**MODELO COMPILACIÓN DE EVIDENCIAS**

**5ª CONVOCATORIA**

**ÍNDICE**

[**1.** **DISPOSITIVOS SUMINISTRADOS.** 4](#_Toc192750549)

[**2.** **INSTALACIÓN Y CONFIGURACIÓN INICIAL.** 5](#_Toc192750550)

[**3.** **DETECCIÓN Y RESPUESTA EN LOS ENDPOINTS.** 6](#_Toc192750551)

[**4.** **FUENTES A MONITORIZAR.** 7](#_Toc192750552)

**CIBERSEGURIDAD GESTIONADA**

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, NIF, 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.

# **DISPOSITIVOS SUMINISTRADOS.**

|  |  |
| --- | --- |
| Información que aportar | La solución deberá incluir el mínimo de dispositivos requeridos para el segmento.Se deberán adjuntar las capturas de pantalla que evidencien el número de dispositivos suministrados conforme a lo indicado en la memoria técnica.* **Segmento IV: hasta 99 dispositivos.**
* **Segmento V: hasta 145 dispositivos.**
 |
| Tipo de evidencia esperada | **Personalizada.** |
| Observaciones | -Se deberá comprobar que las capturas de pantalla 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. |

# **INSTALACIÓN Y CONFIGURACIÓN INICIAL.**

|  |  |
| --- | --- |
| Información que aportar | Instalación y configuración inicial de las herramientas de seguridad para la detección, interrupción y respuesta ante amenazas en los endpoints (servidores, PCs, portátiles, teléfonos móviles…) y/o a nivel global (p.e. sondas), integrados con una solución SIEM donde se recopile la información procedente de distintas fuentes de la empresa para su correlación y análisis.Se deberán aportar capturas de pantalla de las opciones de configuración/parametrización adaptadas al cliente que acrediten la configuración inicial otorgada a la solución para la detección de amenazas (consola centralizada o instalación individual). |
| Tipo de evidencia esperada | **Personalizada.** |
| Observaciones |  |

# **DETECCIÓN Y RESPUESTA EN LOS ENDPOINTS.**

|  |  |
| --- | --- |
| Información que aportar | La solución implantada debe contemplar mecanismos de detección y respuesta en los endpoints pudiendo suministrarse la protección EDR junto con el resto de los componentes de la solución implantada o pudiendo ésta integrarse con soluciones EDR ya existentes en los endpoints.Se deberán aportar capturas de pantalla del funcionamiento de los mecanismos de detección y respuesta en los endpoints otorgados a la solución. |
| Tipo de evidencia esperada | **Genérica.** |
| Observaciones |  |

# **FUENTES A MONITORIZAR.**

|  |  |
| --- | --- |
| Información que aportar | La solución implantada deberá proteger frente a las amenazas que afecten a diversas fuentes de la empresa como endpoints (servidores, PCs, portátiles, teléfonos móviles…) o soluciones Cloud.Se deberán aportar capturas de pantalla que evidencien el software instalado ante las amenazas que afecten a diversas fuentes de la empresa como endpoints (servidores, PCs, portátiles, teléfonos móviles…) o soluciones Cloud. |
| Tipo de evidencia esperada | **Genérica.** |
| Observaciones  |  |