, departamentos o personas, afectando a su operación (afección a más del 10% de usuarios activos).
- Afecte a información confidencial o sensible de la compañía, en particular aquella sujeta a las regulaciones en materia de protección de datos de carácter personal.
- Supongan una alta probabilidad de propagarse dentro de la organización causando daños significativos o interrupción de servicios
- Afecten sobre sistemas electrónicos de información al público con probable impacto sobre los clientes.
- Impliquen posibilidad de amenazas para la seguridad física de las personas.

4.4 Subcontratación

Habida cuenta la condición de CABB como proveedor de un servicio esencial para la sociedad, se consideran críticas todas las tareas que debe realizar el SOC por razón de la sensibilidad de la información que se maneja y la interacción directa que se requiere entre el personal técnico del SOC y el de CABB al objeto de lograr una coordinación adecuada, ágil y eficaz en la gestión y resolución de los ciberincidentes o fallos de seguridad informática que pudieran observarse, por lo que queda prohibida la subcontratación.

4.5 Fases del proyecto

El desarrollo del proyecto en el marco temporal del contrato deberá contar con una planificación. Las empresas licitadoras propondrán un Plan de Proyecto estructurado en una serie de fases de alto nivel en las cuales se llevarán a cabo un conjunto mínimo de servicios a prestar. Las fases y los servicios que constituirán el alcance mínimo de cada una de ellas, se describen a continuación.

4.5.1 Fase de Implantación

Durante esta fase el adjudicatario iniciará la asunción de los servicios integrando sus equipos de trabajo, tomando conocimiento de las infraestructuras, entornos técnicos, procedimientos de trabajo, herramientas y estándares de CABB, e incluyendo las actividades necesarias y la elaboración de documentación a que hubiera lugar para la transferencia del conocimiento y adecuada prestación del servicio.

Se incluyen en esta fase los trabajos para la implantación del sistema de monitorización de eventos (hardware, software y comunicaciones), en coordinación con el personal técnico de CABB, así como la ejecución de los servicios iniciales de auditoría perimetral e interna (Hacking

Ético), y análisis de vulnerabilidades que permitan establecer una línea base con la situación de partida al inicio del servicio.

Esta Fase tendrá una duración máxima de cinco meses para la plena puesta en marcha del Contrato.

4.5.2 Fase de Pleno Servicio

Tras la fase de implantación el adjudicatario deberá prestar el servicio completo bajo las condiciones exigidas en el presente pliego y en el contrato.

4.5.3 Fase de Devolución de los servicios

Esta fase se deberá realizar cuando se determine la finalización del servicio, ya sea por cumplimiento del plazo inicial establecido para el contrato, o por la resolución del contrato instada por alguna de las partes con base en el incumplimiento contractual.

Durante esta fase el adjudicatario deberá comprometer los recursos y ejecutar, con total diligencia y plena colaboración, las actividades necesarias para devolver el servicio a CABB o a quien esta designe. Entre estas actividades se incluyen la devolución de toda la documentación elaborada durante el proyecto (procedimientos, informes, etc.) que no obrasen en poder de CABB y toda la información relacionada con la plataforma de monitorización y correlación de eventos, en particular las reglas de correlación y los eventos registrados durante un año, en formato estándar de forma que puedan ser reutilizados en otra plataforma.

La fase de devolución se deberá iniciar al menos con tres meses de antelación a la fecha prevista de finalización del servicio, ya sea total por cumplimiento del plazo inicial establecido para el contrato o del plazo de sus prórrogas, o parcial por resolución del contrato. Adicionalmente a la devolución de los servicios, la ejecución de los mismos durante la fase de devolución seguirá siendo responsabilidad del adjudicatario a todos los efectos.

4.6 Metodología de trabajo

CABB está encauzando la gestión de sus servicios de Seguridad de la Información y de TIC a un modelo de procesos que garanticen la mejora continua. Para conseguirlo, todas las actividades derivadas de lo solicitado en este pliego deberán ser abordadas desde la perspectiva ofrecida por la ISO 27001 y el conjunto de buenas prácticas contenido en ITIL.

Durante la vigencia del contrato el adjudicatario deberá atenerse a los procedimientos, procesos y metodologías aprobados por CABB en cualquiera de sus formas.

4.7 Otras condiciones

4.7.1 Lugar de prestación del servicio

Los trabajos presenciales previstos en el proyecto se desarrollarán en las oficinas centrales de CABB ubicadas en:

Oficinas Centrales de CABB
c/ San Vicente 8, Edificio Albia 1ª planta
48001 Bilbao

No se excluye la posibilidad de realizar alguna reunión o entrevista puntual en otras sedes de la compañía o instalaciones de terceros para obtener algún tipo de información adicional o realizar alguna de las actividades de ingeniería social previstas en los servicios de Hacking Ético.

El trabajo no presencial, correspondiente al servicio de SOC, se desarrollará en las dependencias del adjudicatario, excepto aquellos servicios que por sus características deban desarrollarse total o parcialmente en las instalaciones de CABB (por ejemplo, reuniones de seguimiento, pruebas de Hacking Ético o resolución de incidentes de especial gravedad).

Las reuniones de seguimiento entre el responsable por parte de CABB y el Jefe de Proyecto por parte del adjudicatario podrán realizarse indistintamente en las dependencias de CABB o del adjudicatario, según estime necesario el responsable del proyecto por parte de CABB y debe estar contemplado en la oferta del licitador.

Para actuar frente a un incidente de seguridad grave, la empresa adjudicataria deberá poder acudir a CABB en un plazo máximo de 2 horas. En la oferta técnica, se deberá documentar adecuadamente esta capacidad.

El contratista deberá dar cumplimiento al Anejo II de este pliego, correspondiente a Prevención de Riesgos Laborales.

4.7.2 Horario de prestación del servicio

La actividad de Centro de Operaciones de Ciberseguridad (SOC) se prestará bajo el siguiente esquema:

- Servicio remoto: Su trabajo se desarrollará en horario 24 x 7 efectuándose en su mayor parte desde las dependencias de la empresa adjudicataria, excepto aquellos servicios

que por sus características deban desarrollarse total o parcialmente en las instalaciones de CABB (por ejemplo, pruebas de Hacking Ético).

- Atención presencial: en caso de incidente de seguridad grave, personal especializado del SOC deberá desplazarse a instalaciones de CABB, para lo que el licitador deberá prever un mínimo de 20 horas anuales de prestación presencial. El equipo de trabajo deberá ser dimensionado por el adjudicatario en base a la información suministrada en el pliego, así como a su experiencia por el tipo de actividades a realizar.

4.7.3 Acceso a los sistemas CABB

El adjudicatario queda obligado a establecer una conexión privada a la Red Corporativa de Datos de CABB para realizar los trabajos especificados en el presente contrato que así lo requieran.

Para realizar la interconexión de las comunicaciones entre la organización del adjudicatario y el CABB, el adjudicatario deberá proporcionar dos líneas dedicadas de internet, de diferente operador de telecomunicaciones, para ofrecer y garantizar la continuidad del servicio y dotarlo de alta disponibilidad.

Los equipos de red de estas líneas de operador, que son necesarios dentro de las oficinas del CABB, se instalarán en los centros de proceso de datos de las oficinas de Bilbao en dos ubicaciones distintas, o en otra ubicación de CABB, que así lo especifiquen los técnicos del CABB durante la ejecución.

Las comunicaciones entre ambas partes deberán estar tunelizadas mediante túneles IPSec a fin de garantizar el envío de tráfico seguro entre las dos partes.

Será a criterio de CABB, previa propuesta el adjudicatario, la definición última de las características y capacidad de las líneas de comunicaciones, una vez analizados los requisitos y volumen de tráfico de la conexión.

El adjudicatario deberá adoptar las medidas de seguridad que sean necesarias para garantizar que la solución del servicio sea únicamente accesible por el personal autorizado para ello, tanto por parte del adjudicatario como del CABB; y mantenerlo aislado del resto de clientes de otros servicios.

Queda dentro del alcance del presente pliego por parte del contratista y sin coste adicional, proporcionar todos los elementos físicos, licencias y configuración necesarios para cumplir estos requisitos.

4.8 Causas de resolución del contrato

Los siguientes supuestos suponen el incumplimiento de obligaciones esenciales por lo que, sin menoscabo de aquellas otras indicadas específicamente en cualquier otro apartado del presente documento, así como las recogidas en el PCAP, pueden dar lugar a la resolución del contrato atendidas las circunstancias del caso:

- La aportación de información falsa o imprecisa por parte del adjudicatario, incluso aquella aportada durante el proceso de Licitación, o durante cualquier fase del proyecto.

- La falsedad en el nivel de conocimientos del equipo ofertado y los conocimientos reales demostrados en la ejecución de los trabajos, o una prestación del servicio manifiestamente ineficiente o negligente.

- El incumplimiento de la obligación contractual esencial de prestar el servicio contratado con los medios humanos de la cualificación y experiencia comprometidos en la oferta.

- La falta de respuesta reiterada a los requerimientos del Supervisor de Proyecto de CABB, en particular:

  - Incumplimientos injustificados de los horarios del servicio de atención presencial

  - Faltas reiteradas e injustificadas en la atención a las llamadas telefónicas o correos electrónicos recibidos.

  - Incumplimiento reiterado de los Acuerdos de Nivel de Servicio.

- La violación, en cualquiera de sus aspectos, del apartado 4.10 “Confidencialidad de la Información” del presente documento.

4.9 Confidencialidad de la información

CABB considera que toda la información y documentación manejada durante el proyecto, del tipo que sea (electrónica, escrita o impresa, visual, verbal…), es estrictamente confidencial, por lo que cualquier vulneración de este principio que se observe será objeto de sanción de acuerdo a los términos establecidos en el apartado correspondiente de este pliego, incluso llegando a ser causa de resolución inmediata del contrato si así se estimara, todo ello sin perjuicio de las responsabilidades penales o de otro tipo a que hubiera lugar.

Toda la información y documentación que se maneje en el ámbito del presente contrato es propiedad de CABB. El adjudicatario se compromete a no difundir ni divulgar esta información, ni hacer uso alguno de ella más allá de las actividades vinculadas al contrato y que hayan sido expresamente autorizadas por escrito por CABB, así como a devolver la documentación que obre

en su poder a la finalización del mismo, incluso aquella almacenada en formato electrónico o por cualquier otro medio existente o futuro. Esta obligación ostentará el carácter de indefinida, desde el momento de la adjudicación de los trabajos.

El adjudicatario está obligado a comunicar a CABB la relación del personal de la organización implicado en el proyecto, solicitando autorización previa para aquellos que deban hacer uso de esta información, así como informar de cualquier modificación en esta relación que pueda ocurrir durante el desarrollo del proyecto.

Además de las anteriores obligaciones, el personal del adjudicatario está obligado a:

- Adaptarse a, y cumplir estrictamente, las normas internas de CABB en cuanto a políticas de seguridad, así como cualquier otra que sea de aplicación durante este proyecto.

- Mantener la información confidencial en estricta reserva y debidamente protegida mientras obre en su poder.

- Divulgar la información confidencial únicamente a las personas autorizadas para su recepción dentro de la organización.

- Instruir al personal que estará encargado de recibir la información confidencial en el correcto uso de la misma y sus responsabilidades adquiridas.

Previo al inicio de la prestación del servicio será requisito indispensable dar cumplimiento a los requisitos previstos en el Sistema de Gestión de la Seguridad de la Información (SGSI) de CABB, en particular:

- Cuestionario de Evaluación de Riesgos de Terceros
- Compromiso de Confidencialidad
- Aceptación de las Normas de Uso

Para la ejecución del contrato será necesario que el adjudicatario tenga acceso y realice tratamientos de datos de carácter personal de los datos aportados por CABB (en concreto, datos de usuarios de las redes y sistemas de información de CABB como nombre, apellido, DNI, datos generales de navegación como URL y nombre de archivos descargados, asunto, remitente o destinario de los correos electrónicos enviados o recibidos), por lo que asumirá las funciones y obligaciones que el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, estipula para los Encargados de Tratamiento. En cumplimiento del artículo 28 de dicho Reglamento, este acceso y tratamiento de datos de carácter personal quedará regulado en un contrato específico que se formalizará tras la adjudicación (Contrato como Encargado de Tratamiento). Las condiciones y términos de acceso por parte del adjudicatario a datos personales como parte de la prestación del servicio

se regularán por escrito en dicho contrato, estableciéndose expresamente que el adjudicatario, como Encargado del Tratamiento, únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad que el Encargado del Tratamiento está obligado a implementar. Además, estará obligado a elaborar la Evaluación de Riesgos del tratamiento (o a apoyar a CABB en su elaboración si así fuese requerido) y, en función del resultado de dicho análisis, la Evaluación de Impacto en la Privacidad.

4.10 Documentación de los trabajos

El adjudicatario deberá suministrar a CABB las nuevas versiones de la documentación que se vaya generando como parte del servicio.

4.11 Sanciones y Penalizaciones

Se podrán aplicar las siguientes sanciones, sin perjuicio de las establecidas en el PCAP:

- El incumplimiento de los niveles de servicio establecidos se penalizará de acuerdo a lo recogido en las tablas del Anejo IV “Acuerdos de nivel de servicio”, siempre que las causas sean imputables al adjudicatario.

- El incumplimiento por parte del adjudicatario de la cláusula de confidencialidad supondrá una sanción económica del 30% del importe de adjudicación, y adicionalmente podrá acarrear la resolución del contrato si CABB así lo considera.

- El incumplimiento por parte del adjudicatario de la obligación de prestar el servicio con los medios humanos de la cualificación y experiencia exigidas, conllevará una sanción de cuatrocientos euros (400 €) por cada día y medio humano de incumplimiento, sin perjuicio de la posibilidad de resolución del contrato por esta causa.

La imposición de la sanción económica o la resolución del contrato no impide a CABB el exigir al adjudicatario el cumplimiento de sus obligaciones contractuales ni la indemnización de daños y perjuicios a que pudiera tener derecho, ni tampoco le eximiría de cualquier otra responsabilidad, penal o de cualquier otro tipo en la que hubiera incurrido.

5 DURACIÓN

El contrato tendrá una duración de 1 año, con posibilidad de 2 prórrogas consecutivas de un año cada una.

Las prórrogas serán optativas para CABB y obligatorias para el adjudicatario, siempre y cuando sea preavisado con al menos dos meses de antelación sobre la fecha de finalización del contrato.

No obstante lo anterior, por tratarse de servicios que atienden una necesidad permanente, llegado a su término CABB podrá prorrogar el contrato, de forma obligatoria para el contratista, hasta que un nuevo adjudicatario se haga cargo del servicio, sin que esta prórroga pueda superar los seis meses, y sin que sea de aplicación a este caso el plazo de preaviso indicado anteriormente.

El cómputo de los plazos comenzará con la firma del Acta de Inicio de los trabajos, que deberá realizarse en la fecha que indique el Supervisor del Contrato y que en ningún caso superará los 30 días desde la fecha de la firma del contrato.

No se efectuará revisión del precio de adjudicación, ni aún en caso de prórroga del contrato.

05 de marzo de 2025

Fdo:

Marian Mena Domínguez
Gestor del contrato

Jose Luis Unzueta Portillo
Subdirector de informática

ANEJO I
PLANTILLAS PARA PRESENTACIÓN DE LA DOCUMENTACIÓN PARA LA EVALUACIÓN DEL EQUIPO DE TRABAJO: CURRICULUM VITAE

Información personal

Nombre	**[Apellidos, Nombre]**
Domicilio	
Nacionalidad	
Fecha de nacimiento	**[Día/mes/año]**

Experiencia laboral

Fechas (de – a)	Duración	Nombre y dirección del empleador	Tipo de empresa o sector	Puesto o cargo ocupados	Principales actividades y responsabilidades
[Empezar por el más reciente e ir añadiendo aparte la misma información para cada puesto ocupado.]	[Expresada en años con decimales]				[De forma genérica]

Proyectos en los que ha participado

Título del proyecto	Descripción del proyecto	Entidad empleadora	Entidad destinataria	Actividad realizada	Duración	Metodología y herramientas utilizadas
[Indicar exclusivamente para aquellos similares al objeto de este proyecto]		[Tal como esté identificada en el apartado de "Experiencia Laboral"]		[Descripción de las funciones realizadas]	[Expresada en meses]	

Educación y formación (reglada)

Fechas (de – a)	Nombre y tipo de organización que ha impartido la educación o la formación	Principales materias o capacidades ocupacionales tratadas	Título de la cualificación obtenida
[Empezar por el más reciente e ir añadiendo en líneas inferiores la misma información para cada curso realizado relacionado con el objeto del proyecto.]			

Formación complementaria

Fechas (de – a)	Número de horas formativas	Nombre y tipo de organización que ha impartido la educación o la formación	Principales materias o capacidades ocupacionales tratadas	Acreditación obtenida
[Empezar por el más reciente e ir añadiendo en líneas inferiores la misma información para cada curso realizado relacionado con el objeto del proyecto.]				[Si procede]

Información adicional	[Introducir aquí cualquier información que se considere relevante para el objeto del este proyecto]

ANEJO II

PREVENCIÓN DE RIESGOS LABORALES

ANEXO: PREVENCIÓN DE RIESGOS LABORALES

1 MEDIDAS DE PREVENCIÓN Y PROTECCIÓN

La empresa adjudicataria aplicará las medidas que integran el deber de prevención previsto en el artículo 14 de la Ley de Prevención de Riesgos Laborales, con arreglo a los siguientes principios: a) Evitar los riesgos.

b) Evaluar los riesgos que no se puedan evitar.
c) Combatir los riesgos en su origen.
d) Adaptar el trabajo a la persona, en particular en lo que respecta a la concepción de los puestos de trabajo, así como a la elección de los equipos y los métodos de trabajo y de producción, con miras, en particular, a atenuar el trabajo monótono y repetitivo y a reducir los efectos del mismo en la salud.

e) Tener en cuenta la evolución de la técnica.
f) Sustituir lo peligroso por lo que entrañe poco o ningún peligro.
g) Planificar la prevención.
h) Dar las debidas instrucciones a los trabajadores.

2 MODALIDAD PREVENTIVA

La empresa adjudicataria acreditará a CABB el modelo de organización de la Prevención de Riesgos Laborales adoptado para el desarrollo de las actividades preventivas, incluyendo el o los responsables en materia de prevención de riesgos laborales. En caso de que el modelo adoptado sea el concierto con un Servicio de Prevención Ajeno, la empresa adjudicataria aportará copia del contrato en vigor.

A su vez remitirá el contrato de asociación a la correspondiente Mutua de accidentes de trabajo y enfermedades profesionales.

3 EVALUACIÓN DE RIESGOS Y PLANIFICACIÓN DE ACTIVIDADES

La empresa adjudicataria deberá disponer de la Evaluación de Riesgos, y su correspondiente Planificación de Actividades Preventivas, de los trabajadores objeto del presente Pliego de Prescripciones, de acuerdo con el artículo 16 de la Ley 31/ 1995. Una vez elaborada, la empresa adjudicataria tendrá a disposición de CABB dicha documentación para su control.

4 EVALUACIÓN DE RIESGOS DE LOS CENTROS DE CABB

La empresa adjudicataria, antes del comienzo de los trabajos, recibirá del Supervisor de CABB información sobre los riesgos inherentes a los Centros de Trabajo/ Instalaciones a los que accederán los trabajadores objeto del presente Pliego de Prescripciones.

Esta información será entregada por escrito, en caso de que en las instalaciones en las que se realizarán los trabajos existan riesgos graves o muy graves, estando obligada la empresa contratista a firmar el recibí de dicha información.

5 MEDIDAS DE EMERGENCIAS

La empresa adjudicataria, al acceder a los Centros de Trabajo de CABB, recibirá información sobre las medidas de emergencia a tener en cuenta en los Centros de Trabajo/ Instalaciones a los que accederán los trabajadores objeto del presente Pliego de Prescripciones.

6 VIGILANCIA DE LA SALUD

La empresa adjudicataria garantizará a los trabajadores a su servicio la vigilancia periódica de su estado de salud en función de los riesgos inherentes al trabajo, y los protocolos de reconocimientos específicos, aplicados cuando sea necesario.

La empresa adjudicataria está obligada a presentar a CABB, si ésta lo requiriera, la documentación acreditativa de la modalidad en materia de Vigilancia de la Salud adoptada por ésta, así como los Reconocimientos Médicos de todos sus trabajadores con la calificación de APTO de acuerdo con el puesto de trabajo a desempeñar.

7 FORMACIÓN E INFORMACIÓN

La empresa adjudicataria garantizará la adecuada formación y adiestramiento de su personal en materia de Prevención de Riesgos Laborales y Primeros Auxilios, dando cuenta documentalmente de las acciones llevadas a cabo para ello. Además, la empresa adjudicataria pondrá a disposición de CABB la documentación que acredite la explicación a su personal de la Evaluación de Riesgos y Plan de Acción Preventiva llevada a cabo en su empresa, y que poseen la formación específica necesaria al respecto.

La empresa contratista será responsable de trasladar a los trabajadores designados para los trabajos objeto del presente pliego toda la información en materia de prevención que le sea trasladada en cumplimiento de la obligación de coordinación de actividades empresariales, y tendrá a disposición de CABB los registros correspondientes de la difusión de dicha información.

8 EQUIPOS DE PROTECCIÓN INDIVIDUAL

De acuerdo con el Plan de Acción Preventiva de la Evaluación de Riesgos que deberá realizar la empresa adjudicataria, es responsabilidad de la misma la entrega de los equipos de protección individual (EPI´s) para la realización de los trabajos objeto del presente pliego, así como el empleo de los mismos por sus trabajadores, entendiendo por equipo de protección individual, cualquier equipo destinado a ser llevado o sujetado por el trabajador para que le proteja de uno o varios riesgos, que puedan amenazar su seguridad o su salud, así como cualquier complemento o accesorio destinado a tal fin.

La empresa adjudicataria tendrá a disposición de CABB el registro de entrega de EPI´s a los trabajadores. Así mismo realizará el mantenimiento y revisión de los EPI´s de acuerdo con las instrucciones del fabricante, y acreditará CABB los resultados de los mismos cuando ésta lo requiera.

9 ESTUDIO Y CONTROL DE LA SINIESTRALIDAD

En caso de accidente, la empresa adjudicataria lo notificará inmediatamente a CABB y le remitirá con la mayor brevedad posible el correspondiente informe de investigación.

10 AUDITORIA DE PREVENCIÓN

En caso de que la modalidad preventiva de la empresa adjudicataria no fuese concertada con un Servicio de Prevención Ajeno, y de acuerdo con el artículo 29 del Reglamento de los Servicios de Prevención, se tendrá a disposición de CABB el Informe de la preceptiva Auditoría de Prevención de Riesgos Laborales, así como el correspondiente Plan de Acciones Correctoras.

11 TÉCNICO RESPONSABLE

La empresa adjudicataria designará, con independencia de la modalidad de organización en materia de Prevención de Riesgos Laborales y de los recursos necesarios para el desarrollo de las actividades preventivas adoptadas, a un técnico interlocutor válido en materia de prevención de riesgos laborales con CABB.

12 COORDINACIÓN DE ACTIVIDADES EMPRESARIALES

En cumplimiento del Real Decreto 171/2004, CABB, dentro de su Sistema de Gestión de la Prevención de Riesgos Laborales, está implantando un Procedimiento para la Coordinación de Actividades Empresariales (GE 018.11), cuya aplicación es el medio de coordinación prioritario para las contrataciones de servicios. Su cumplimiento se considerará obligatorio para la empresa adjudicataria.

En los casos en que se estime conveniente, CABB y la empresa adjudicataria podrán establecer otros medios de coordinación complementarios. En estos casos, la empresa adjudicataria acreditará por escrito que ha informado a los trabajadores asignados para la realización de los trabajos objeto del presente Pliego, sobre los medios de coordinación establecidos en los términos previstos en el artículo 18.1 de la Ley 31/1995.

13 GESTIÓN

Toda la documentación en materia de Prevención de Riesgos Laborales, tanto la relacionada en el pliego de condiciones como cualquiera otra que CABB solicite a la empresa contratista, estará a disposición del Supervisor del Contrato o de las personas que se disponga desde CABB como encargados de la Coordinación de Actividades Empresariales.

El contratista acreditará en dicha plataforma el cumplimiento formal de los requisitos generales en materia de PRL y los específicos en relación a los trabajadores, maquinaria, equipos de trabajo, vehículos y medios auxiliares que se van a utilizar en el servicio según se indica en el presente anexo de PRL

De igual forma, la empresa adjudicataria deberá atender las peticiones que le realice CABB en aplicación de su Sistema de Gestión de la Prevención de Riesgos Laborales.

Listado de EMPRESAS													
Datos empresa Contratista									Vinculación en Proyecto		Persona de contacto plataforma SerCAE		
Razón social	CIF	Tipo de empresa	Tipo actividad empresa (Multi-respuesta)						Fecha Inicio	Fecha Fin	Nombre y apellidos	Email	Teléfono
			Empresa de coordinación de Seguridad y Salud	Actividad construcción	Actividad amianto (fibrocemento)	Actividad d Riesgo Eléctrico	Otra actividad						

14 PENALIZACIONES POR INCUMPLIMIENTO

Con independencia de otras responsabilidades legales en que el adjudicatario pueda incurrir por incumplimiento de la normativa de prevención de riesgos laborales, los incumplimientos de las obligaciones contenidas en este anexo se calificarán y penalizarán de la siguiente forma:

- Falta leve, que llevará aparejada penalización de 100 € a 300 €: el incumplimiento de las obligaciones contenidas en los apartados 2, 4, 9, 10, 11 y 12 de este Anexo.
- Falta grave, que llevará aparejada penalización de 301 € a 1.500 €: el incumplimiento de las obligaciones contenidas en los apartados 5, 6, 7, 8 y 13 de este Anexo.
- Falta muy grave, que llevará aparejada penalización de 1.501 € a 6.000 €: el incumplimiento de las obligaciones contenidas en los apartados 3 y 14 de este Anexo.

La incurrencia en tres (3) faltas leves, en el periodo de un año (o en el plazo de ejecución del contrato, si fuere inferior), será equivalente a la incurrencia en una falta grave.

La incurrencia en una (1) falta muy grave o en dos (2) faltas graves, en el periodo de un año (o en el plazo de ejecución del contrato, si fuere inferior), dará derecho a CABB a resolver el contrato con pérdida de la fianza definitiva.

NOTA 1: ***Todos los documentos exigidos en este anexo, deberán ser remitidos a CABB firmados por el responsable que designe la empresa adjudicataria.***

NOTA 2: ***Una vez adjudicado el contrato, la empresa adjudicataria, en caso de que observase cambios en los riesgos, medidas preventivas, instrucciones, procedimientos o procesos de CABB, que afecten a la Seguridad y Salud de los Trabajadores designados para la ejecución de los trabajos objeto del presente pliego, deberá comunicarlo al Supervisor del contrato de CABB.***

El Jefe de Prevención- CABB

	PROTOCOLO DE COORDINACIÓN DE ACTIVIDADES EMPRESARIALES CON EMPRESAS CONTRATISTAS	Expediente nº

Organización preventiva

Datos generales de la empresa

Nombre o Razón social	Domicilio Social		
Provincia	**Municipio**	**Código postal**	**Teléfono**

a) Asunción personal por el empresario

Nombre del empresario:

b) Designación uno o varios trabajadores (especificar nº trabajadores según nivel de formación en PRL)

Nivel básico		Nivel intermedio		Nivel superior	

c) Servicio de Prevención Propio y/o Ajeno

Especialidad	SPP	SPA	Nombre del SPA	Especialidad	SPP	SPA	Nombre del SPA
Seguridad Trabajo	☐	☐		Ergonomía y Psicosociología	☐	☐	
Higiene Industrial	☐	☐		Medicina del Trabajo	☐	☐	

Gestión de la prevención

La empresa garantiza el cumplimiento de las siguientes disposiciones:	**SI**	**NO**	**N.A.**
Tener realizada la evaluación de los riesgos para todas las actividades objeto del presente contrato.			
Haber realizado una planificación preventiva en base a la evaluación de los riesgos.			
Haber realizado la auditoría legal de prevención de riesgos laborales (sólo en el caso de Servicio de Prevención Propio)	☐	☐	☐
En relación con los trabajadores que participan en los trabajos objeto del presente contrato, la empresa garantiza que:	**SI**	**NO**	**N.A.**
Han recibido información preventiva sobre los riesgos y medidas de prevención y protección			
Tienen formación específica de los riesgos derivados de su puesto de trabajo			
Acreditación de que todos los trabajadores encargados del manejo y utilización de las grúas, dumpers y demás maquinaria utilizada en obra disponen de los carnés acreditativos de formación específica.	☐	☐	☐
Disponen de los medios de protección colectiva e individuales (EPI) adecuados a los trabajos			
Disponen del correspondiente certificado de aptitud médica para su trabajo habitual			
Disponen de certificados de cualificación profesional en caso de ser necesaria la realización de trabajos reglamentados.	☐	☐	☐
En caso de ser necesario el suministro por parte del contratista de equipos de trabajo, equipos de protección individual (EPI) o productos químicos, garantiza que:	**SI**	**NO**	**N.A.**
Se dispone de declaración de conformidad CE de los equipos de trabajo a emplear, o en su ausencia certificado de adecuación al Real Decreto 1215/1997	☐	☐	☐
Se dispone de declaración de conformidad CE de los EPI suministrados a sus trabajadores			
Se dispone de las fichas de seguridad de los productos químicos a emplear			
Plan de Prevención de riesgos laborales del contratista:	**SI**	**NO**	**N.A.**

Tiene implantado un Sistema de Gestión de Prevención de Riesgos Laborales			
Dispone de un Manual de Prevención de Riesgos Laborales			
Dispone de una Política de Prevención de Riesgos Laborales			
Ha definido por escrito las responsabilidades y funciones en Prevención de Riesgos Laborales			
Ha solicitado a los subcontratistas y trabajadores autónomos, la documentación acreditativa de haber cumplido con todas las obligaciones en materia de prevención y riesgos laborales	☐	☐	☐
Haber recibido de las empresas subcontratistas y trabajadores autónomos, la evaluación de riesgos laborales para los trabajos.	☐	☐	☐
Dispone de procedimientos o instrucciones por escrito para el desarrollo de la acción de prevención de riesgos con nombramiento de los recursos preventivos, cada vez que sea necesario su disponibilidad.	☐	☐	☐

Como responsable en materia preventiva, certifico el cumplimiento de los datos anteriormente expuestos y pongo a disposición de CABB la documentación acreditativa.

Nombre y Firma:	Cargo: Teléfono:	Fecha:

NOTA 1: Una vez adjudicados los trabajos, la empresa adjudicataria, en caso de que observase cambios en los riesgos, medidas preventivas, instrucciones, procedimientos o procesos de CABB, que afecten a la Seguridad y Salud de los Trabajadores designados para la ejecución de los trabajos objeto del presente pliego, deberá comunicarlo al Supervisor de Servicios Contratados En CABB.
NOTA 2: La Política de Prevención de Riesgos Laborales de CABB está disponible en todos sus Centros de Trabajo.

RELACIÓN DE PERSONAL INTERVINIENTE.

Fecha actualización:

NOMBRE TRABAJADOR	**D.N.I.**	**EMPRESA**

Sello de la empresa responsable de los trabajos

Fdo:
Cargo:
Empresa:

RELACIÓN DE MAQUINARIA Y MEDIOS AUXILIARES UTILIZADOS EN EL SERVICIO

Fecha actualización:

MODELO	**MATRICULA O Nº IDENTIFICACIÓN***	**EMPRESA DE MONTAJE***	**FECHA ULTIMA INSPECCION***	**FECHA DEL PROXIMA REVISIÓN***	**MARCADO CE****	**EMPRESA CONTRATANTE***

Sello de la empresa responsable de los trabajos

Empresa:

* Siempre que sea de aplicación ** En su defecto que sea de aplicación el R.D. 1215

Fdo:

Cargo:

POLÍTICA DEL SISTEMA INTEGRADO DE GESTIÓN (Rev.04)

CABB, como empresa que desarrolla una actividad orientada al ciudadano en todas las áreas relativas al ciclo integral del agua, considera la Calidad en la prestación de sus servicios, como factor clave de su Gestión. Para tal fin tiene establecido, a través de los distintos niveles jerárquicos, un Sistema Integrado de Gestión de: Calidad, Planes de Seguridad del Agua de Consumo, Prevención de Riesgos Laborales, Protección del Medio Ambiente e Investigación, Desarrollo e Innovación, y Energía.

A través de los principios indicados en esta Política, la Dirección de CABB muestra su compromiso de prestar un servicio adecuado a las necesidades de sus clientes y usuarios, proteger el medio ambiente, contribuir al uso sostenible del agua, garantizar la integridad de las personas eliminar los peligros y reducir los riesgos, impulsar la I+D+i, asegurar la inocuidad del agua en todo el Sistema General de Abastecimiento y mejorar la eficiencia energética de sus instalaciones y procesos para satisfacer las necesidades y expectativas de todas sus partes interesadas: clientes, usuarios, accionistas, personas de la organización, colaboradores, proveedores y sociedad en general. Estos principios son:

- Definir, implantar y mantener un Sistema Integrado de Gestión eficiente, dinámico y adecuado a la organización, conforme a esta Política, que permita establecer periódicamente objetivos y metas, así como controlar y evaluar su grado de cumplimiento, con el fin de mejorar continuamente su eficacia y desempeño.
- Cumplir los requisitos legales, reglamentarios y otros requisitos suscritos aplicables a nuestra actividad, así como los requisitos establecidos por las Normas de referencia, estableciendo procedimientos para conocerlos y mantenerlos actualizados.
- Garantizar la formación, sensibilización e información a los trabajadores, para concienciarles sobre la importancia del desarrollo correcto de sus actividades, enfatizando la consulta y participación e implicación activa en la consecución de los objetivos de la organización, así como los comportamientos creativos e innovadores.
- Integrar a nuestros colaboradores, contratistas y suministradores en el compromiso activo de mejora continua y actuar de forma transparente con las administraciones, instituciones y comunidades del entorno.
- Promover actuaciones encaminadas a la reducción de la accidentalidad laboral, a proporcionar condiciones de trabajo seguras y saludables para la prevención de lesiones y del deterioro de la salud, así como para la minimización de los impactos de nuestros vertidos, emisiones y consumos, teniendo en cuenta los medios técnicos y económicos disponibles y estableciendo los procedimientos adecuados de control, vigilancia, corrección y actuación frente a emergencias, fomentando la reutilización, el reciclado y la gestión adecuada de los residuos y de los recursos naturales.
- Promover el buen uso de la energía en la empresa, la mejora del diseño para lograr una mayor eficiencia energética de las instalaciones y procesos de la organización, así como la adquisición de productos y servicios energéticamente eficientes.
- Acometer proyectos de I+D+i acordes con esta Política, propiciando alianzas ventajosas y, de manera general, estableciendo medidas de protección de los resultados de dichos proyectos.
- Asegurar la disponibilidad de la información y los recursos necesarios para alcanzar los objetivos y metas.
- Ofrecer la máxima seguridad y confianza al consumidor mediante la aplicación de un estricto sistema de Análisis de Peligro y Puntos Críticos de Control basado en un permanente y exhaustivo control higiénicosanitario y de calidad del agua en todas las etapas del Sistema General de Abastecimiento, así como en general, un sistema de gestión del riesgo.
- El Sistema Integrado de Gestión se fundamenta en la prevención de no conformidades en general, y de la contaminación y daños y deterioro de la salud de las personas de la organización, en particular, por lo que todas las personas de la organización tienen la libertad y la responsabilidad de poner en conocimiento de la Dirección, por lo canales establecidos, cualquier situación real o potencial que ponga en peligro el correcto funcionamiento del Sistema.

El Sistema Integrado de Gestión se define y se desarrolla en el Manual del Sistema Integrado de Gestión y demás documentación emanada del mismo, siendo por tanto de obligado cumplimiento para todas las personas que tengan responsabilidades en la ejecución de actividades comprendidas en el Sistema Integrado de Gestión.

ANEJO III

CERTIFICACIONES DE SEGURIDAD

- Certificaciones de seguridad del EC-Council
- Certificaciones de seguridad de Information Systems Audit and Control Association (ISACA)
- Certificaciones de seguridad de International Information System Security Certification Consortium (ISC)[2]
- Certificaciones de seguridad de CompTIA
- Certificaciones de seguridad de Global Information Assurance Certification (GIAC)
- Certificaciones de seguridad de Institute for Security and Open Methodologies (ISECOM)
- BS 25999/UNE-ISO 22301 Lead Auditor
- CERT-Certified Computer Security Incident Handler Certification
- CISSP: Certified Information Systems Security Professional
- CHFJ: Computer Hacking Forensic Investigator ✓ CISMP: Information Security Management Principles.
- CNDA: Certified Network Security Arquitect
- CompTIA Security+
- CompTIA Advanced Security Practitioner
- ECSA: Certified Security Analyst
- ENSA: Network Security Administrator
- CCFE: Certified Computer Forensics Examiner
- CCNA Security: Cisco Certified Network Professional Security
- CCTHP: Certified Cyber Threat Hunting Professional
- CDDP: Certified Data Privacy Professional
- CDP: Certified Protection Professional
- CDRP: Certified Data Recovery Professional
- CEPT: Certified Expert Penetration Tester
- CEREA: Certified Expert Reverse Engineering Analyst
- CMWAPT: Certified Mobile and Web Application Penetration Tester
- CMFE: Certified Mobile Forensics Examiner
- CPT: Certified Penetration Tester
- CRTOP: Certified Red Team Operations Professional
- CREA: Certified Reverse Engineering Analyst
- CSSA: Certified SCADA Security Architect
- CSAP: Certified Security Awareness Practitioner ✓ CGEIT: Certified in the Governance of Enterprise IT ✓ CISA: Certified Information Systems Auditor.
- CISM: Certified Information Security Manager.
- CPP: Certified Protection Professional
- CREST: Penetration Testing Certifications
- CRISC: Certified in Risk and Information Systems Control
- CCSP: Cisco Certified Security Proffesional
- EC-Council Certified Ethical Hacker
- EC-Council Computer Hacking Forensic Investigator
- EC-Council Certified Security Analyst
- EC-Council Licensed Penetration Tester

- EC-Council Network Security Adminstrator
- EC-Council Certified Incident Handler
- EC-Council Certified Security Specialist
- EC-council Certified Disaster Recovery
- EC-Council Chief Information Security Officer
- GIAC: Global Information Assurance Certification
- GPEN: GIAC Cerfified Penetration Tester
- GWAPT: GIAC Web Application Pentration Tester
- GXPN: GIAC Exploit Researcher and Advanced Penetration Tester
- GCIH: GIAC Certified Incident Handler
- ISO/IEC 27001 Lead Auditor
- ISO/IEC 27001 Expert Implementator
- OCSP: Offensive Security Certified Professional
- OPSA: OSSTM Professional Security Analyst
- OPST: OSSTM Professional Security Tester
- OPSE: OSSTM Professional Security Expert
- OWSE: OSSTM Wireless Security Expert
- OSWP: Offensive Security Wireless Professional
- SSCP: Systems Security Certified Practitioner
- Certificaciones de SANS Institute
- Certified Ethical Hacker (CEH)
- CompTIA Cybersecurity Analyst (CySA+)
- SANS Threat Hunting and Incident Response (THIR)
- Formación en algún máster universitario (oficial o propio) en Seguridad de la Información o asimilable (ciberseguridad, seguridad informática).
- Otras Certificaciones de EC-Council, ISACA, $(ISC)^2$, CompTIA o GIAC directamente relacionadas con el objeto del pliego.

ANEJO IV

ACUERDO DE NIVEL DE SERVICIO

Implantación

Ámbito	SLA	Detalle	Valor objetivo	Medición	Criterio	Sanción
SOC	Cumplimiento de la "Fase de Implantación"	Días naturales de retraso, imputables al adjudicatario, respecto al plazo establecido para la "Fase de implantación"	0	Fin plazo Fase de implantación	- Por cada día de retraso.	200 €

- Las sanciones son acumulativas.
- Los días son laborables.

Servicio de monitorización (Alertas e informes)

SLA	Detalle	Valor objetivo		Porcentaje mínimo de cumplimiento	Medición	Criterio	Sanción
Servicio de monitorización y respuesta							
Tiempo de atención de las alertas	Tiempo máximo para atender las alertas generadas	Críticas	Atención inmediata	95%	Mensual	Por cada incumplimiento del SLA	900 €
		Muy Altas / Altas	< 4 horas	95%	Mensual	Por cada incumplimiento del SLA	500 €
		Medias	< 8 horas	90%	Mensual	Por cada incumplimiento del SLA	300 €
		Bajas	< 48 horas	90%	Mensual	Por cada incumplimiento del SLA	100 €
Tiempo de notificación de incidentes	Tiempo máximo para notificar un incidente desde su detección	Críticos	1 hora	95%	Mensual	Por cada incumplimiento	900 €

						del SLA	
		Muy Altos / Altos	4 horas	95%	Mensual	Por cada incumplimiento del SLA	500 €
		Medios	8 horas	90%	Mensual	Por cada incumplimiento del SLA	300 €
		Bajos	48 horas	90%	Mensual	Por cada incumplimiento del SLA	100 €
Tiempo de respuesta de incidentes	**Tiempo máximo para dar respuesta a un incidente desde su notificación**	Críticos	15 minutos	95%	Mensual	Por cada incumplimiento del SLA	900 €
		Muy Altos / Altos	30 minutos	95%	Mensual	Por cada incumplimiento del SLA	500 €
		Medios	2 horas	90%	Mensual	Por cada incumplimiento del SLA	300 €
		Bajos	2 horas	90%	Mensual	Por cada incumplimiento del SLA	100 €
Tiempo de propuesta de recomendación	**Tiempo máximo para proponer una recomendación para mitigación del incidente desde su detección**	Críticos	2 horas	95%	Mensual	Por cada incumplimiento del SLA	900 €
		Muy Altos / Altos	Entre 4 y 16 horas	95%	Mensual	Por cada incumplimiento del SLA	500 €
		Medios	Entre 16 y 160 horas	90%	Mensual	Por cada incumplimiento del SLA	300 €
		Bajos	Según cada caso	90%	Mensual	Por cada incumplimiento del SLA	100 €
Disponibilidad del servicio	**Disponibilidad del portal del SOC**	100%		99,99%	Mensual	Por cada incumplimiento del SLA	300

SLA	Valor de Compromiso	Porcentaje de cumplimiento mínimo	Medición	Criterio	Sanción
Entrega informe alerta crítica	<=30 minutos	95%	Cuatrimestral	- Por cada incumplimiento del SLA. - Por cada 10 minutos de retraso, sobre cada intervención.	600 € 100 €
Entrega informe alerta Muy alta o alta	<=1 hora	90%	Cuatrimestral	- Por cada incumplimiento del SLA. - Por cada 20 minutos de retraso, sobre cada intervención.	300 € 100 €
Entrega informe mensual de prestación de servicio	5 primeros días mes siguiente	95%	Cuatrimestral	- Por cada incumplimiento del SLA. - Por cada día de retraso, en cada entrega.	200 € 100 €
Diseño e implantación nuevo informe o cuadro de mandos (dashboard) en plataforma SIEM, bajo demanda (máximo 3 por mes)	10 días (tras petición)	95%	Cuatrimestral	- Por cada incumplimiento del SLA. - Por cada día de retraso, en cada entrega.	200 € 100 €

- Los días son laborables.
- Las sanciones son acumulativas.

Forense

SLA	Nivel de Severidad Incidente	Valor de Compromiso	Horario	Porcentaje de cumplimiento mínimo	Medición	Criterio	Sanción
Tiempo de respuesta para inicio en trabajos análisis forense	Crítica / Muy alta	3 horas	24x7	95%	Cuatrimestral	- Por cada incumplimiento del SLA - Por cada hora de retraso sobre el valor de compromiso en cada intervención requerida	600 € 200 €

- Se define como tiempo de “Respuesta para Inicio en trabajos de Análisis Forense” como el tiempo transcurrido desde la notificación de una petición de análisis hasta el tiempo máximo que un especialista se desplaza a las instalaciones del cliente para comenzar el trabajo forense. - Las sanciones son acumulativas.

Análisis de vulnerabilidades y Hacking Ético

SLA	Valor de Compromiso	Porcentaje de cumplimiento mínimo	Medición	Criterio	Sanción
Entrega informe de vulnerabilidades internas	5 días tras finalización de fecha de análisis programado	95%	Anual	- Por cada incumplimiento del SLA. - Por cada día de retraso, en cada entrega.	300 € 100 €
Entrega informe auditoría perimetral de vulnerabilidades	5 primeros días mes siguiente	95%	Anual	- Por cada incumplimiento del SLA. - Por cada día de retraso, en cada entrega.	300 € 100 €
Entrega informe test de seguridad (Hacking Ético)	15 días tras finalización de pruebas	100%	Anual	- Por cada incumplimiento del SLA. - Por cada día de retraso, en cada entrega.	300 € 100 €

- Los días son laborables.
- Las sanciones son acumulativas.