**MODELO COMPILACIÓN DE EVIDENCIAS**

**1ª CONVOCATORIA**

**ÍNDICE**

[**1.** **HERRAMIENTAS DE LA SOLUCIÓN.** 3](#_Toc135585015)

[**2.** **PRODUCTOS SUMINISTRADOS.** 5](#_Toc135585016)

[**3.** **DISPOSITIVOS SUMINISTRADOS.** 6](#_Toc135585017)

[**4.** **CONFIGURACIÓN INICIAL Y ACTUALIZACIONES DE SEGURIDAD.** 7](#_Toc135585018)

[**5.** **FORMACIÓN.** 8](#_Toc135585019)

**CIBERSEGURIDAD**

A continuación, se muestran las evidencias extraídas para justificar la implantación y el funcionamiento de la solución de digitalización conforme a lo dispuesto el Anexo IV de la Orden de bases reguladoras.

Además, se especifica el tipo de captura para cada apartado, que puede ser:

* **Personalizada:** en este tipo de captura se requiere que aparezca información identificativa del Beneficiario, por ejemplo, nombre de la empresa, CIF, emails cuyo dominio sea el dominio web del Beneficiario, etc.
* **Genérica:** no es necesario incluir información específica del Beneficiario, pero sí evidenciar que la captura o información de la hoja de producto aportadas, corresponden a la herramienta implantada en el Beneficiario, bien porque se visualiza el nombre de la herramienta y coincide con el indicado en la memoria técnica, o bien porque las capturas de pantalla tienen el mismo interfaz que las “personalizadas” aportadas en este mismo documento.

# **HERRAMIENTAS DE LA SOLUCIÓN.**

|  |  |
| --- | --- |
| Información que aportar | *Adjuntar, a continuación, las capturas de pantalla de las opciones de configuración/parametrización de los distintos productos suministrados (consola centralizada o en cada instalación individual) que evidencien todas las coberturas exigidas para la solución:*   * ***Antimalware:*** *la solución deberá proporcionar una herramienta que analice el dispositivo, su memoria interna y los dispositivos de almacenamiento externos.* * ***Antispyware:*** *la solución deberá proporcionar una herramienta que detecte y evite el malware espía.* * ***Correo seguro:*** *la solución deberá proporcionar herramientas de análisis del correo electrónico con las siguientes características:*   + *Antispam, con detección y filtro de correo no deseado.*   + *Antiphishing, con detección de correos con enlaces o malware que se sospecha sirvan para robar credenciales.* * ***Navegación segura:***   + *Control de contenidos.*   + *Antiadware para evitar anuncios maliciosos.* * ***Análisis y detección de amenazas:*** *la solución deberá permitir conocer el comportamiento de las amenazas conocidas y nuevas.* * ***Monitorización de la red:*** *la solución deberá proporcionar herramientas que analicen el tráfico de red y alerten de amenazas.*   ***Las capturas de pantalla deberán evidenciar todos y cada uno de los elementos de la lista anterior.***  *Podrán incluirse capturas de pantalla de la data sheet u hoja del producto en las que figuren estas funcionalidades.* |
| Tipo de evidencia esperada | ***Genérica*** |
| Observaciones | *Para aceptar capturas genéricas para este requisito se debe evidenciar que la herramienta de las capturas es la implantada en el Beneficiario. Se puede admitir un documento genérico de características del producto, siempre que:  - Las capturas de los dispositivos y productos suministrados sean correctas y evidencien la implantación en el Beneficiario concreto.   - Todas las herramientas concretas que se documenten en el archivo que se aporte como evidencia cubran las herramientas solicitadas para este requisito en la Orden de Bases.* |

# **PRODUCTOS SUMINISTRADOS.**

|  |  |
| --- | --- |
| Información que aportar | *Adjuntar, a continuación, las capturas de pantalla que evidencien las licencias o la instalación de los productos para los dispositivos indicados en el formulario.* |
| Tipo de evidencia esperada | ***Personalizada*** |
| Observaciones |  |

# **DISPOSITIVOS SUMINISTRADOS.**

|  |  |
| --- | --- |
| Información que aportar | *Adjuntar, a continuación, las capturas de pantalla que evidencien el número de dispositivos suministrados conforme a lo indicado en el formulario de justificación.* |
| Tipo de evidencia esperada | ***Personalizada*** |
| Observaciones | *Se deben aportar capturas de pantalla que evidencien el número total de dispositivos, según lo indicado en la memoria técnica.*  *Podrán obtenerse capturas de las consolas de control donde figuren los dispositivos en los que están instaladas las soluciones o de ventanas en las que aparezca el nombre de cada equipo y el producto instalado.* |

# **CONFIGURACIÓN INICIAL Y ACTUALIZACIONES DE SEGURIDAD.**

|  |  |
| --- | --- |
| Información que aportar | *Adjuntar, a continuación, las capturas de pantalla de las opciones de configuración/ parametrización, adaptadas al cliente que acrediten la configuración inicial otorgada a la solución y las últimas actualizaciones de las firmas de malware y otras bases de datos para la detección de amenazas (consola centralizada o instalación individual).* |
| Tipo de evidencia esperada | ***Personalizada*** |
| Observaciones | *Se deben aportar capturas de pantalla de la configuración específica realizada en el cliente.* |

# **FORMACIÓN.**

|  |  |
| --- | --- |
| Información que aportar | *Adjuntar, a continuación:*   * *Capturas de pantalla del material entregado al Beneficiario en el marco de la tutorización para la configuración del software de seguridad* * *Kit de concienciación en ciberseguridad.*   *Asimismo, se debe demostrar que la formación ha sido impartida o facilitada a través de cualquiera de las siguientes evidencias:*   * *Declaración responsable del Beneficiario / Agente Digitalizador* * *Correo electrónico con envío de la documentación de la formación* * *Evidencias obtenidas a partir de la propia solución implantada al Beneficiario y vinculada al mismo* * *Cualquier otra evidencia que demuestre la impartición del curso* |
| Tipo de evidencia esperada | ***Personalizada*** |
| Observaciones | *Además de los requisitos de formación comunes, la formación impartida al Beneficiario deberá incluir una tutorización para la configuración del software de seguridad, así como incluir un kit de concienciación en ciberseguridad para complementar la solución con habilidades de firewall humano.*  **Este requisito no aplica para la justificación de la Fase 2.** |