ANEXO I. CATÁLOGO DE SOLUCIONES A IMPLEMENTAR

La empresa adjudicataria deberá garantizar que las soluciones de ciberseguridad implementadas cumplan con los requisitos técnicos establecidos en este pliego. Estas soluciones deberán ser modernas, eficaces y adecuadas para las necesidades específicas de las pymes y autónomos participantes. A continuación, se detallan los requisitos técnicos para cada tipo de solución.

1. Herramientas de protección.

- Deberá ser un Agente único, que incluya en una misma solución tanto EPP como EDR.
- Solución incluida en el catálogo STIC-105 del CCN como CUALIFICADO ENS ALTO, para las dos categorías.
- Solución completamente nube y alojada en territorio de la Unión Europea.
- Soporte para sistemas Legacy como: Windows 7, Windows 2008 o similares.
- Consumo de recursos muy limitado, máximo 5% con todos los componentes.
- Soporte mínimo para Windows, Linux, Mac, Android e iOS.
- Descubrimiento e instalación de dispositivos sin protección, aunque no disponga de Directorio Activo en la red.
- Consola en español.
- Búsqueda de IOC's, basados en hash de fichero, nombre, ubicación o conexión y reglas Yara, en tiempo real.
- Posibilidad de importación masiva de reglas Yara o IoCs a través del formato STIX 2.x
- Capacidad de aislamiento de los equipos con posibilidad de autorizar la conexión de algunas aplicaciones.
- Firewall personal por puesto de trabajo con posibilidad de ser manejado tanto por el usuario como por el administrador. Incluirá protección, y granularidad para discernir ataques, entre otros, como: SYN flood, TCP Port Scan, Smart DNS, OS Detection, etc...
- Servicio gestionado de clasificación del 100% de las aplicaciones, ejecutables y librerías de los equipos de forma externa sin usar recursos locales de la máquina y sin necesidad de intervención del usuario.
- Capacidad de bloqueo de procesos ejecutables hasta que sea confirmado por el personal de laboratorio.
- Capacidad de tener diferentes modos de configuración del bloqueo de procesos: audit, hardening y lock.
- Capacidad de bloqueo de dispositivos USB, bluetooth, móviles. Webcam y módems.
- Capacidad de auditoría y bloqueo de acceso a páginas web por categorías y listas blancas y negras.
- Trazabilidad de la actividad de amenazas detectadas hasta 365 días.

- Soporte técnico de nivel 1, 2 y 3 (R&D) en español.
- Soporte técnico 24x7.
- Soporte de laboratorio en español.
- Centro de desarrollo en territorio nacional.
- Sistema de reducción de superficie de ataque con granularidad para auditar o bloquear herramientas involucradas en ataques del tipo living-off-the-land.
- Servicio de validación e inclusión de Indicadores de Ataque de alta confianza.
- La solución debe permitir la creación de roles personalizados en los que se establecerá que opciones de la consola estarán disponibles y sobre que equipos se podrá actuar. Estos roles serán aplicados a los usuarios administradores de la consola.

2. Securización de las comunicaciones.

- El dispositivo de firewall debe admitir la configuración de tres zonas de seguridad: externa, privada y opcional (DMZ).
- El sistema de dispositivo de firewall debe admitir direcciones IP estáticas y dinámicas (DHCP y PPPoE) en la interfaz externa.
- El dispositivo de firewall tiene configuraciones de relé DHCP que permiten la adición de hasta tres servidores DHCP con la capacidad de realizar comunicaciones simultáneas con hasta 3 servidores DHCP.
- El dispositivo de firewall puede habilitar DHCPv6 en una interfaz externa.
- El rendimiento del dispositivo de firewall debe admitir un rendimiento de firewall de 3,5 Gbps y un rendimiento UTM de 1,2 Gbps (GAV e IPS combinados).
- El dispositivo de firewall debe admitir 350.000 conexiones simultáneas.
- El dispositivo de firewall debe ser un UTM, que incorpore filtrado de URL, IPS, GAV, control de aplicaciones, DLP, protección contra amenazas de día cero, proporcionar una capacidad de detección y respuesta, incluida la correlación entre la red y el punto final, e incluir firewall de DNS consolidado y educación antiphishing.
- El dispositivo de firewall debe ser un firewall de próxima generación, que incorpore filtrado de URL, IPS, antivirus de próxima generación, control de aplicaciones, DLP, protección de próxima generación contra amenazas de día cero, proporcionar una capacidad de detección y respuesta, incluida la correlación entre la red y el punto final, e incluir firewall de DNS consolidado y educación antiphishing.
- El dispositivo de firewall debe admitir la implementación de políticas de seguridad en la capa de aplicación (capa 7), también conocida como proxy de aplicación.
- El dispositivo de firewall debe incluir políticas de seguridad en los servidores proxy de capa de aplicación preconfigurados con valores predeterminados seguros para admitir los siguientes protocolos comunes:
    - HTTP / HTTPS
    - POP3 / POP3S
    - IMAP / IMAPS
    - SMTP / SMTPS
    - FTP
    - DNS
    - SORBO
    - H323
- El dispositivo de firewall debe admitir la autenticación a través de servidores RADIUS, SecureID, LDAP, Active Directory o similares.

- El dispositivo de firewall debe admitir la autenticación transparente en los servidores de Active Directory (inicio de sesión único).
- El dispositivo de firewall puede habilitar/deshabilitar SSLv3 en acciones de proxy HTTPS/SMTP.
- El dispositivo de firewall debe admitir reglas de configuración para que los proxies explícitos acepten solicitudes directas de los clientes y recuperen información en nombre de los clientes.
- El dispositivo de firewall debe admitir la capacidad de habilitar FTP web habilitando el proxy explícito para utilizar comandos FTP nativos y enviar los datos en una respuesta HTTP.
- El dispositivo de firewall debe admitir la capacidad de configurar un proxy SMTP para analizar documentos incrustados con macros y la opción de eliminar macros antes de enviar el documento al destinatario previsto.
- El dispositivo de firewall debe admitir la capacidad de utilizar certificados autofirmados para realizar una inspección profunda de paquetes de correo a través de un proxy SMTP a través de TLS.
- El dispositivo de firewall debe admitir la capacidad de aprovechar el proxy HTTPS para la inspección profunda de contenido.
- El dispositivo de firewall puede aprovechar el proxy HTTPS para limitar el acceso a las cuentas de Google de los consumidores, pero aún así permitir el acceso a Google Apps for Work/Google Apps for Educators.
- El dispositivo de firewall debe admitir la capacidad de establecer el intervalo de tiempo máximo para los inicios de sesión FTP fallidos por conexión en las acciones de proxy de cliente y servidor FTP.
- El dispositivo de firewall también otorgará la capacidad de usar el dispositivo como un servidor NTP con creación automática de políticas NTP para dispositivos en redes de confianza.
- El dispositivo de firewall debe ser compatible con DNS dinámico.
- El dispositivo de firewall debe tener defensas de ataque fragmentadas para que el dispositivo pueda volver a ensamblar los paquetes fragmentados antes de pasarlos a la red interna.
- El dispositivo de firewall debe ser capaz de filtrar el contenido dentro de los protocolos más comunes. Como tal, deberían poder filtrar por tipo de contenido MIME.
- El dispositivo de firewall debe proteger los servidores de correo electrónico internos contra la retransmisión abierta. Debería ser capaz de configurar su computadora para dominios que acepten correo electrónico.

- El dispositivo de firewall debe permitir la configuración de umbrales para detectar ataques de inundación (inundación) y denegación de servicio (DoS) y denegación de servicio distribuido (DDoS).
- El dispositivo de firewall admite la detección de anomalías del protocolo (PAD) para DNS y otros protocolos comunes.
- El dispositivo de firewall admite la indicación de nombre de servidor (SNI) para configurar dominios para la funcionalidad de bloqueo, permiso, inspección.
- El dispositivo de firewall complementa la capacidad de bloqueo de CN existente con SNI para bloquear específicamente ciertos dominios de Google.
- El dispositivo de firewall debe admitir el bloqueo y la administración del tráfico por dominio disponible a través de nombres de dominio completos (FQDN) para bloquear el tráfico de los sitios alojados en redes de entrega de contenido (CDN).
- El dispositivo de firewall admite la capacidad de bloquear dominios mediante funciones de comodín.
- El dispositivo de firewall admite la capacidad de establecer políticas para direcciones IP mediante funciones comodín.
- Los dispositivos de firewall admiten la capacidad de denegar conexiones hacia o desde un país en particular (bloqueo de ubicación geográfica) a nivel de política.
- La solución UTM debe ser compatible con VPN móviles.
- La solución UTM debe admitir al menos 1000 VPN móviles que utilicen IPSec.
- La solución UTM debe admitir al menos 600 usuarios móviles que utilicen VPN SSL.
- La solución UTM debe admitir la capacidad de descargar el software del cliente SSL desde el firewall.
- La solución UTM debe admitir la disponibilidad del software de cliente SSL para Windows XP, Windows Vista, Windows 7, 8, 10 y macOS, Android e iOS.
- La solución UTM debe ser compatible con VPN entre oficinas (de sucursal a sucursal).
- La solución UTM admite al menos 600 VPN entre oficinas utilizando IPSec.
- La solución UTM debe admitir interacciones con cualquier otro producto de marca que tenga soporte IPSec estándar.

3. Control de acceso a la información.

- Es requisito que toda la gestión, control e integración esté realizada en la nube.
- Toda la gestión se debe de poder realizar desde un interfaz web que sea multi capa y multi cliente. Además, debe de permitir ser operado por múltiples administradores con diferentes tipos de accesos basados en roles y con autenticación multi factor.
- El panel de control y visualización debe de proveer, al menos, las siguientes funcionalidades:
    - Autenticaciones establecidas y con éxito y falladas.
    - Alertas y Notificaciones con posibilidad de mandarlas por correo electrónico, al menos para las siguientes condiciones:
        - Usuario deniega el Push de acceso.
        - El Proxy/Gateway está desconectado o ha reconectado con la nube.
        - Ejecución de la sincronización en Directorio Activo o solución de LDAP.
        - Problemas con las cuentas de usuario: expiración de subscripción, gestión de delegación, etc.
    - Información sobre licencias.
    - Número de recursos protegidos por tipo.
    - Información crítica, como, por ejemplo, notificaciones de tipo Push denegadas.
- Los logs deben de ser exportables y en tiempo real, con toda la información acerca del elemento que los accionó: origen, usuario, recurso, fecha y hora, etc…
- Se debe de soportar multi factor de autenticación para las siguientes aplicaciones:
    - SAML
    - Soluciones basadas en RADIUS y VPNs
    - Servidores y estaciones de trabajo Windows con protección de inicio de sesión
    - Estaciones de trabajo macOS con protección de inicio de sesión
    - ADFS
    - RDP
    - RD Web
    - APIs de autenticación (REST) para portales web y aplicaciones desarrolladas internamente por la empresa
- La solución debe de permitir la configuración de políticas de autenticación basadas en grupos de usuario, recursos protegidos, funcionalidades de riesgo y métodos de autenticación a ser usados.
- Esta solución deberá aportar un factor de autenticación usando un token en una aplicación móvil junto con contraseña de uso única basada en OATH.
- El fabricante de la solución debe de soportar, al menos 3 opciones en cuanto a la autenticación:

  - Token en app. Móvil, a través de una aplicación gratuita para móviles o tablets en iOS y Android.
  - TOTP hardware token, fabricado por el mismo fabricante para garantizar la información sensible del dispositivo.
  - TOTP hardware token fabricado por un tercero con claves secretas importadas usando el formato OATH PSKC (RFC 6030).
- Los usuarios deben de estar visualizados y gestionados tanto si están creados localmente o sincronizados con un directorio externo.
- La definición de los métodos de autenticación deberá de estar disponibles para los administradores y estos serán, entre otros:
  - Contraseña
  - Autenticación basada en Push
  - Autenticación basada en Desafio/Respuesta
  - Contraseña única basada en tiempo
- Como parte de la solución, se incluirá un interfaz que permita configurar políticas de riesgo sin coste adicional.
- La plataforma ofrecerá uno o varios ayudantes virtuales para que los administradores empiecen a operar con la solución en las funciones básicas: creación de grupos, usuarios y protección de recursos.
- Se deberá de poder personalizar con el portal de acceso web y la imagen de los correos y notificaciones PUSH.
- La creación de usuarios deberá de ser posible, al menos, de dos maneras:
  - Manual: registrando la información de usuario que debe de incluir, como mínimo, id de usuario único, único email y nombre y apellido.
  - Automática a través de:
    - Microsoft Directorio Activo
    - Azure Directorio Activo
    - Base de datos estándar LDAP
- La herramienta debe soportar SAML 2.0 y actuar como Proveedor de Identidad (IdP) para poder ser integrada con aplicaciones en la nube que soporten SAML 2.0
- Deberá de ser posible una manera de definir funcionalidades de riesgo y añadirlas de manera opcional a las políticas de autenticación. Estas funcionalidades deberán de poder combinarse dentro de una misma política.
- Se requiere que haya una funcionalidad basada en tiempo permitiendo la configuración de horas dentro de días de la semana y hora dentro de días específicos que se asociaran a las diferentes políticas con el fin de limitar su uso.
- Se requiere que se pueda limitar el acceso por país donde se solicita la entrada, pudiendo limitar o permitir por política.

- Se deberá de poder instalar un agente en portátiles con Windows, servidores y estaciones para añadir funcionalidades de Windows Logon.
- Se deberá de poder instalar un agente en estaciones con macOS para añadir funcionalidades de Windows Logon.
- Las autenticaciones basadas en notificaciones tipo Push y en código QR deberán incluir al menos, el nombre del usuario intentando autenticarse, el día y la hora y el recurso al que se está accediendo.
- Para autenticación SAML, la notificación Push y el mensaje del código QR tienen que incluir también detalles acerca de la localización física del dispositivo y navegador Web que intenta conectar.
- Para autenticaciones en Windows y macOS, la notificación Push y el mensaje del código QR deberá incluir el nombre del dispositivo, sistema operativo y localización si es posible de determinar.

4. Copias de seguridad

La solución de copia de seguridad deberá ser 100% cloud o nube y realizar una copia de seguridad de todos los elementos informáticos del autónomo y/o pyme: los servidores Windows, las instancias en la nube, los ordenadores de sobremesa y los portátiles de la organización frente al tiempo de inactividad o la pérdida de datos, manteniéndola de forma ilimitada durante la vigencia del contrato.

La solución de copia de seguridad deberá permitir recuperar archivos y carpetas individuales o realizar una restauración completa de la máquina antigua, en el mismo hardware o en otro distinto. No deberá ser necesario reinstalar el sistema operativo ni reconfigurar las aplicaciones. Deberá recuperar archivos y carpetas con una sencilla recuperación de instantáneas puntuales.

La solución de copia de seguridad deberá permitir la restauración de los datos a su sitio original (in-place), bajar datos localmente o mediante enlace de URL público que contenga información específica del backup (objetos, carpetas, servicios completos). Adicionalmente deberá contar con una descarga automatizada de los datos.

La solución de copia de seguridad deberá garantizar la integridad de los datos respaldados y que éstos no puedan ser manipulados. También deberá garantizar que estos datos no puedan ser violentados por terceros. Todas las funcionalidades de La solución de copia de seguridad deben estar incluidas y deben incorporarse en la oferta sin incurrir en sobrecostes para el autónomo y/o pyme por incremento de funcionalidades.

La solución de copia de seguridad deberá dar opción de recuperar los datos que necesite mediante, donde los necesite funciones de restauración diferencial: restaurar en la ubicación original, en una ubicación diferente del destino original, en un nuevo dispositivo de destino, ejecutar una recuperación bare metal o descargar archivos directamente. deberá permitir reducir el tiempo de recuperación al restaurar sólo los bloques modificados de un archivo.

La disponibilidad de la solución de copia de seguridad deberá estar basada en un modelo de 24 horas por 7 días a la semana. El acceso a la solución de copia de seguridad deberá ser a través de navegador.

La solución de copia de seguridad deberá disponer de funcionalidad de auditoría a través del navegador. También la función de buscador de la información de auditoría por períodos específicos de tiempo y la posibilidad de obtener reportes de supervisión en formato “CSV”.

La solución de copia de seguridad deberá permitir la creación de usuarios con diferentes niveles de permisos y múltiples roles de usuarios.

La solución de copia de seguridad deberá tener una funcionalidad de vista previa que permita al administrador encontrar y liberar más rápidamente el elemento requerido, sin la necesidad de bajar el documento localmente antes corroborar que es el documento deseado para restaurar.

La solución de copia de seguridad deberá proporcionar diferentes opciones de búsqueda inteligente, destacando:

1. Búsqueda recursiva global que le permita buscar simultáneamente en estas cuatro categorías para encontrar y restaurar rápidamente los datos perdidos:
    - Tipos de datos
    - A través del tiempo
    - En todos los usuarios
    - En todas las versiones
2. “Búsqueda borrosa” en los casos donde no se conozca la palabra o nombre exacto de lo que se está buscando.
3. Búsqueda inteligente que permita buscar información de todo el Backup así como también periodos o “Copias” específicas.