CONTRATACIÓN DEL SUMINISTRO E IMPLANTACIÓN DE LA NUEVA INFRAESTRUCTURA DE SEGURIDAD DE LA CCA

PLIEGO DE PRESCRIPCIONES TÉCNICAS

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	1/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

ÍNDICE

1. OBJETO DEL CONTRATO 4
2. SUMINISTRO 5
2.1 Requisitos técnicos 5
2.1.1 Infraestructura firewall de comunicaciones para la barrera de seguridad perimetral 6
2.1.2 Solución de EndPoint 10
3. CONFIGURACIÓN, INSTALACIÓN Y PUESTA EN SERVICIO 11
3.1 Asistencia técnica especializada 12
3.2 Configuración e instalación 12
3.3 Puesta en servicio, limitación temporal y ventanas de parada 13
3.4 Pruebas de aceptación 14
3.5 Explotación y mantenimiento 14
3.5.1 Plan de formación 14
3.6 Gastos de transporte 14
3.7 Recepción definitiva 15
4. GARANTÍA 16
4.1 Actualizaciones firmware y software 16
4.2 Recursos técnicos especializados 17
4.3 Reparación y sustitución de equipos 17
4.4 Gastos asociados a la reparación/sustitución 18
4.5 Revisión periódica de los servicios implementados 18
4.6 Gestión de la seguridad 18
5. CONDICIONES ESPECÍFICAS 20
5.1 Medios técnicos y materiales 20
5.2 Inventariado, etiquetado y grabado de los bienes suministrados 20
5.3 Situación actual 20
6. ACUERDOS DE NIVEL DE SERVICIO DE LA GARANTÍA 22
6.1 Condiciones de medida 22
6.2 Indicadores 23
7. MODELO DE RELACIÓN Y ORGANIZACIÓN 26
7.1 Control y seguimiento 26

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	2/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

7.1.1 Informes 26
7.1.2 Foros de gestión y dirección 26
8. CONDICIONES GENERALES 28
8.1 Cumplimiento de normativa y certificaciones 28
8.2 Confidencialidad de la información 28
8.3 Seguridad 28
8.4 Propiedad intelectual del resultado de los trabajos 29

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	3/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

1. OBJETO DEL CONTRATO

El objeto de esta contratación lo constituye el suministro, configuración, instalación, puesta en servicio y garantía de la infraestructura hardware y software de seguridad de la Cámara de Cuentas de Andalucía (en adelante, CCA), con objeto de adecuar a la Institución a los nuevos requerimientos de seguridad informática, eliminando las limitaciones de los actuales equipos por razones de obsolescencia, capacidad de proceso y ancho de banda.

La infraestructura adquirida se ubicará en el centro de procesos de datos de la CCA, sito en la calle Don Fadrique, en la ciudad de Sevilla.

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	4/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

2. SUMINISTRO

A continuación, se detallan las características técnicas mínimas de los elementos hardware y software objeto del presente contrato; las propuestas que ofrezcan características inferiores no serán tomadas en consideración. Los requisitos mínimos detallados no pretenden ser una relación exhaustiva de las características técnicas de los equipos objeto de suministro; se recogen únicamente las características relevantes.

La solución propuesta deberá ser integral e incluir los elementos necesarios para el cumplimiento de todos los condicionantes, requisitos y especificaciones técnicas descritos a lo largo del presente pliego (hardware, licencias firmware/software, dimensionamiento, cableado, consumo eléctrico, etc.).

Todos los equipos provistos por los diferentes contratistas serán de nueva fabricación, no admitiéndose equipos remanufacturados, reacondicionados o de segunda mano; el responsable del contrato podrá requerir a los adjudicatarios documentación que acredite la nueva fabricación de los equipos provistos.

Los equipos suministrados se añadirán a una configuración ya existente; el licitador debe garantizar la interoperabilidad de los elementos ofertados, que deberán integrarse plenamente con la infraestructura informática y de comunicaciones actual, no interferir ni producir malfuncionamientos, mantener todas las funcionalidades existentes y ser capaces de soportar los sistemas de información que está previsto que se implanten sobre ellos. A tal respecto, todos los elementos de conexionado, tanto eléctricos como de comunicaciones, serán suministrados por el licitador en número suficiente para que la infraestructura adquirida quede plenamente operativa en todas sus prestaciones e integrada con las redes de comunicaciones existentes, y validados por la CCA.

Toda integración, cambio, sustitución o adquisición que resulten necesarios, derivados de la no compatibilidad de los sistemas ofertados con los existentes, serán responsabilidad de la persona adjudicataria, quien deberá realizar todas las tareas oportunas para conseguir el funcionamiento total del entorno final requerido sin que esto suponga ningún coste añadido para la CCA, sin pérdida de la continuidad de los servicios que se prestan y sin perjuicio de los plazos establecidos en los pliegos de contratación.

2.1 Requisitos técnicos

El equipamiento a suministrar por la persona adjudicataria consiste en la dotación de la infraestructura hardware y software de seguridad de la CCA, a fin de cubrir los siguientes objetivos:

- Mejorar la capacidad, continuidad y disponibilidad de la infraestructura de comunicaciones con objeto de facilitar la prestación de nuevos servicios TIC de alto valor añadido con requerimientos de infraestructura de comunicaciones de muy altas prestaciones.

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	5/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

- Mejorar la seguridad de los servicios TIC mediante el incremento en la capacidad gestión e inspección de tráfico de red y la puesta en funcionamiento de nuevas funcionalidades de seguridad: funcionalidades de cortafuegos (firewall), especialmente, sus capacidades de VPN, IPS, reglas de nivel 7 con opciones de prevención de amenazas y utilizando tecnologías de última generación (NGFW).
- Mejorar la seguridad de los servidores y puestos de trabajo Windows, Linux y dispositivos móviles basados en Android: funcionalidades de EndPoint.
- Mejorar la seguridad debido a la gestión avanzada de logs, vulnerabilidades e incidentes.

Concretamente, y como equipamiento mínimo contemplado dentro de la contratación, las distintas personas licitadoras deberán suministrar:

1. Infraestructura firewall de comunicaciones para la barrera de seguridad perimetral.
2. Solución de EndPoint.

2.1.1 Infraestructura firewall de comunicaciones para la barrera de seguridad perimetral

Se requiere una solución basada en arquitectura redundante: al menos se deberán suministrar 2 equipos idénticos con capacidad para trabajar en modalidad activo/activo.

Cada equipo suministrado debe cumplir las siguientes especificaciones técnicas mínimas:

- Arquitectura, tamaño y alimentación:

  - Ubicación en rack de 19".
  - Doble fuente de alimentación con posibilidad de sustitución en caliente.
  - Hardware tolerante a fallos con arquitectura de alta disponibilidad en todos sus componentes (fuentes de alimentación, ventiladores, módulos de red, tarjetas de proceso, etc.).
  - Compatibilidad para el despliegue en distintas arquitecturas de red de alta disponibilidad (clúster) permitiendo, al menos, las configuraciones activo/activo y activo/pasivo.

- Características generales:

  - Capacidad para soportar todas las medidas de seguridad aplicadas, por cada equipo individualmente sin degradación de servicio; en caso de que se proporcionen diferentes medidas de rendimiento se tomará como válida la más restrictiva de todas.
  - Capacidad para identificar aplicaciones web/URL en base a certificados emitidos por servidores.
  - Capacidad para soportar un mínimo de 192.000 de sesiones y cursar, al menos, 13.500 nuevas sesiones por segundo.

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	6/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

- Capacidad de albergar distintos tipos de servicios de seguridad de manera combinada: firewall, soporte nativo de reglas de nivel 7, y control de aplicaciones, prevención de amenazas, sistemas de protección de intrusión (IDS/IPS) y VPNs. Debe incluirse en la propuesta todo el licenciamiento software y firmware necesario, tanto por adquisición como por suscripción cuando corresponda, para garantizar el funcionamiento de todos los requerimientos mínimos de la solución propuesta. El licenciamiento debe estar vigente durante, al menos, el periodo completo de garantía ofertado.
- Capacidad para, con todas las funcionalidades de seguridad activas (firewall y control de aplicaciones, antivirus, IPS/IDS, prevención de amenazas, antispyware y VPN), cursar un tráfico de al menos 1 Gbps.

- Prestaciones firewall y control de aplicaciones:

  - Throughput mínimo de control de aplicaciones: 2 Gbps.
  - Capacidad de crear políticas y reglas basadas en grupos/usuarios locales y remotos.
  - Integración con Microsoft Active Directory, Terminal Services y LDAP.
  - Capacidad de poder identificar usuarios desconocidos, que no forman parte del dominio, mediante portal de autenticación propio (captive portal) haciendo uso de, al menos, uno o algunos de los siguientes protocolos: Kerberos, NTLM, SAML SSO, TACACS+, RADIUS, Certificados de Cliente o autenticación local.
  - Definición local de reglas de control por aplicaciones propias y/o específicas con capacidad de definir reglas de filtrado que incluyan múltiples categorías.
  - Capacidad de limitar el ancho de banda de una aplicación, pudiendo controlar tanto el volumen de tráfico de la subida como la bajada sobre la misma regla de acceso que la aplicación.
  - Capacidad de identificar las aplicaciones, tanto si utilizan los puertos TCP/UDP estándar, como si utilizan cualesquiera otros puertos específicos.
  - Capacidad de identificación de aplicaciones que usen túneles encriptados SSL.
  - Capacidad de definir medidas de protección ante ataques de denegación de servicio que permitan restringir direcciones IP origen y/o destino o el usuario interno que pueda estar originando el ataque. Estas medidas deben poder activarse atendiendo a criterios basados en el conjunto de interfaces desde donde se origina y hacia dónde va dirigido el tráfico. Se deberá contar, al menos, con los siguientes tipos de protección: SYN Flood, UDP Flood, ICMP Flood, protección ante inundaciones por nuevas sesiones, o protección por ataques de desborde por límites de sesiones establecidas, pudiendo en cada caso establecer los umbrales necesarios para activar dichas protecciones.
  - Capacidad de descifrar tráfico SSH y detección de aplicaciones no legítimas.
  - Capacidad de realizar capturas del tráfico que atraviesa sus interfaces, de forma que se puedan establecer criterios para la captura en base a IPs, puertos, protocolos, aplicaciones.
  - Posibilidad de fijación de cuotas de navegación o QoS, por categoría.

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	7/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

- Capacidad de aplicar políticas de bloqueo de ficheros atendiendo a criterios como origen y destino del tráfico, usuarios o grupos que originan las descargas, tipo de aplicación o de tráfico que generan las descargas de fichero y para el caso de navegación en internet se puede bloquear las descargas de ficheros cuando dicha navegación sea hacia URL categorizadas como peligrosas o que puedan suponer amenazas de seguridad.
- Certificación ICSA.

- Prestaciones de prevención de amenazas:

  - Throughput mínimo: 1 Gbps.
  - Capacidad de bloqueo de amenazas conocidas, como virus, exploits, malware, spyware y vulnerabilidades reconocidas.
  - Capacidad de limitación de la transferencia no autorizada de archivos e información confidencial.
  - Habilitación de navegación segura por Internet.
  - Capacidad de identificar malware desconocido a través de una sandbox.
  - Soporte de actualización de firmas de forma desatendida, tanto de forma periódica como en modo "push".

- Prestaciones IDS/IPS:

  - Throughput mínimo: 1 Gbps.
  - Soporte de inspección basado en firmas.
  - Utilización de la identificación de aplicaciones como criterio para seleccionar los perfiles de protección de vulnerabilidades, de forma que se apliquen solo aquellas firmas específicas según la aplicación que se está utilizando.
  - Posibilidad de que las medidas de protección ante ataques de DoS, puedan ser activadas atendiendo a criterios como la zona o conjunto de interfaces desde donde se origina el tráfico, zona o conjunto de interfaces hacia dónde va dirigido el tráfico y pudiendo restringir dentro de estos interfaces las direcciones IP origen y destino a inspeccionar o el usuario interno de la red que puede estar originando el ataque.
  - Soporte de inspección de anomalías de protocolo y de tráfico.
  - Soporte de actualización de firmas de forma desatendida, tanto de forma periódica como en modo "push".

- Prestaciones VPN:

  - Capacidad para ejercer de terminador de túneles IPSec (LANtoLAN y CLIENTtoLAN), con algoritmos de encriptación e integración en LDAP para, al menos, 150 conexiones.
  - Capacidad de establecer VPN SitetoSite.
  - Throughput mínimo: 500 Mbps.

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	8/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

- Prestaciones de detección de equipos comprometidos en la red:

    - Capacidad, mediante firmas, de detectar posibles equipos comprometidos en la red que intenten establecer comunicación con servidores de comando y control, permitiendo realizar acciones predeterminadas como bloquear o monitorizar y registrar mediante logs este tipo de tráfico.
    - Capacidad de habilitar mecanismos de DNS sinkholing que permitan interceptar las peticiones de resolución de dominios realizadas desde servidores propios DNS internos a la red o hacia servidores DNS externos de forma que se identifique los equipos internos comprometidos por algún tipo de malware.

- Especificaciones de conectividad y red:

    - Redundancia: los puertos de red deben poder redundarse en modo activo/activo, a través de la especificación 802.3ad, o activo/pasivo sin el empleo del protocolo VRRP.
    - Soporte de protocolos de routing dinámico: OSPF, BGP y RIP.
    - Los interfaces del firewall deben soportar los siguientes modos de funcionamiento: modo TAP para monitorizar tráfico de forma pasiva a través de puertos mirror, modo transparente para inspección de tráfico en el flujo de datos y despliegues “in line”, modo layer 2 o switching y modo layer 3 o routing y la capacidad de usarlos todos de forma simultánea.
    - Capacidad de realizar policy based routing en base a IP o en base a red de origen, o también basado en usuarios/grupos o por tipo de aplicación.
    - Etiquetado: se debe cumplir la especificación 802.1q para el etiquetado de tráfico de hasta 4094 VLANs.
    - Soporte para la especificación 802.1x para el acceso a redes.
    - Filtro de paquetes: a través de la definición de reglas en el módulo de red, se deben poder definir acciones sobre el tráfico, para rechazar o aceptar, sin necesidad de una aplicación específica.
    - QoS: las funciones de calidad de servicio deben incluir al menos “rate-limiting” para cualquier tipo de aplicación.
    - Soporte de protocolos de routing unicast IP, RIPv2 y OSPF.
    - Soporte de protocolos de routing multicast IP, PIM-SM (IGMPv2).
    - El equipo suministrado debe tener al menos la siguiente distribución de puertos:

        - 4 puertos 10Gbps SFP+ con conector LC.
        - 4 puertos 1Gbps con conexión RJ45.
        - 1 puerto 1Gbps con conexión RJ45 para gestión y configuración.
        - 1 puerto USB 3.0.

- Especificaciones de gestión y administración:

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	9/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

- Arquitectura hardware separada para gestión y servicio, con recursos hardware dedicados independientes, que en ningún caso se compartan con el plano de datos, con el objetivo de poder garantizar que una sobrecarga del hardware destinado a prestar el servicio no afecte a la gestión y viceversa.
- Gestión vía entorno de comandos CLI (Command Line Interface): el equipo ofertado debe permitir ser configurado a través de un entorno de comandos. El acceso a dicho entorno se debe poder realizar mediante SSH.
- Gestión web: el equipo ofertado debe poderse configurar mediante un navegador web a través de acceso HTTPS.
- Capacidad para la obtención de datos estadísticos y de monitorización.
- Capacidad para ofrecer una MIB que genere traps SNMP ante eventos producidos en la plataforma.
- La solución presentada debe de ser capaz de realizar gestión de logs y generación de informes (incluso informes personalizados).
- Capacidad de analizar mensajes de *syslog* con información de *login* y *logout* para identificación de usuarios.

2.1.2 Solución de EndPoint

Se requiere una solución que cubra, al menos, 50 servidores y 165 puestos de trabajo Windows, 25 servidores Linux (basados en Debian y RHEL, y compatibles a ambas distribuciones), así como también 75 dispositivos móviles basados en Android.

La solución debe cumplir las siguientes especificaciones técnicas mínimas:

- Características generales:

  - La consola de gestión podrá estar ubicada en las instalaciones de la CCA, o en la nube del fabricante, siempre que garantice el cumplimiento de nivel alto del Esquema Nacional de Seguridad y la legislación de protección de datos aplicable. Además, todos los dispositivos incluidos en el alcance del contrato deben gestionarse desde una única consola de gestión, a excepción de los dispositivos móviles, que podrán gestionarse desde otra distinta.
  - Capacidad de protección frente a virus, malware, troyanos, gusanos, spyware y ransomware, valorándose la adaptación a las nuevas variantes que surjan.
  - Capacidad de control de aplicaciones.
  - Capacidad de protección frente a vulnerabilidades.
  - Capacidad de prevención de intrusiones.
  - Capacidad de bloqueo de comandos y controles.
  - Capacidad de control de dispositivos.
  - Capacidad de EndPoint Detection and Response (EDR).

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	10/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

3. CONFIGURACIÓN, INSTALACIÓN Y PUESTA EN SERVICIO

La persona adjudicataria será la responsable de la configuración, instalación y puesta en servicio de todos los sistemas y elementos suministrados, y de la plena operatividad de los mismos.

La persona adjudicataria deberá adaptarse a los procedimientos definidos por la CCA y se compromete a asegurar, en todo momento, la continuidad y disponibilidad de los servicios TIC impactados por la puesta en servicio del equipamiento suministrado. Para ello, deberá llevar a cabo una consultoría inicial para el análisis y diseño del plan de configuración, instalación y puesta en servicio del equipamiento suministrado en base a la situación actual de partida, a la normativa aplicable y buenas prácticas reconocidas en materia de seguridad, y a las necesidades y restricciones planteadas por la CCA, el cual deberá incluir como mínimo y a modo de referencia:

- Plan de configuración e instalación del equipamiento hardware y software suministrado, que deberá recoger, como mínimo:

    - Un estudio de las necesidades reales a nivel de negocio respecto de los niveles de protección de los activos, los roles de usuarios y los compromisos de conectividad de la CCA.
    - Un estudio de la instalación física contemplando posible movimiento y/o retirada de forma segura y garantizada del hardware existente en los racks.
    - Un estudio de las configuraciones de los sistemas que se pretenden sustituir, así como un análisis de las mismas con objeto de realizar una correcta migración.
    - La persona adjudicataria diseñará una nueva arquitectura de red teniendo en cuenta la solución tecnológica propuesta, los roles de usuarios y la naturaleza de servidores. Deberá incluir:
        - VLANs destinadas para los usuarios, las impresoras y para los servidores.
        - Configuración y bastionado de la electrónica de red de la CCA acorde a la solución tecnológica propuesta por el licitador.
    - Propuesta de configuración de la infraestructura firewall de comunicaciones:
        - Reglas: cuáles serán, tipo de nivel de las mismas, filtros adicionales que han de aplicarse, medidas de gestión de calidad de servicio, usos de traducciones de IP y puertos, etc.
        - Conectividad: configuración del terminador de túneles VPN, así como varios clientes de prueba, de la VPN SiteToSite y de enrutamiento actual.
    - Propuesta de configuración de la solución de EndPoint:
        - Configuración y niveles de protección para cada tipo de equipo y función que desarrolla.
        - Máquinas virtuales necesarias para la implantación de la solución, que actuaran de servidores, y sus características técnicas y configuraciones. Tanto el software middleware (sistema operativo, hipervisor, etc.), como el hardware necesario, será puesto a disposición por la CCA.

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	11/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

- Plan de puesta en servicio, ventanas temporales y horarias de ejecución, que además deberá recoger el plan de despliegue de los agentes de la solución de EndPoint al total de dispositivos y tipología de equipos de la CCA.
- Plan de pruebas de aceptación.
- Plan de explotación y mantenimiento, que incluirá el plan de formación.

Cada uno de los anteriores puntos se concretará en un documento entregable separado que deberá ser validado por la CCA.

3.1 Asistencia técnica especializada

La persona adjudicataria pondrá a disposición del proyecto personal técnico cualificado in-situ durante la ejecución del plan de configuración, instalación y puesta en servicio, con el objeto de llevar a cabo, entre otras, las siguientes tareas:

- Asistencia en la planificación y definición de la implantación del equipamiento suministrado.
- Información sobre posibles incompatibilidades entre elementos básicos y el equipamiento instalado o que se pretenda instalar.
- Instalación de nuevas actualizaciones del firmware y/o software de gestión del equipamiento adquirido; deberá garantizar la compatibilidad hardware y software de los nuevos elementos con el resto de los elementos existentes.
- Atención a las incidencias generadas por el conjunto de sistemas instalados, ya sea directa o indirectamente, y comprobación de que la resolución de estas incidencias se ha efectuado con el adecuado grado de optimización y con plena conformidad con las exigencias técnicas de todos los niveles funcionales coexistentes en el proyecto: equipo físico, software de base, middleware, aplicaciones y, en su caso, sistemas de información específicos afectados por la instalación.
- Asesoramiento a la CCA en materia de gestión de las comunicaciones y la seguridad de la información.
- Parametrización de la visualización de estadísticas y generación de informes.
- Integración con las herramientas de monitorización utilizadas en la CCA.
- Redacción de procedimientos relativos a la operativa de la infraestructura, definición de políticas, estadísticas, revisión de logs, etc.
- Propuesta de mejoras.

La persona adjudicataria deberá disponer de acceso a un soporte avanzado en las tecnologías implicadas por parte de los fabricantes de las mismas, de manera que se intente minimizar, como consecuencia de la aparición de imprevistos, incidencias o problemas, el posible impacto sobre los sistemas de información productivos o la propia ejecución del plan de configuración, instalación y puesta en servicio.

3.2 Configuración e instalación

La configuración e instalación del equipamiento suministrado deberá ser realizada por personal certificado por los fabricantes de los elementos incluidos en la solución propuesta, e incluirá:

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	12/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

- Desembalaje, ensamblado y montaje de todos los componentes suministrados.
- Anclaje en los chasis y armarios correspondientes, conexionado eléctrico y de red y entrega de los elementos auxiliares que corresponda para su puesta en servicio (soportes del software de base, firmware, etc.).
- Entrega de toda la documentación definida, como paso previo de las tareas de implantación.
- Instalación/actualización de firmware o cualquier microcódigo de todos los componentes hardware ofertados, en caso de que así se requiera, y de las soluciones software ofertadas. Configuración y parametrización de los sistemas para su funcionamiento básico.
- Configuración y parametrización del equipamiento hardware y software suministrado para su funcionamiento tal y como se ha definido en el plan de configuración e instalación.
- Concretamente, y relativo a la implantación de la infraestructura firewall de comunicaciones, la persona adjudicataria deberá llevar a cabo los cambios que sean precisos en la electrónica de red de la CCA para la correcta puesta en servicio de la solución propuesta. Por esta razón, el personal encargado de su implantación también deberá estar también certificado en la electrónica de red de la CCA.
- En relación con la solución de EndPoint, la persona adjudicataria deberá llevar a cabo las siguientes tareas:

    - Instalación de los servicios de la solución de EndPoint en los servidores definidos.
    - Instalación de al menos 2 agentes de la solución de EndPoint para cada tipo de equipo y función que desarrolla; el resto del plan de despliegue será ejecutado por la CCA.

3.3 Puesta en servicio, limitación temporal y ventanas de parada

Dadas las características de la infraestructura adquirida, no se permitirán ventanas de parada sobre los servicios actualmente productivos durante la puesta en servicio del equipamiento suministrado. La planificación de las intervenciones del plan de puesta en servicio y los procedimientos a llevar a cabo, conlleven o no corte de servicio, serán definidos por la CCA, debiendo la persona adjudicataria adaptarse a las ventanas diarias y horarias definidas (pudiendo tratarse de actuaciones en horario nocturno y/o fin de semana).

La persona adjudicataria garantizará que, tras la configuración, instalación y puesta en servicio de los sistemas suministrados, la disponibilidad, la continuidad, y las funcionalidades y servicios prestados por la nueva plataforma sean correctos, y que no se manifiesten incidencias o malfuncionamientos.

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	13/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

3.4 Pruebas de aceptación

Las pruebas de aceptación tendrán como fin certificar que el equipamiento hardware y software suministrado y la ejecución del plan de configuración, instalación y puesta en servicio cumplen todos los requisitos especificados. Específicamente, deberán contemplar un proceso de hacking ético, que tratará de poner a prueba la solución implantada, debiendo ser los resultados validados por la CCA.

La prueba de aceptación a realizar deberá ser acordada por todas las partes antes de comenzar la puesta en servicio, e incluirá, al menos, las validaciones de funcionamiento de todo el hardware y software suministrado. En caso de suministro e instalación de sistemas destinados a una configuración en alta disponibilidad, las pruebas de funcionamiento incluirán las pruebas de alta disponibilidad de la solución instalada.

3.5 Explotación y mantenimiento

Durante la fase de configuración, instalación y puesta en servicio del nuevo equipamiento suministrado, la persona adjudicataria facilitará el acceso a toda la información técnica que la CCA precise y se comprometerá a seguir los procedimientos establecidos en cuanto a la gestión de la configuración. Asimismo, la persona adjudicataria se encargará de elaborar y entregar todos los procedimientos de operación, configuraciones y versiones del software base y copias maestras ("imágenes") derivados de la instalación del equipamiento adquirido.

3.5.1 Plan de formación

La persona adjudicataria será responsable de la capacitación sobre los equipos y tecnologías suministradas, y deberá elaborar y llevar a cabo un plan de formación que comprenda, como mínimo:

- Capacitación sobre la infraestructura firewall de comunicaciones y la solución de EndPoint implantadas para su eficaz explotación, mantenimiento y troubleshooting, teniendo en cuenta las características de la plataforma de la CCA.
- Transferencia de información sobre la solución implantada, lo que incluirá configuraciones y parametrizaciones.

En ambos casos, el público objetivo será el Servicio de Informática de CCA.

La persona adjudicaría deberá contar con las siguientes características para la elaboración del plan de formación:

- Los formadores serán los implantadores o estarán respaldados por ellos.
- La transferencia se realizará en la sede de CCA, según calendario establecido por ella.
- Deberá contar con un mínimo de 30 horas de formación.
- El plan de formación y el material formativo deberá ser validado por CCA.

3.6 Gastos de transporte

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	14/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

Todos los gastos de transporte y seguros que conlleve el suministro serán por cuenta de la persona adjudicataria, hasta la configuración, instalación y puesta en servicio del mismo en los locales designados por la CCA.

3.7 Recepción definitiva

La recepción definitiva se realizará en la forma legalmente establecida una vez que se haya realizado el suministro de todos los elementos, sistemas o productos, y las actividades contempladas en el plan de configuración, instalación y puesta en servicio.

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	15/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

4. GARANTÍA

Durante el plazo de garantía, la persona adjudicataria será la única responsable del correcto funcionamiento de los equipos suministrados bajo una modalidad de soporte 24x7, participando del:

- Proceso de gestión de incidencias, con objeto de restaurar los servicios TIC lo más rápidamente posible ante la aparición de cualquier incidente y/o malfuncionamiento y resolver aquellas solicitudes que necesiten de una capacidad o conocimiento experto para su resolución cuando el grado de complejidad así lo requiera.
- Proceso de gestión de problemas, con objeto de gestionar las causas subyacentes de las incidencias que impacten sobre los sistemas de información de la CCA y la infraestructura técnica que los soporta. El alcance va desde que se identifica un problema, ya sea de manera proactiva o reactiva, hasta la petición de cambio a gestión de cambios que da solución al error identificado.
- Proceso de gestión de peticiones, con objeto de dar respuesta ágil y ordenada de todas las peticiones derivadas por la CCA y relacionadas con el equipamiento suministrado.

Así, la persona adjudicataria pondrá a disposición de la CCA los recursos necesarios que permitan dar respuesta, dentro de los niveles de servicio acordados, a todas aquellas incidencias y problemas que provoquen un malfuncionamiento de los equipos adquiridos, así como a todas aquellas actuaciones que pudieran resultar en aumentos de la capacidad de procesamiento y/o la mejora de la calidad del servicio.

Los servicios asociados a la garantía se prestarán preferentemente de forma remota en las dependencias de la persona adjudicataria. No obstante, dada la naturaleza de los mismos, habrá trabajos que requerirán la presencia in-situ de equipos de trabajo en las oficinas centrales de la CCA, sin que ello deba afectar a las condiciones de la oferta.

Cualquier actuación dentro del servicio de garantía deberá ser avalada y certificada por el fabricante del equipo en cuestión.

4.1 Actualizaciones firmware y software

Se entienden comprendidas las actualizaciones del firmware y software de base de todos los equipos hardware suministrados. Estará por tanto incluido todo el conjunto de programas que conforman y sirven de base a un sistema informático para su buen funcionamiento y que están estrechamente vinculados al hardware (firmware, sistema operativo y las utilidades que le son propias, consolas de gestión, etc.). De igual forma, se entienden comprendidas las actualizaciones de los productos software adquiridos.

Dentro de estas actualizaciones están incluidos no sólo el derecho de uso durante el periodo de la contratación, sino también el acceso a nuevas versiones y actualizaciones, acceso a parches para la corrección de bugs y acceso a bases de datos de conocimiento.

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	16/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

Para el caso específico de los equipos de comunicaciones, también se incluye la actualización de determinadas bases de datos especializadas, como son las bases de datos de firmas de antivirus en los equipos cortafuegos y los distintos motores de escaneo y detección.

Se exceptúan las aplicaciones hechas a medida, así como los paquetes de programas de terceros con finalidades específicas.

4.2 Recursos técnicos especializados

La persona adjudicataria deberá garantizar y asegurar la capacitación técnica de los recursos asignados a la prestación de los servicios de garantía, y deberá poner a disposición de la CCA un servicio de apoyo para la asistencia y/o consultoría de personal especializado. Atenderán las cuestiones y dudas técnicas que puedan plantearse referentes a modificaciones en la configuración de los equipos suministrados para su optimización y tunning.

Los técnicos que la persona adjudicataria disponga para realizar las asistencias “in situ” deberán acudir a las reparaciones provistos de la correspondiente acreditación y herramientas. Los perjuicios ocasionados, incluida la denegación de acceso por la ausencia de esta acreditación, sólo serán imputables a la persona adjudicataria correspondiente.

4.3 Reparación y sustitución de equipos

La persona adjudicataria deberá asegurar, bajo su responsabilidad, la provisión de cualquier clase de repuestos. En caso de reparación, el equipamiento reparado quedará en perfectas condiciones de funcionamiento, siendo éste capaz de suministrar la misma capacidad de proceso y funcionalidad que tenía antes de la incidencia o incluso superior. La persona adjudicataria será responsable de los daños que pueda ocasionar en sus acciones de reparaciones sobre los equipos u ocasionados por los componentes suministrados en dichas reparaciones, asumiendo todos los importes económicos que se deriven de sus posibles actuaciones.

Si resultase imposible la reparación de un equipo por no existir las piezas necesarias o por cualquier otra causa, o bien el coste de su reparación fuese superior al precio de mercado de un equipo nuevo de similares características, la empresa habrá de plantear soluciones alternativas, tales como préstamos, cambio de equipos, o cualquier opción para conseguir la continuidad del servicio, que siempre deberá ser aceptada explícitamente por el responsable del contrato de la CCA.

En cualquier caso, la sustitución de componentes o equipos completos averiados deberá realizarse siempre con elementos de iguales o superiores características y/o prestaciones. El equipo de sustitución deberá estar en perfecto estado de funcionamiento. Así, la persona adjudicataria será responsable de cuantas acciones de instalación básica y de apoyo a la configuración de software correspondan para la puesta en funcionamiento del equipo y de los servicios que estuviera prestando.

La persona adjudicataria deberá disponer del material adecuado para la reparación de los equipos y su continuidad.

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	17/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

4.4 Gastos asociados a la reparación/sustitución

Los gastos generados por cualquier operación exigida por la reparación o sustitución de equipos, incluido el movimiento o retirada de las máquinas, seguros, los gastos de viaje y dieta de los técnicos, o cualquier coste adicional imputable a dicha causa, serán por cuenta de la persona adjudicataria, el cual no podrá reclamar abonos adicionales por estos conceptos.

La persona adjudicataria se responsabilizará de la instalación de los sistemas y sus elementos y de la plena operatividad de los mismos.

4.5 Revisión periódica de los servicios implementados

La persona adjudicataria revisará semestralmente la configuración de los sistemas implantados, y deberá elaborar un informe que será validado por CCA donde incluya la evaluación de los cambios realizados entre periodos, indicando su adecuación a la normativa aplicable y buenas prácticas reconocidas en materia de seguridad, además de las posibles actualizaciones de firmware/microcódigos disponibles.

Este informe podrá derivar en un plan de acción, en el que la persona adjudicataria podrá colaborar para su implantación.

4.6 Gestión de la seguridad

La persona licitadora incluirá en su solución técnica una propuesta de "gestión de la seguridad", que contemplará, al menos:

- SIEM:
    - La persona adjudicataria implantará un SIEM (on promise y/o en la nube) que gestionará y transmitirá las alertas de incidencias al centro de operaciones del licitador (a continuación, SOC) o al equipo de administración de CCA, según indique esta última (que podrá variar su decisión según circunstancias durante el período de vigencia de la garantía).
    - La CCA recibirá un informe trimestral donde incluirá entre otras cosas:
        - Tiempo de detección (MTTI) y respuesta (MTTC) a incidentes de seguridad.
        - Número de incidentes abiertos en activos críticos durante ese período.
        - Cantidad de tráfico por VLAN.
        - Número de amenazas detectadas.
    - Se valorará el alcance a nivel de infraestructura de la CCA incluida en dicho SIEM, que como mínimo deberá contemplar la infraestructura hardware y software objeto de este contrato.

- Gestión de vulnerabilidades:

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	18/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

- La persona adjudicataria administrará un gestor de vulnerabilidades y transmitirá las alertas de vulnerabilidades y exposiciones detectadas al SOC o al equipo de administración de CCA, según indique esta última (que podrá variar su decisión según circunstancias durante el período de vigencia de la garantía).
- La CCA recibirá un informe trimestral donde incluirá, entre otras cosas:
    - Número de sistemas con vulnerabilidades reconocidas.
    - Número de certificados TLS/SSL configurados incorrectamente.

- SOC:

    - La persona adjudicataria deberá instalar, bajo la supervisión de la CCA, el hardware y software necesario para la gestión del SIEM, la gestión de vulnerabilidades, y demás servicios de gestión de la seguridad. Este hardware y software correrá a cargo de la persona adjudicataria, y podrán ofrecerse bajo una modalidad de servicios en la nube.
    - El licitador deberá analizar y priorizar los resultados obtenidos y dará respuesta a incidencias de seguridad, bien asesorando a la CCA, bien asumiendo la responsabilidad de su resolución. En relación a este último aspecto, a petición de la CCA, se podrá solicitar al licitador soporte técnico "ad hoc" para determinadas situaciones críticas relacionadas con la seguridad.

- La persona adjudicataria deberá colaborar con CCA para proveer de información a las diferentes herramientas de CCN-CERT que requiera utilizar.

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	19/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

5. CONDICIONES ESPECÍFICAS

5.1 Medios técnicos y materiales

La persona adjudicataria prestará los servicios relacionados con la configuración, instalación y puesta en servicio del equipamiento suministrado o la gestión de la garantía de los productos adquiridos con medios materiales propios (líneas de comunicaciones, equipos informáticos, teléfonos móviles, etc.). Todo el personal que preste estos servicios y necesite ser notificado, deberá disponer de smartphone con línea de datos activa.

La persona adjudicataria también deberá conectar sus distintas sedes a la Red Corporativa de la CCA, en caso de ser necesario para la ejecución de las prestaciones contratadas.

5.2 Inventariado, etiquetado y grabado de los bienes suministrados

Todos los bienes suministrados mediante el presente expediente requieren ser etiquetados para su inventariado por parte de la CCA; el proceso completo de etiquetado debe realizarlo la empresa suministradora, y los costes asociados a este proceso estarán incluidos dentro de los trabajos a realizar dentro de esta contratación.

La empresa suministradora deberá realizar todos los pasos indicados en el procedimiento de inventariado de bienes vigente en la CCA.

Es responsabilidad de la persona adjudicataria proporcionar la información de inventario necesaria para el correcto seguimiento de los activos de la CCA, ya sea en su fase de provisión o de garantía. Igualmente, la persona adjudicataria se comprometerá al uso de la herramienta de gestión de activos de la CCA, adecuándose a los métodos y tecnologías de recogida de información definidas por la CCA.

El soporte de dicha información será especificado por la CCA para todos los activos y sus elementos, tanto hardware como software. Asimismo, la persona adjudicataria deberá mantener actualizado dicho inventario por los mismos medios frente a los cambios debidos a sustituciones o recambios ocasionados por deficiencias detectadas con posterioridad a la entrega.

5.3 Situación actual

Por razones de seguridad, no se incluye en este pliego cierta información sobre la infraestructura actual de comunicaciones y solución de EndPoint de la CCA, que podría ser de utilidad para la elaboración de una adecuada propuesta por parte de las distintas personas licitadoras. No obstante, esta información será entregada posteriormente a la publicación de este concurso, previa solicitud y suscripción del correspondiente compromiso de confidencialidad.

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	20/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

Las personas licitadoras, y posteriormente la persona adjudicataria de este contrato, considerarán la información que el órgano de contratación les suministre durante las diferentes etapas del proceso de licitación como estrictamente confidencial y, por tanto, serán de aplicación las clausulas contempladas en el apartado 8.2 del presente pliego.

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	21/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

6. ACUERDOS DE NIVEL DE SERVICIO DE LA GARANTÍA

Como medio para garantizar la calidad de la garantía, se establecerán unos ANS y el compromiso por parte de la persona adjudicataria de cumplirlos. Estos ANS podrán evolucionar a lo largo de la ejecución del contrato con el fin de conseguir una mejora continua en la calidad del servicio efectivamente proporcionado. Los recursos, tanto humanos como de otra índole, disponibles para el servicio de garantía, deberán ser dimensionados de forma cualitativa y cuantitativa como mínimo para garantizar los ANS vigentes en cada momento.

Los ANS se basarán en la definición de unos indicadores de calidad que reflejen de forma objetiva la calidad del servicio real proporcionado, con especial atención a los aspectos más críticos del mismo, y en el establecimiento de un umbral o valor mínimo de calidad para cada uno de ellos. Se han elaborado atendiendo a los siguientes criterios:

- El establecimiento de indicadores de calidad del servicio de garantía prestado, de manera que la CCA pueda realizar una evaluación objetiva de los servicios y que la persona adjudicataria de esta licitación tenga una base para la corrección de las eventuales deficiencias en la prestación y para la mejora de sus procesos y organización.
- La automatización del seguimiento y control de los indicadores de calidad del servicio de garantía recogidos en los ANS. Los datos para la revisión de los indicadores del ANS se obtendrán de las distintas herramientas ya implantadas en el la CCA.
- La persona adjudicataria se comprometerá a realizar todas las acciones organizativas necesarias para permitir un adecuado control de todos los ANS identificados como mínimos en este pliego.

CCA, a través de su dirección técnica, podrá proponer cambios en la estructura de los ANS mínimos requeridos, que en todo caso deberán ser consensuados con la persona adjudicataria. Los cambios podrán afectar tanto a los elementos del servicio objeto de medición como a la frecuencia, la unidad de medición y el nivel de servicio.

6.1 Condiciones de medida

En el cálculo de los indicadores no se contabilizarán los tiempos que se indican a continuación:

- No contabilizarán como tiempo de indisponibilidad las paradas programadas que se realicen en las condiciones preestablecidas y acordadas.
- No se contabilizarán las demoras que estén completa y exclusivamente en el ámbito de las responsabilidades de terceros (otros proveedores externos, la propia CCA, etc.).
- Pérdidas de servicio debidas a causa de fuerza mayor (incendios, inundaciones, etc.), aunque en este caso se aplicarán los acuerdos alcanzados en el proceso de continuidad.

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	22/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

6.2 Indicadores

Para realizar el seguimiento de las prestaciones de los servicios recibidos, se establecen los siguientes indicadores del servicio.

INDICADOR	DEFINICIÓN	UNIDAD	OBJETIVO
	Porcentaje de incidencias con tiempo de resolución en plazo Según la tipología, impacto y urgencia de la incidencia, se establece una prioridad a la misma. Se calcularán los siguientes indicadores, según la prioridad asignada, del total de incidencias con tiempo de resolución en plazo entre todas las incidencias resueltas por el proveedor para la misma prioridad.		
IO_01	• **Porcentaje de incidencias con tiempo de resolución en plazo, con prioridad muy alta:** el tiempo máximo de resolución de la incidencia será de 4 horas hábiles de servicio desde la asignación de la incidencia. En estos casos, CCA podrá requerir de asesoramiento "ad hoc" por parte del licitador para su resolución.	Porcentaje	IO_01 >= 90%
IO_02	• **Porcentaje de incidencias con tiempo de resolución en plazo, con prioridad alta:** el tiempo máximo de resolución de la incidencia será de 12 horas hábiles de servicio desde la asignación de la incidencia. En estos casos, CCA podrá requerir de asesoramiento "ad hoc" por parte del licitador para su resolución.	Porcentaje	IO_02 >= 80%
IO_03	• **Porcentaje de incidencias con tiempo de resolución en plazo, con prioridad normal:** el tiempo máximo de resolución de la incidencia será de 18 horas hábiles de servicio desde la asignación de la incidencia.	Porcentaje	IO_03 >= 70%
	Tiempo medio de resolución de incidencias Según la tipología, impacto y urgencia de la incidencia, se establece una prioridad a la misma. Se calcularán los siguientes indicadores según la prioridad asignada, como la suma del tiempo de resolución de todas las incidencias entre todas las incidencias resueltas por el proveedor para la misma prioridad.		

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	23/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

INDICADOR	DEFINICIÓN	UNIDAD	OBJETIVO
IO_04	• **Tiempo medio de resolución de incidencias, con prioridad muy alta**	Horas hábiles	IO_04 <= 4
IO_05	• **Tiempo medio de resolución de incidencias, con prioridad alta**	Horas hábiles	IO_05 <= 12
IO_06	• **Tiempo medio de resolución de incidencias, con prioridad normal**	Horas hábiles	IO_06 <= 18
	Tiempo de sustitución de elemento hardware Para aquellas incidencias que requieran para su resolución definitiva de la sustitución de un elemento hardware, se establece el tiempo de sustitución de elemento hardware como el tiempo comprendido entre la asignación inicial de la incidencia y la sustitución completa del elemento hardware afectado y deberá ser reemplazado por personal técnico certificado del licitador.		
IO_07	• **Porcentaje de incidencias con tiempo de sustitución de elemento hardware en plazo**	Porcentaje	IO_07 >= 80%
IO_08	• **Tiempo medio de sustitución de elemento hardware**	Horas hábiles	IO_08 <= 24
IO_09	**Porcentaje de incidencias asignadas al adjudicatario con incumplimiento en el plazo de resolución que son reclamadas** Porcentaje de incidencias asignadas al adjudicatario que, con incumplimiento en el plazo de resolución según su prioridad, son reclamadas respecto del total de incidencias asignadas al adjudicatario.	Porcentaje	IO_09 <= 1%
IO_10	**Porcentaje de incidencias resueltas por la persona adjudicataria que son reabiertas** Porcentaje de incidencias resueltas por la persona adjudicataria que son reabiertas respecto del total de incidencias resueltas por la persona adjudicataria. Se entiende resuelta por la persona adjudicataria aquella incidencia en la que es el propio adjudicatario el que hace la propuesta de cierre de la incidencia.	Porcentaje	IO_10 <= 1%

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	24/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

INDICADOR	DEFINICIÓN	UNIDAD	OBJETIVO
	Tiempo medio de resolución de peticiones Según la tipología, impacto y urgencia de la petición, se establece una prioridad a la misma. Se calcularán los siguientes indicadores según la prioridad asignada, como la suma del tiempo de resolución de todas las peticiones entre todas las peticiones resueltas por el proveedor para la misma prioridad.		
IO_11	- **Tiempo medio de resolución de peticiones, con prioridad muy alta**	Horas hábiles	IO_11 <= 24
IO_12	- **Tiempo medio de resolución de peticiones, con prioridad alta**	Horas hábiles	IO_12 <= 48
IO_13	- **Tiempo medio de resolución de peticiones, con prioridad normal**	Horas hábiles	IO_13 <= 72

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	25/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

7. MODELO DE RELACIÓN Y ORGANIZACIÓN

El modelo de relación del contrato tiene como objetivo establecer un marco organizativo que permita cumplir los objetivos establecidos.

La CCA designará un responsable del contrato, así como los recursos humanos que estime necesarios para la supervisión, control y comprobación de la correcta prestación del suministro y servicios contratados, entre los que cabe destacar un director técnico.

La persona adjudicataria deberá especificar, al menos, un responsable del contrato, que coordinará la ejecución del mismo de acuerdo con este pliego de prescripciones técnicas.

La comunicación se establecerá principalmente entre los interlocutores nombrados por ambas partes.

7.1 Control y seguimiento

Durante el desarrollo de los trabajos, la CCA podrá establecer los controles de calidad que considere necesarios sobre la actividad desarrollada y los productos obtenidos. El seguimiento y control del servicio se efectuará mediante la presentación, por parte de la persona adjudicataria, de informes, reuniones y cuantas acciones se estimen oportunas.

7.1.1 Informes

La persona adjudicataria deberá poner a disposición de la CCA, al menos, la siguiente información:

- Informe de progreso, que recogerá el estado de los trabajos, a fecha en que se realiza. Será el resultado del análisis de los datos que proporciona el equipo de trabajo del contrato y constituye la principal fuente de información sobre los trabajos realizados y la situación de los mismos. Describe las tareas acometidas y por acometer, su grado de consecución, así como sus objetivos. Registra, asimismo, los problemas acaecidos e identifica los riesgos y oportunidades identificados en relación con el contrato. Este documento se generará a medida con la información relevante para cada uno de los foros de gestión.
- Cualquier otro tipo de informe técnico, de gestión o planificación que se solicite por la CCA durante el desarrollo del servicio.

7.1.2 Foros de gestión y dirección

Los foros de gestión y dirección constituyen el marco para la toma de decisiones compartidas con el fin de alcanzar los objetivos estratégicos establecidos para los servicios de esta contratación.

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	26/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

- Comité de seguimiento y de dirección: estará formado por el responsable del contrato, los correspondientes directores técnicos de la CCA, el responsable del contrato de la persona adjudicataria y las personas designadas por el mismo. Sus principales objetivos serán, dentro del marco de referencia en cuestión:

    - Velar por el grado de cumplimiento de los ANS y elaborar planes de acción para corregir las posibles desviaciones que se produzcan respecto a los niveles de servicio objetivo.
    - Realizar el seguimiento de los proyectos en curso y consumo de recursos del contrato.
    - Controlar el cumplimiento de las directrices estratégicas establecidas.

Todas las reuniones que se organicen durante la ejecución del contrato deberán ir acompañadas de un documento previo a su realización, orden del día de la reunión, donde se indicarán los temas a tratar en la misma. Tras la realización de la reunión, la persona adjudicataria presentará el acta de la reunión en los siete días posteriores, donde se especificarán los temas tratados, así como los acuerdos o conclusiones a las que se han llegado en la reunión.

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	27/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

8. CONDICIONES GENERALES

8.1 Cumplimiento de normativa y certificaciones

Los bienes físicos suministrados deberán ser conformes con la normativa vigente de la Unión Europea y española en lo referente a ergonomía, medio ambiente, ahorro energético, compatibilidad electromagnética, seguridad eléctrica y mecánica y reducción de la radiación emitida.

8.2 Confidencialidad de la información

La información a la que tenga acceso la persona adjudicataria como consecuencia del contrato tendrá un carácter confidencial. No podrá transferir información alguna sobre los trabajos a terceras personas o entidades sin el consentimiento expreso y por escrito de la CCA.

La persona adjudicataria, en cumplimiento de la "Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales", y 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 (Reglamento General de Protección de Datos - RGPD), únicamente tratará los datos de carácter personal a los que tenga acceso en el marco del presente contrato conforme a las instrucciones de la CCA, y no los aplicará o utilizará con un fin distinto al estipulado, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el caso de que la persona adjudicataria, o cualquiera de sus miembros, destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será responsable de las infracciones cometidas. Una vez finalizada la relación contractual, los datos de carácter personal tratados por la adjudicataria, así como el resultado del tratamiento obtenido, deberán ser destruidos o devueltos a la CCA en el momento en que ésta lo solicite.

8.3 Seguridad

Las proposiciones deberán garantizar el cumplimiento de los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información que constituyen el Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. En concreto, se deberá asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que son objeto de la presente contratación.

Para lograr esto, se aplicarán las medidas de seguridad indicadas en el anexo II del ENS, en función de los tipos de activos presentes en el sistema de información y las dimensiones de información relevantes.

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	28/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		

Deberá también tenerse en cuenta lo dispuesto en la Resolución de 8 de mayo de 2018, del Presidente de la CCA, por la que se publica el Acuerdo de Pleno, por el que se aprueban las normas que regulan la Política de Seguridad de la Información en el ámbito de la administración electrónica en la CCA.

Además, se deberá atender a las mejores prácticas sobre seguridad recogidas en las series de documentos CCN-STIC (Centro Criptológico Nacional-Seguridad de las Tecnologías de Información y Comunicaciones), disponibles en la web del CERT del Centro Criptológico Nacional (http://www.ccn-cert.cni.es/), así como a las recomendaciones de Andalucía-CERT, como centro especializado en la materia en el ámbito andaluz.

8.4 Propiedad intelectual del resultado de los trabajos

Todos los estudios y documentos, así como los productos y subproductos elaborados por el contratista como consecuencia de la ejecución del presente contrato serán propiedad de la CCA, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos. El adjudicatario renunciará expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del presente contrato pudiera corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de la CCA.

La presente cláusula no será de aplicación a los productos y herramientas preexistentes empleados para la ejecución del contrato protegidos por derechos industriales o de propiedad intelectual.

Código Seguro De Verificación	octOpSj9bAW/LAws/5VRbw==	Estado	Fecha y hora
Firmado Por	Pedro Angel Alcantara Capiscol - Jefe del Servicio de Informática	Firmado	31/05/2019 08:47:49
Observaciones		Página	29/29
Url De Verificación	https://portafirmas3.ccuentas.es/verifirma/code/octOpSj9bAW/LAws/5VRbw==		