PLIEGO DE PRESCRIPCIONES TÉCNICAS PARTICULARES PARA LA DEFINICIÓN DE UNA METODOLOGÍA DE EVALUACIÓN DE LA CIBERSEGURIDAD DE PRODUCTOS/DISEÑOS INDUSTRIALES Y ADQUISICIÓN DE EQUIPAMIENTO ADICIONAL PARA EL LABORATORIO INDUSTRIAL (EXPTE. 2021013)

I.- OBJETO Y ALCANCE DEL SERVICIO

El objeto de la presente licitación es la definición de una metodología de evaluación en materia de ciberseguridad de productos y diseños industriales, su posterior validación a través de dos pilotos en dos empresas, y la contratación del suministro, integración, puesta en marcha y soporte de equipamiento tecnológico adicional para el laboratorio de ciberseguridad industrial de la Fundación ZIUR.

El Laboratorio Industrial de la Fundación ZIUR actualmente cuenta con dispositivos de automatización y control, además de dispositivos de seguridad que pueden ser conectados dependiendo del proceso industrial que se quiera emular o mostrar en cada momento.

Tras un año de uso del laboratorio, y la realización de diferentes evaluaciones de productos industriales, se ha detectado la necesidad de contar con una metodología de evaluación reconocida internacionalmente, así como con la necesidad de adquirir equipamiento tecnológico adicional, con el fin de disponer en el mismo de los componentes, tanto hardware como software, que de forma habitual se encuentran conectados a redes industriales, lo que permite una recreación adecuada de las circunstancias y necesidades de ciberseguridad de las empresas que componen el tejido industrial de Gipuzkoa, de forma que se pueda simular con la máxima realidad una infraestructura de red industrial tipo.

II.- CONTENIDO DEL SERVICIO

II.1.- DISEÑO Y PUESTA EN PRÁCTICA DE LA METODOLOGÍA

II.1.a. - Definición de una metodología para la evaluación de ciberseguridad de un producto industrial:

El objeto que se pretende con este apartado es definir una metodología que le permita a ZIUR llevar a cabo una evaluación ligera de la ciberseguridad de un producto, cuyas principales características deberán ser:

- La aplicación de la metodología debe ser sencilla y no suponer una carga importante de trabajo, ni para ZIUR, ni para la empresa que proporciona el producto para su análisis.
- La evaluación deberá analizar tanto aspectos basados únicamente en la recolección de información, como en la realización de pruebas mediante las herramientas que ZIUR actualmente dispone en su laboratorio de ciberseguridad industrial.
- El nivel de ciberseguridad a analizar para cada producto, con el objetivo de cumplir con el requerimiento de ligereza de la metodología, será básico, por lo que la definición de los aspectos o controles de ciberseguridad a analizar deberá ir alineado a este nivel.
- Deberán definirse claramente los criterios a analizar, así como el procedimiento necesario para llevar a cabo la evaluación de cada control o aspecto analizado, de forma que los resultados de la evaluación sean predecibles y repetibles en base a los datos específicos analizados.

- La metodología debe estar basada en los estándares, regulaciones y mejores prácticas que, actualmente, tienen mayor aplicación en el entorno industrial, como por ejemplo: IEC 62443, ISO27000, NIST, Reglamento 155, etc.

Los resultados de la evaluación que se realice para cada producto se plasmarán en un "Informe de evaluación de ciberseguridad básica de producto". El contratante deberá definir una plantilla modelo de informe final resultante que reflejará, al menos, los siguientes puntos:

- Los puntos fuertes, así como, fundamentalmente, los puntos débiles en relación a la ciberseguridad del producto analizado.
- El resultado de las pruebas realizadas haciendo uso de las herramientas del laboratorio de ZIUR empleadas durante el análisis.
- El nivel de madurez global en materia de ciberseguridad de producto.
- Recomendaciones de mejoras en el diseño del producto a trasladar a la empresa industrial.

El informe no reflejará en ningún momento las acciones concretas a llevar a cabo en el caso de los puntos débiles identificados. Únicamente pondrá de manifiesto la necesidad de abordar mejoras en el ámbito analizado, de forma que los resultados sirvan a la empresa para contextualizar el nivel de partida de la ciberseguridad del producto analizado y, posteriormente, permitan encaminar los esfuerzos para mejorarla.

II.1.b.- Validación práctica de la metodología para la evaluación de ciberseguridad básica de producto.

Una vez que la metodología para la evaluación de la ciberseguridad básica de producto del apartado anterior se encuentre definida, revisada y validada por ZIUR, se llevará a cabo una experiencia piloto con el análisis de dos productos de dos empresas industriales de Gipuzkoa que permitirá alcanzar los siguientes objetivos:

- Testear de forma práctica la metodología planteada, de forma que se puedan realizar las correcciones necesarias sobre la misma.
- Formar en el uso y ejecución de la metodología al personal de ZIUR, empleando para ello esta experiencia práctica.
- Definir y planificar los trabajos con las 2 empresas que participen en la experiencia piloto, a cargo de la empresa adjudicataria.
- Ejecutar las dos experiencias piloto, que deberán desarrollarse en las instalaciones del Laboratorio de ZIUR.

II.2.- EQUIPAMIENTO DEL LABORATORIO A SUMINISTRAR

II.2.a.- Detalle del material a suministrar

El adjudicatario, para el desarrollo de la actividad objeto del contrato, deberá:

a) Suministrar el siguiente equipamiento:

- Elementos de seguridad perimetral

Tipo	Requisitos	Cantidad
Cortafuegos industrial	Dispositivo de seguridad que dispongan funcionalidades de cortafuegos en capa 4 (stateful firewall) del ámbito puramente industrial.	2 (1 unidad de dos fabricantes distintos)
NGFW	Cortafuegos NGFW, con al menos 8 puertos Gigabit Ethernet UTP y con rendimiento de al menos 550 Mb/s.	1

Con respecto a los cortafuegos de tipo industrial:

- Productos proporcionados por fabricantes específicos del ámbito industrial, con amplia implantación en la industria de Gipuzkoa.
- Formato físico adecuado para instalación en carril DIN.
- Conectividad ethernet cableada.
- Al menos 4 puertos ethernet 10/100 Mbps.
- Alimentación 24 VDC
- Se valorará que dispongan de funcionalidades adicionales para proporcionar acceso remoto.

En relación al NGFW, las principales funcionalidades requeridas son:

- Que no sea de un fabricante que ya tenga presencia en el laboratorio (Fortinet, Checkpoint, Forcepoint).
- Soporte para análisis en L7 tanto de protocolos habituales en el entorno IT como en el ámbito puramente industrial (Profinet, Modbus/TCP, etc.).
- Identificación de ataques a través del análisis de las peticiones DNS.
- Funcionalidades IDS/IPS.
- Análisis de tráfico TLS/SSL.
- Capacidades antimalware.
- Protección frente a ataques DDoS.
- URL filtering.
- Servicios de Sandbox con capacidad identificación de amenazas en el propio cortafuegos basadas en técnicas de machine learning.
- Servicios de prevención de amenazas basados en Threath Intelligence.

- Elementos de red
    - 1 Punto de acceso Wifi de tipo oficina interior, con soporte para Wifi 802.11n
    - 1 Conversor de medios de serie a Ethernet

- Pasarela y servicio IIoT

Tipo	Requisitos	Cantidad
Dispositivo hardware pasarela IIoT	Dispositivo Gateway IIoT para la captación de datos de los elementos PLC existentes en el laboratorio tecnológico	1
Servicio SaaS	Servicio en la nube que permita la ingesta de los datos obtenidos del laboratorio tecnológico mediante el dispositivo anterior, con al menos una capacidad de recopilar 50 indicadores por segundo. Incluyendo el diseño de al menos un panel de control básico.	1

Se solicitan las licencias, servicios y equipamiento necesario para disponer de una plataforma que permitan gestionar el ciclo de vida del dato relacionado con los sistemas industriales, a fin de explotarlos en una plataforma especializada con fines como mantenimiento preventivo, mejora de los procesos de producción, etc.

Se requiere que la solución cuente con certificaciones de ciberseguridad como ISO 15408 y Common Criteria, tanto en la parte de dispositivo físico para la captación de datos, los protocolos de comunicaciones empleados, así como los mecanismos de gestión de acceso a los datos centralizados en el entorno Cloud.

- Software para el despliegue de una solución para la realización de copias de seguridad y control de integridad de los programas en ejecución en los elementos del Laboratorio.

Actualmente no se dispone en el laboratorio de un software de estas características, por lo que no podemos llevar a cabo un control de cambios de configuración sobre los elementos que nos permitan, en un momento dado, recuperar de una manera fácil y automatizada la configuración del Laboratorio a un punto concreto. Permitiéndonos así recuperar la funcionalidad del Laboratorio ante una situación de desastre.

Tipo	Requisitos	Cantidad
Software para copias de seguridad y control de integridad de los programas en PLCs	Software que permita la realización automática de copias de seguridad, así como la realización de chequeos periódicos de la integridad de los programas en ejecución de los siguientes elementos industriales: PLC Schneider M340, PLC OMRON NX1P, PLC Siemens 1512SP	1

Los requerimientos del software son los siguientes:

- El software debe basarse en el despliegue de una arquitectura basada en un servidor principal, agentes y clientes, sin necesidad de instalación de bases de datos externas.
- Debe permitir la comparativa detallada del código del proyecto para todo tipo de componentes, como PLCs, HMIS, Scadas, Robots, Documentos office, Eplan, Pdfs, Binarios, ASCII, etc.
- Debe disponer de funcionalidades para la obtención de detalles de los cambios detectados en proyectos de TIA Portal Step7, TIA Portal WinCC, Simatic S7, WinCC Flexible, Simatic WinCC, RSLogix 5, 500 y 5000, Studio 5000, Omron Cx-Programmer, TwinCAT, Scalance, AVEVA Wonderware, Sinumerik 840D, Unity, PL7, … Incluyendo en la comparación la estructura del proyecto y visualización gráfica de las diferencias.
- Las tareas periódicas programadas para la realización de copias de seguridad deben poder ser ejecutadas desde el propio servidor o mediante agentes instalados en otros equipos.
- Las tareas de copias se deben poder activar mediante el envío de datos por OPC UA.
- Las tareas dedicadas a la verificación de la versión en ejecución en un elemento industrial deben tener la capacidad del envío de alertas a un SIEM.
- Los clientes del software deben poder ser ejecutados como versión portátil, sin necesidad de proceder con la instalación de los mismos en los puestos.

- Software para el control de acceso a la red (NAC)

Tipo	Requisitos	Cantidad
Software NAC	Solución software que permita el despliegue de una solución de control de acceso a la red, con licencias para, al menos, 100 dispositivos.	1

El software NAC deberá proporcionar las siguientes funcionalidades:

Compatibilidad:

- El Sistema debe poseer de mecanismos de perfilado de perfilado de dispositivos. Para el perfilado se deberán usar al menos los siguientes mecanismos:
- La solución debe contar con firmas de profiling incorporadas. En cualquier caso, se podrán realizar actualizaciones de las mismas en función de los dispositivos que se conecten.
  - Activos: NMAP, WMI, SSH, SNMP
  - Pasivos: MAC-OUI, DHCP, TCP, Netflow v5/v10, IPFIX, sFlow, Span Port, HTTP User-Agent, IF-MAP
  - Otros: Agente Posture, integración con soluciones MDM, certificados.
- La solución debe contar con firmas de profiling incorporadas. En cualquier caso, se podrán realizar actualizaciones de las mismas en función de los dispositivos que se conecten.
- El sistema detectará automáticamente posibles conflictos en el perfilado y marcará los Endpoints si detecta incongruencias.
- El sistema deberá utilizar protocolos estándar que garanticen su compatibilidad con distintos equipos de acceso (switches, routers, firewalls, controladores WLAN, terminadores VPN) de distintos fabricantes.
- El sistema deberá realizar descubrimiento y perfilado de dispositivos sin necesidad de sondas o equipos adicionales en sedes remotas.

- El sistema debe poderse integrar en más de un dominio corporativo para realizar consultas en el Directorio Activo.
- Se deberán soportar integraciones con sistemas de entidades externas:
  - Microsoft Active Directory
  - RADIUS
  - Directorios LDAP
  - MySQL, Microsoft SQL, PostGRES y Oracle 11g ODBC-compliant SQL server
  - Servidores de Token
  - Kerberos
  - Microsoft Azure Active Directory
  - Google G Suite
  - Built-in SQL Store, static host-list
- Soporte de autenticaciones mediante 802.1X, autenticación MAC y con portal cautivo.
- Soporte de autenticación basado con SNMP con switches que no soporten protocolos RADIUS.
- Se deberán poder realizar simulaciones de políticas de seguridad antes de su implantación.
- Soporte de servicios AAA (Authentication, Authorization and Accounting) con los métodos de autenticación más utilizados en la industria:
  - RADIUS, RADIUS CoA, TACACS+, Web authentication, and SAML v2.0
  - EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
  - PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public)
  - TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP)
  - EAP-TLS
  - EAP-TEAP (Tunneled EAP)
  - PAP, CHAP, MSCHAPv1, MSCHAPv2, and EAP-MD5
  - Wireless and wired 802.1X and VPN
  - OAuth2
  - Microsoft NAP and NAC
  - Windows machine authentication
  - Online Certificate Status Protocol (OCSP)
  - SNMP generic MIB, SNMP private MIB
  - Common Event Format (CEF), Log Event Extended Format (LEEF)
- Posibilidad de separar los procesos de Autenticación y Autorización – cada proceso deberá poder utilizar bases de datos distintas.
- Se deberá soportar RadSec para comunicación segura entre el RADIUS y los NAS.
- Se deberá soportar el envío de CoA (Change of Authentication) mediante atributos RADIUS estándar a equipos Wired y Wireless. No será necesario proporcionar credenciales de administración para ejecutar el CoA.
- El sistema tendrá funcionalidades de Autorización del acceso en función de características como pertenencia a un grupo de usuarios, tipo de dispositivo móvil, aplicación utilizada, localización del dispositivo, estado de salud (Health Check) del dispositivo, etc…
- Se soportará la definición de hasta 5 servidores NTP version 4.
- El sistema implementará los siguientes estándares RFC
  - RFC 2246 The TLS Protocol Version 1.0
  - RFC 2248 Network Services Monitoring MIB
  - RFC2548 Microsoft Vendor-specific RADIUS Attributes

  - RFC 2759 Microsoft PPP CHAP Extensions, Version 2
  - RFC 2865 Remote Authentication Dial In User Service (RADIUS)
  - RFC 2866 RADIUS Accounting
  - RFC 2869 RADIUS Extensions
  - RFC 2882 Network Access Servers Requirements: Extended RADIUS Practices
  - RFC 3579 RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)
  - RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines
  - RFC 3748 Extensible Authentication Protocol (EAP)
  - RFC 4017 Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs
  - RFC 4137 State Machines for Extensible Authentication Protocol (EAP) Peer and Authenticator
  - RFC 4849 RADIUS Filter Rule Attribute
  - RFC 5216 The EAP-TLS Authentication Protocol
- El sistema soportará la gestión automática de claves de acceso para que puedan controlar el acceso de dispositivos mediante SSID con WPA2 y claves pre-compartidas (PSK) diferentes (MPSK). Esta funcionalidad podrá estar destinada a dispositivos IoT que acceden por un mismo SSID pero que no disponen de suplicante 802.1X y requieren un acceso controlado.
- Se soportará TACACS+ y control de acceso a equipos mediante comandos específicos que se podrán limitar tanto para denegarlos o permitirlos. Se soportará el uso de comandos wildcard (.*) para definir por ejemplo ACLs.
- El sistema será capaz de generar mensajes de Syslog para terceros.
- Los mensajes de Syslog podrán filtrarse en función de diferentes tipos de eventos y a servidores diferentes.
- El sistema soporta mensajes de Syslog en los siguientes formatos: Standard, LEEF, CEF y RFC5424.
- El sistema soportará la configuración del usando direccionamiento IPv6. Se podrá configurar sólo IPv4, solo IPv6 o Dual-Stack.
- Se deberá soportar IPv6 entre el servidor y los equipos autenticadores (NAD).
- Se soportará el uso de TACACS+ sobre IPv6.
- Para el acceso de invitados se soportarán redes en IPv6, incluyendo los siguientes flujos (auto-registro, web-login, OnBoard, Social-Logins).
- Se soportará la creación de Clusters del sistema basado en redes con IPv6.
- El sistema permitirá configurar el uso que se le dará a cada certificado, de tal forma que se podrá seleccionar entre diferentes usos: Servidores AD/LDAP, Database, EAP, Servidores de Contexto Externo, RadSec, SAML, SMTP, Otros asegurando así el propósito de dicho certificado.

Acceso de invitados con portales cautivos de acceso:

- Se podrá realizar el registro de dispositivos mediante portales cautivos, orientado a Guest, soluciones BYOD y gestión de dispositivos.

- El sistema incluirá la posibilidad de generar diferentes portales cautivos para la autenticación de invitados compatible con las soluciones WLAN más habituales de los distintos fabricantes de la industria.
- El portal cautivo incluirá funcionalidades avanzadas de auto-registro, mediante las cuales el invitado podrá generar su propia cuenta de invitado sin comprometer la seguridad de la red.
- El portal proporcionará diversos métodos para la entrega de credenciales de invitado: email, SMS, impresión de tickets.
- El portal proporcionará métodos avanzados de aprobación de la visita por parte de la persona que recibe al invitado que permitan autorizar la visita de manera flexible y sin intervención de personal de IT.
- El tiempo de expiración de las cuentas de invitados deberá ser configurable.
- Los portales cautivos permitirán personalizar el look&feel de forma completa, con posibilidad de adaptación del código HTML completo y de las hojas de estilo CSS.
- Los formularios de acceso de invitados podrán personalizarse en todos sus campos con al menos las siguientes capacidades mínimas:
    - Inclusión en el portal de menús desplegables que permitan registrar información relativa al invitado (motivo de la visita, duración de la misma, persona a la que visita, y cualquier opción adicional. El contenido de estos campos será personalizable.
    - Generación de portales HTML de distinto tamaño en función del tamaño y resolución de las pantallas de los dispositivos móviles. El portal deberá redimensionarse automáticamente en función del dispositivo que lo visualiza.
    - Posibilidad de incluir todo de tipo de contenido multimedia en el portal: imágenes, audio, video, etc… que varíe de forma dinámica según patrones establecidos. Este contenido podrá referenciarse a enlaces externos o podrá ser incluido en el propio Sistema. No existirá limitación de imágenes o contenidos que se podrán incluir.
- El portal proporcionará informes de actividad relativa al tráfico de invitados: número de visitas, contenido multimedia mostrado, numero de SMS enviados con credenciales, etc…
- El portal permitirá integrarse con soluciones de doble factor de autenticación.
- Se podrán realizar integraciones con sistemas de terceros mediante OpenAuth para permitir a los usuarios invitados validarse con sus credenciales en las redes sociales más utilizadas en España, según el último estudio publicado por el observatorio nacional de las telecomunicaciones y la SI (ONTSI).
- Los portales de acceso permitirán integración con redes sociales como Facebook, Facebook WiFi, Google Plus, Twitter, Instagram, LinkedIn, etc.

Health-Check:

- La solución NAC deberá incorporar mecanismos para realizar el control de salud de los dispositivos que se conecten a la red.
- Se deberán soportar agentes pesados (que requieren instalación) y agentes solubles (agentes que se ejecutan sin quedar permanentes en los endpoints).
- Se soportará health-check mediante funcionalidad “agentless” donde no se requiera la instalación de un agente para entornos Windows.
- La solución deberá proporcionar un workflow sencillo para que los usuarios puedan puedan provisionarse cualquiera de los dos agentes. La provisión se realizará mediante portales cautivos configurables.

- El chequeo de salud deberá permitirse para los sistemas operativos mediante agente: Windows, Linux y MacOS.
- El agente de Linux soluble estará soportado en CentOS, Fedora, RHEL y SUSE.
- Este agente comprobará el estado y actualización de anti-virus, anti-spyware, firewalls, etc…y proporcionará instrucciones de remediación en caso de que el dispositivo viole las políticas corporativas.
- La información de estado proporcionada por el agente deberá de poder ser consultada en tiempo real.
- El agente tendrá la capacidad de detener o arrancar procesos internos de los dispositivos en caso de ser necesario.
- El agente tendrá acceso a las variables de registro de los dispositivos y podrá agregar o eliminar variables en caso de ser necesario.
- Se valorará que el agente ligero NAC realice comprobaciones avanzadas como detección de programas P2P y utilización de llaves USBs como dispositivos de almacenamiento.
- En caso de dispositivos corporativos se soportará el control del health-check mediante WMI sin necesidad de agente.
- Se soportará la ejecución de scripts personalizados a través del agente para recolectar información adicional a través de dichos scripts.
- Se podrán ejecutar script personalizados para realizar remediación a través del agente.

Gestión de dispositivos Móviles:

- El sistema proporcionará una infraestructura PKI interna que permita generar credenciales específicas de para dispositivos móviles que sirvan para autorizar estos dispositivos en la red (certificados digitales).
- La PKI interna permitirá configurarse como Root-CA, Intermediate-CA, Imported-CA o Registration Authority.
- Debe ser compatible con los dispositivos más habituales: iOS (Apple iPad, iPhone), Android, MacOS X, Windows Mobile, Windows 7.
- Las credenciales utilizadas para los dispositivos móviles permitirán controlar el acceso de estos dispositivos a la red y denegarlo en caso de robo o pérdida del dispositivo.
- Se valorará la capacidad del sistema para configurar de manera automática el suplicante 802.1X de los dispositivos móviles.
- Se valorará la capacidad del sistema para configurar de manera automática los parámetros de uso habituales en el entorno de trabajo: servidor de correo, cliente VPN, etc…
- El sistema proporcionará estadísticas de uso e inventario de los dispositivos móviles.
- Se valorará que la generación y entrega de credenciales para dispositivos móviles suponga una carga de trabajo mínima para el departamento de IT.
- Se valorará que cualquier empleado pueda realizar el proceso de autenticación y autorización de dispositivos móviles sin necesidad de ayuda del departamento de IT.
- Se valorará el empleo de más de un método de detección e identificación de los dispositivos móviles, para evitar la suplantación de identidades (Device Profiling).
- El sistema tendrá la capacidad de utilizar las credenciales de autenticación de red (802.1X) para autenticar también las sesiones de las aplicaciones móviles.
- Los certificados emitidos podrán ser gestionados por un administrador y filtrados por usuario y dispositivos para su revisión, eliminación o revocación.

- Los usuarios podrán disponer de un acceso seguro para conocer los dispositivos que tienen asociados un certificado y revocar/eliminarlos de forma personalizada. Este acceso será configurable y opcional para los usuarios.
- Se podrá limitar el número de dispositivos que pueden disponer de certificado para cada usuario corporativo.
- La solución permitirá sobrescribir los campos Subjet y/o Subject Alternative Name (SAN) en un CSR enviado de forma manual para mantener estándar de seguridad.

Integraciones:

- Se podrán realizar integraciones con terceros. El sistema debe contar con posibilidad de dichas integraciones de manera flexible sin intervención del Fabricante.
- Se podrá configurar integraciones con terceros mediante consultas http/https para el intercambio de información.
- Integración con la solución GUARDIAN de Nozomi Networks, presente actualmente en el laboratorio de ZIUR
- El sistema deberá poder exportar a sistemas de terceros información contextual de los usuarios autenticados: username, dispositivo usado, estado del posture, punto de conexión, etc.
- Se deberá contar con integraciones con CheckPoint para compartir información contextual de los usuarios: información de Accounting y login/logout de usuarios.
- El sistema soportará la recepción de eventos vía Syslog para ejecutar acciones sobre la infraestructura de acceso, desconectando usuarios o cambiándoles de VLANs.
- Se deberá soportar la integración con sistemas MDM para recibir información sobre los dispositivos enrolados en dichas plataformas. Se deberá poder comprobar esta información para crear una política de acceso personalizada.
- Se podrá definir cada cuanto tiempo hacer el pulling de datos de las plataformas MDM y además la hora de inicio.

Otros:

- La solución NAC debe contar con las siguientes certificaciones de Seguridad:
  - FIPS 140-2
  - Extended Package for Authentication Servers Version 1.
  - Collaborative Protection Profile for Network Devices Version 1.0
- El sistema debe contar con un sistema de reporting integrado para generar informes programados y bajo demanda sobre la red, usuarios, dispositivos y autenticaciones.
  - Los informes podrán ser personalizados en cuanto a la fecha y al contenido de los mismos.
  - Se deberán poder hacer informes bajo demanda de autenticaciones satisfactorias y fallidas en periodos de tiempo limitados.
  - Se admitirán filtros en los informes para establecer resultados en función de cualquier atributo RADIUS: NAS, fuente de autenticación, status, etc.
  - Se deberán poder generar dos tipos de informes:
    - Informe PDF de alto nivel con información básica y agregada mediante gráficas.
    - Informe con los datos en bruto en formato CSV con los campos personalizables.

- Los informes podrán generar notificaciones a direcciones de correo electrónico o mediante SMS.

- Sistema de virtualización y de copias de seguridad para el despliegue del software detallado en los dos puntos anteriores.

Tipo	Requisitos	Cantidad
Host y software de virtualización	Servidor para virtualización con las siguientes características: • 32 GB RAM • 4 puertos Gigabit Ethernet • Dos discos 480 GB SSD • Fuente de alimentación redundante • Licencia VMware vSphere	1
Sistema NAS	Sistema de copias de seguridad para el anterior sistema de virtualización compuesto por: • Una unidad NAS con, al menos, 6 Tb netos. • Software de virtualización Veeam Backup.	1

- Software de acceso remoto

Tipo	Requisitos	Cantidad
Licencia TeamViewer	Licencia Teamviewer	1
Licencia AnyDesk	Licencia AnyDesk	1

Todas las referencias al suministro de la instalación contemplan todos aquellos materiales necesarios para garantizar la puesta en marcha y el buen funcionamiento de los equipos, como –a modo enunciativo, pero no limitativo- el cableado, conectores, elementos de instalación, etc., debiendo la empresa contratista suministrar cuanto sea necesario sin que ello suponga coste adicional para ZIUR.

Así mismo el precio del contrato incluye una partida a tanto alzado para servicios de albañilería, conexiones eléctricas, etc., debiendo la empresa contratista contratar los mismos sin que ello suponga coste adicional para ZIUR.

La empresa adjudicataria vendrá obligada a entregar a la Fundación copia de todos los productos y materiales que se realicen durante la ejecución del contrato en los soportes y formatos que se señalen por la propia Fundación, debiendo ser los materiales que se presenten directamente editables y susceptibles de adaptación y explotación por parte de la Fundación.

En aplicación de lo dispuesto en el artículo 308.1 de la Ley 9/2017 de Contratos del Sector Público, los derechos de propiedad intelectual y/o industrial que se puedan derivar del trabajo contratado serán cedidos a la Fundación ZIUR. Dicha cesión se realiza con carácter exclusivo, sobre cualquier derecho de explotación y modalidad (presente y futura) de explotación de estos, con la facultad de otorgar

autorizaciones exclusivas y transmitir los derechos a terceros, por todo el tiempo, territorio, ámbito y alcance permitido por la legislación aplicable. En caso de incluir contenidos, elementos o materiales de terceros, la empresa adjudicataria se asegurará de ceder a la Fundación el uso y explotación pacífica de los mismos, en los mismos términos que los derechos de propiedad intelectual y/o industrial que se puedan derivar del trabajo contratado anteriormente referidos.

II.2.b) Normas comunes a los materiales a suministrar.

Todos los sistemas, componentes y productos a adjudicar en este contrato deberán ser conformes con la normativa vigente de la Unión Europea y española en lo referente a sus aspectos de calidad, ergonómicos, medioambientales, de ahorro energético, de compatibilidad electromagnética y de seguridad. En particular, deberán cumplir los siguientes apartados:

- **Disposiciones de obligado cumplimiento:**

Cuando los sistemas, sus componentes o productos estén sujetos a cumplimiento de requisitos técnicos establecidos en Reglamentos, Directivas o en otras disposiciones normativas de obligado cumplimiento, tanto en el ámbito europeo como el nacional, el suministrador será responsable del cumplimiento de los mismos.

- **Marcado CE:**

Los productos que se suministren para el contrato serán conformes con la Decisión 768/2008/CE del Parlamento Europeo y del Consejo de fecha 9 de julio de 2008, incluyendo en su caso el marcado CE correspondiente, acreditando por tanto la conformidad con los requisitos esenciales que le son aplicables para su comercialización en la Unión Europea, tales como:

- 2014/35/EU (Directiva de Baja Tensión, LV Directive)
- 2014/30/EU (Directiva de Compatibilidad Electromagnética, EMC Directive)
- 2011/65/EU (Directiva de restricción de ciertas sustancias peligrosas, RoHS Directive)
- 2012/19/EU (Directiva RAEE de residuos de aparatos eléctricos y electrónicos, WEEE Directive)

- **Seguridad general de los productos. Funcionalidades de seguridad:**

Los productos que se adjudiquen para los contratos basados se ajustarán a la directiva 2001/95/CE relativa a la seguridad general de los productos (R.D. 1801/2003, de 26 de diciembre, sobre seguridad general de los productos B.O.E. de 10 de enero de 2004).

- **Características y gestión medioambientales:**

En materia de restricciones a la utilización de determinadas sustancias peligrosas y sobre la gestión de los residuos de los productos eléctricos y electrónicos ofertados en el presente contrato, serán de aplicación la Ley 22/2011, de 28 de julio, de residuos y suelos contaminados, el Real Decreto 219/2013, de 22 de marzo, sobre restricciones a la utilización de determinadas sustancias peligrosas en aparatos eléctricos y

electrónicos, y el Real Decreto 110/2015, de 20 de febrero, sobre residuos de aparatos eléctricos y electrónicos.

De conformidad al artículo 202 LCSP, se establece la condición especial de ejecución de carácter medioambiental consistente en la obligatoriedad de acreditar ante el órgano de contratación la adecuada gestión de los residuos de conformidad a la normativa vigente en la materia:

- Se llevará un control documental y registral sobre la cantidad y tipo de residuo que se entregará al gestor.
- Los residuos a entregar al gestor deberán estar debidamente separados.
- Se entregará al gestor los residuos generados y se tramitará el proceso necesario de tratamiento de los mismos
- Se justificará documentalmente la entrega de los residuos al gestor.

- **Compatibilidad electromagnética:**

Todos los sistemas, sus componentes y productos a adjudicar en los contratos basados en este contrato cumplirán los requisitos de protección establecidos en la Directiva 2014/30/UE, de 26 de febrero de 2014, sobre la armonización de las legislaciones de los Estados miembros en materia de compatibilidad electromagnética y en el Real Decreto 186/2016, de 6 de mayo de 2016, por el que se regula la compatibilidad electromagnética de los equipos eléctricos y electrónicos.

- **Accesibilidad universal y diseño para todas las personas:**

De acuerdo con lo previsto en el artículo 126 y DA 18 de la LCSP, se deberán tener en consideración en este contrato todos los elementos que faciliten el uso de los productos ofertados por personas con discapacidad.

- **Acreditación de la normativa, certificados y muestras de los productos:**

Durante la licitación y la vigencia del contrato, los certificados o documentos acreditativos del cumplimiento de las normas aplicables o, en su caso, de los requisitos en ellas establecidas, estarán a disposición de la Fundación ZIUR, así como de los organismos peticionarios.

- **Entrega, instalación y configuración:**

Salvo indicación en contra en el documento de licitación, el precio final ofertado incluirá la entrega de los productos (equipos hardware y/o código software) en las instalaciones de ZIUR, el desembalaje y reciclaje del embalaje correspondiente, la instalación y configuración básica del mismo, documentación técnica, así como las pruebas necesarias para comprobar su correcto funcionamiento.

Los trabajos de puesta en marcha contemplarán todo lo necesario para dejar operativo el laboratorio completo con al menos uno de los diseños propuestos en la oferta validados por ZIUR.

Así mismo, se considerará la puesta en marcha finalizada una vez:

- Se entregue toda la documentación de detalle del equipamiento instalado, su configuración, mapas de arquitectura, mapas de conexionado y documentación de cada elemento, como mínimo.
- Se forme al personal de ZIUR sobre la instalación y configuración realizada, así como todos aquellos aspectos que sean necesarios para poder explotar toda la funcionalidad de dicho Laboratorio.

- **Régimen de garantía del contrato:**

Los equipos se recepcionarán a los 30 días de su suministro, durante ese periodo, cualquier fallo del equipo se solucionará cambiándolo por otro completamente nuevo. A todos los efectos, un cambio de esta naturaleza constará como un único suministro y todos los costes asociados correrán a cargo de la empresa adjudicataria.

El periodo de garantía empezará a contar 30 días después desde el momento en que la Fundación ZIUR dé por finalizada la puesta en marcha de la instalación.

La empresa adjudicataria será responsable de la garantía del material suministrado, debiendo garantizar el correcto funcionamiento de todos los productos suministrados –equipos hardware y software, periféricos, etc.- por un plazo mínimo de garantía de DOS (2) años a contar desde la fecha de la puesta en marcha de la instalación, salvo que en su oferta indique otro superior.

Todas las reparaciones deberán realizarse “in situ”, en el lugar en el que se encuentre el producto en el momento de notificarse la avería. En caso de que no pudiera realizarse la reparación in situ, los gastos de embalaje y traslado del equipo averiado serán de cuenta de la empresa contratista. A petición de la Fundación ZIUR, la subsanación de errores de funcionamiento del software podrá realizarse en remoto, a través de las correspondientes conexiones telemáticas previamente autorizadas.

En cuanto al tiempo máximo de reparación de la avería, desde la comunicación de la incidencia y hasta la resolución de la misma, será el siguiente, dependiendo de la criticidad de la incidencia:

1. Crítica: Máxima severidad, supone la no disponibilidad del equipamiento. Tiempo máximo de respuesta: 24 horas.

2. Grave: Severidad media, supone la no disponibilidad parcial del equipo o una degradación del servicio que impide su normal funcionamiento. Tiempo máximo de respuesta: 48 horas.

3. Leve: Severidad baja, otro tipo de incidencias que no impiden el normal funcionamiento del equipo pero que requiere de alguna acción correctora. Tiempo máximo de respuesta: 96 horas.

En caso de no lograr la reparación en ese plazo deberá procederse a la entrega de un producto análogo de sustitución hasta la completa reparación. Los gastos de la entrega de este equipo de sustitución, incluidos embalaje, transporte e instalación correrán a cargo de la empresa adjudicataria.

En todo caso, será obligatoria la sustitución definitiva de los equipos por otros de iguales o superiores características en el caso de haber realizado tres reparaciones sobre el mismo producto, siempre que lo solicite la Fundación ZIUR.

La empresa adjudicataria deberá tener disponible un correo electrónico para la comunicación de averías o incidencias. El horario del servicio de atención a estas comunicaciones será, como mínimo, de 8h a 18h de lunes a viernes.

Otras características de la garantía serán:

- Cubrirá cualquier defecto, disfunción o avería, y cualquier instalación o configuración realizada incorrectamente.
- En el caso de necesitarse una sustitución de piezas, las nuevas piezas serán iguales o mejores en cuanto a calidad y cualidad que las sustituidas.
- En el caso particular de que la pieza a sustituir sea una unidad de almacenamiento fija (hdd, ssd) la Fundación ZIUR NUNCA entregará la unidad estropeada NI PERMITIRÁ que dicha unidad quede fuera de su custodia. La Fundación ZIUR determinará las excepciones.
- En todos los casos donde sea necesario el envío del producto estropeado a un centro de reparación, los gastos de logística (empaquetado, recogida, envío y retorno) correrán a cargo de la empresa adjudicataria.
- El etiquetado e identificación del producto forma parte de la garantía. Por lo tanto, cualquier deterioro deberá ser subsanado por la empresa adjudicataria.

- **Soporte y/o mantenimiento de los equipos y licencias de software:**

Los trabajos de soporte deberán contemplar al menos los siguientes aspectos durante el plazo de 3 años.

- Soporte de fabricante, actualizaciones de versiones y posibles suscripciones.
- Plan de mantenimiento preventivo y correctivo, actualización SW y suscripciones.

Conjuntamente con la adquisición de equipamientos hardware o conjuntamente con la adquisición de licencias, se incluye en la licitación el mantenimiento y/o soporte que les sean de aplicación.

La duración del mantenimiento y/o soporte será de 3 años, estando contemplado en el precio del contrato, a pesar de lo cual dicho importe deberá ser desglosado en la oferta.

El mantenimiento y soporte tendrán por objetivo realizar las actuaciones necesarias para minimizar los tiempos de no disponibilidad de los productos y maximizar su rendimiento. Se incluirán tareas tales como el diagnóstico y resolución de incidencias, soporte remoto, soporte in situ, piezas de repuesto, actualizaciones de versiones de software y firmware, gestión de suscripciones, análisis de alertas y logs, gestión de licencias, aplicación de parches de software o acceso a información técnica.

II.3.- SERVICIOS

La propuesta debe incluir la prestación de servicios profesionales, por parte del adjudicatario, para llevar a cabo las siguientes tareas:

- Definición en detalle de la metodología diseñada
- Validación práctica de la metodología, implantándola para dos productos industriales de dos empresas industriales de Gipuzkoa
- Generación de un Informe de evaluación de ciberseguridad básica de producto, en castellano y en Euskera, para cada uno de las dos implantaciones anteriores
- Formar en el uso y ejecución de la metodología al personal de ZIUR, empleando para ello la experiencia práctica en las dos empresas
- Puesta en marcha y configuración, en el laboratorio de ZIUR, de todos los elementos contemplados en el apartado III.2
- Formar al personal de ZIUR en el uso de los elementos contemplados en la propuesta.
- Mantenimiento a 3 años
- Elaborar documentación detallada de los trabajos llevados a cabo

III.- MEDIOS HUMANOS Y TÉCNICOS:

Para la realización adecuada del trabajo descrito, la empresa adjudicataria deberá contar en el equipo del proyecto con las capacidades y conocimientos suficientes para la realización de los trabajos en tiempo y forma, de acuerdo con lo establecido en los Pliegos de Cláusulas Administrativas Particulares.

En primer lugar, y en lo que respecta a las figuras de Dirección del Proyecto y Jefatura de Proyecto, nos remitimos a lo establecido en el apartado 15 de los Pliegos de Cláusulas Administrativas Particulares, en lo referido al compromiso de adscripción de medios personales.

En segundo lugar, se enumeran a modo de referencia los roles y/o capacidades técnicas que se consideran necesarias, además de las previstas en el párrafo anterior, tanto para la correcta ejecución y seguimiento del proyecto, como para el desarrollo del mismo. Se deja a criterio de las empresas licitadoras el detalle concreto del equipo que se considere oportuno para el proyecto, que es susceptible de evaluación mediante juicio de valor de acuerdo con lo establecido en los Pliegos de Cláusulas Administrativas Particulares (apartado 18.1), debiendo incluir la experiencia del equipo del proyecto en trabajos similares, y el organigrama y descripción del equipo de trabajo.

- **Experiencia en proyecto de seguridad industrial**
  Implementación y configuración de medidas de seguridad en entornos industriales

- **Experiencia en integración de sistemas**
  Implementación y configuración de las distintas soluciones y servicios necesarios para el funcionamiento del Laboratorio

- **Consultoría y/o auditoría de ciberseguridad**

Se encargará del desarrollo y definición de la metodología para la evaluación de ciberseguridad básica de producto; para tal fin debe disponer de experiencia en proyectos de consultoría y aplicación de las normativas sobre las que se base la metodología.

Todas las personas que intervengan en la realización de los trabajos deberán estar capacitadas para desarrollar los trabajos, actuarán bajo la organización de la empresa adjudicataria y deberán contar con experiencia acreditada en las labores en las que vayan a participar.

Todos los documentos y actividades se realizarán con un planteamiento bilingüe, en euskera y castellano, sin que ello suponga un precio o cargo adicional.

Se aplicarán políticas de comunicación que garanticen el uso no sexista y no androcéntrico del lenguaje, imágenes y contenidos.

72724351F KOLDOBIKA PECIÑA (R: G75203067)
Digitalki sinatuta norengandik: 72724351F KOLDOBIKA PECIÑA (R: G75203067)
Data: 2021.08.24 13:32:52 +02'00'