Núm. expediente: 32/2021/NNTT

1. RESUMEN EJECUTIVO

1.-NOMBRE DE LA ADMINISTRACIÓN SOLICITANTE DEL PROYECTO
Ayuntamiento de Fuengirola

2.-CIRCUNSCRIPCIÓN DE LA ENTIDAD
Provincia: **Málaga**
Comunidad Autónoma: **Andalucía**

3.-UNIDAD ADMINISTRATIVA A LA QUE SE CIRCUNSCRIBE
L01290542-AYUNTAMIENTO DE FUENGIROLA

4.-PERSONA DE CONTACTO
NOMBRE Y APELLIDOS
Nombre y apellidos : **Isabel González Estévez**
TELÉFONO
Incluir el prefijo **0034 952589411**
CORREO ELECTRÓNICO
Correo electrónico corporativo **movilidad@fuengirola.org**

5.-TÍTULO DEL PROYECTO
Proyecto para la implantación de medidas técnicas y organizativas para continuar en la adecuación al esquema nacional de seguridad (ENS) y mejora de la seguridad tanto en el Ayuntamiento como en las dependencias municipales.

6.-DESCRIPCIÓN DEL PROYECTO (incluir fases y tareas del proyecto)1000 CARACTERES

La implantación y mejora de los servicios del Ayuntamiento, tiene que ir de la mano de una infraestructura de base, lógica de control, respuesta rápida ante incidentes y peticiones en el incremento de recursos (nuevos accesos, usuarios, aplicaciones, interacción con otras administraciones). Todo esto protegido adecuadamente por medidas de seguridad a nivel físico, lógico y concienciación del personal, de manera que vayan en línea con la guía CCN-STIC-803 del Esquema Nacional de Seguridad, en cuanto a los criterios que se han de tener en cuenta para su correcto cumplimiento (disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad).Actualmente el Ayuntamiento de Fuengirola posee 10 sistemas de categoría media a los que la ejecución de este proyecto afectaría positivamente.

El citado proyecto divide en 3 hitos que a su vez se dividen en actuaciones:

H1- INTEGRACION CON HERRAMIENTAS DEL CCN-CERT

A1 Lucia y micro Claudia :

H2 AMPLIACIÓN DE CONTROL DE SEGURIDAD EN LOS ACCESOS A LOS SISTEMAS

A1- Sustitución de Cortafuegos

A2 – Adecuación de la Herramienta SIEM con adecuación al ENS

H3- Formación técnica en materia de ciberseguridad

A1 - Plan de concienciación

A2- Plan de formación

1.Licitación y reunión inicial

2. Implementación y despliegue de las herramientas MicroClaudia y LUCIA

3.Cambio de seguridad perimetral y migración de políticas al nuevo entorno.

4.Plan Formación y concienciación.

5.Batería de Pruebas

6.Pago y justificación de actuaciones.

7.-EVIDENCIA, ANÁLISIS Y DATOS QUE MOTIVEN LA NECESIDAD DEL PROYECTO

Ante el contexto creciente en complejidad y número de los ciberataques a los que se ve expuesta la sociedad en la actualidad, agravado si cabe por la pandemia, es imprescindible que las Administraciones Públicas Locales puedan contar con las capacidades de un Centro de Operaciones de Ciberseguridad que les permita gestionar de forma adecuada la seguridad de sus infraestructuras, comunicaciones y servicios digitales prestados a empresas y ciudadanos, mejorando sus capacidades de prevención, detección y respuesta ante incidentes de ciberseguridad.

Todo ello ligado a los requerimientos reflejados en el Esquema Nacional de Seguridad para GARANTIZAR los servicios prestados a la ciudadanía, PROTEGIENDO la información que estos servicios tratan, cuando se apoyan directa o indirectamente en medios electrónicos.

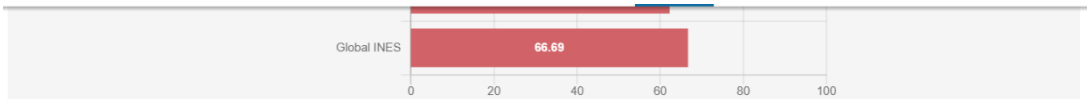
No obstante, es una realidad que, para garantizar y proteger los servicios y la información tratada por éstos, no es posible actuar directamente en ellos, sino que se debe realizar sobre el sistema de información que los soporta. Y esa actuación, en base al riesgo evaluado y a la categorización del sistema, partiendo de la valoración de los servicios y la información, consistirá en aplicar determinadas medidas de seguridad que habrán de permitir reducir el referido riesgo respecto a la seguridad a niveles aceptables.

Todo ello es necesario porque la implementación del ENS es la garantía para mantener la validez legal de las transacciones electrónicas desarrolladas por medios presenciales o telemáticos.

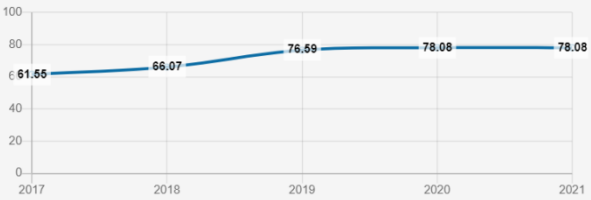
Los incidentes relacionados con eventos en los Sistemas de Información del Organismo, así como una inadecuada custodia y gestión de la vigencia de los documentos electrónicos que intervienen en las transacciones electrónicas, pueden derivar en problemas legales y pueden constituir un serio inhibidor en el uso de medios electrónicos en la Administración.

El eslabón más débil de la seguridad es siempre el empleado, al que los ciber atacantes dedican especialmente su atención, por lo que cualquier estrategia completa de seguridad debe tener en cuenta su adecuada capacitación y concienciación en materia de seguridad y ciber amenazas (de los empleados públicos).

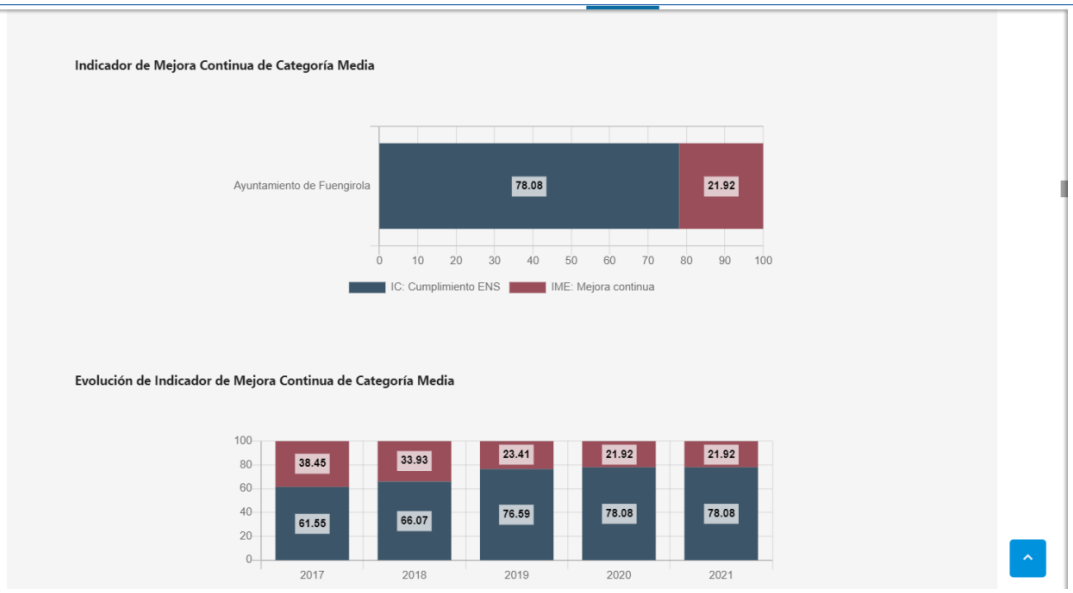
Según los registros en la herramienta INES del CCN-CERT, la situación del Ayuntamiento de Fuengirola desde el 2017 hasta ahora, es la siguiente:

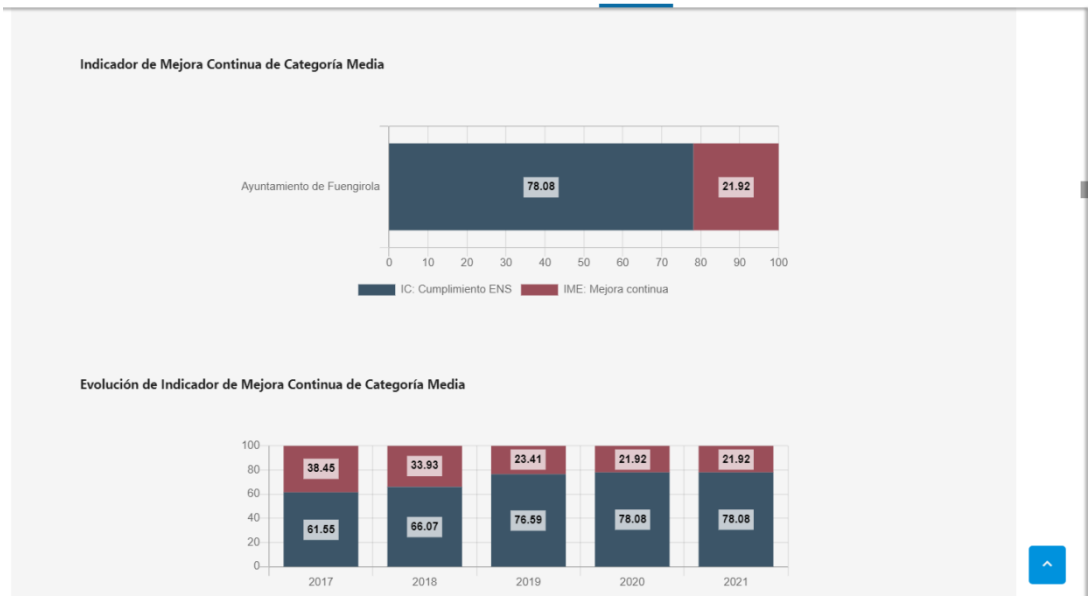


Evolución de Indicadores de Cumplimiento de Categoría Media



Indicadores de Cumplimiento de Categoría Alta





Como se puede observar en los dos últimos años el Ayuntamiento de Fuengirola se ha

quedado estancado en cuanto a medidas de protección de categoría media.

Para llegar a un índice de cumplimiento del 100% es esencial mejorar en medidas de protección, más aún cuando en el último año se han elevado el número de ciberataques que amenazan la seguridad de la información y que requieren de un mayor número de índices de control que ayuden a prevenir incidentes; no sólo a nivel de confidencialidad, sino también de disponibilidad y de integridad.

En los últimos 4 años la formación específica en materia de seguridad se ha limitado a formaciones orientadas a la protección del dato para los usuarios del Ayuntamiento, sin hacer formación específica para los técnicos en IT. Todo esto incrementado por los cambios que se han producido en el ENS.

Está claro que con la implantación y formación en las herramientas que el ccn-cert pone a disposición el Ayuntamiento, así como el aprendizaje en el uso de las ya existentes (lógica) nos ayudará a aproximarnos al 100% del índice de cumplimiento, acompañado por la infraestructura mejorada y adecuada a las exigencias de seguridad recogidas por el ENS.

El Ayuntamiento se propone durante el año 2022 superar las deficiencias existentes con el objetivo de solicitar la certificación en el ENS a partir del 2023.

Es por todo esto, la necesidad de actuar en esta línea reforzando y ampliando los distintos sistemas de seguridad que salvaguardan la información de este ente local y mejorar el conocimiento a nivel técnico.

8.-ALINEAMIENTO CON LAS PRIORIDADES ESTABLECIDAS PARA LOS PROYECTOS

PRIORIDADES (seleccionar con una X)	Marcar con una X
Prioridad 1. Puesta en marcha de un Centro de Operaciones de Ciberseguridad	**X**
Prioridad 2. Desarrollo de los tres servicios más utilizados	
Prioridad 3. Puesta a marcha de un proyecto de automatización	

Prioridad 4. Desarrollo o adaptación de servicios exentos de barreras transfronterizas	
No aplica	

9.-DESCRIPCIÓN DE LAS ACTUACIONES

Nombre de la actuación y descripción. Se deberá tener en cuenta las tipologías de actuaciones subvencionables para cada línea estratégica de acuerdo con los apartados 6 a 10 de la Guía de requisitos

NOMBRE DE LA ACTUACIÓN	DESCRIPCIÓN
Integración con herramientas del CCN-CERT - A1 – Implantación de la herramienta LUCIA	**Implementar con el fin de poder gestionar de un modo eficaz los incidentes en cualquier organismo público (sobre todo aquellas que colaboran con el CCN-CERT) se encuentra disponible en el portal del CERT Gubernamental Nacional la versión 2.5 de la herramienta LUCIA.** **Gracias a ella, es posible comunicar y sincronizar los incidentes provenientes de una entidad con LUCIA Central, la instancia del CCN-CERT desde la que se gestionan todos los ciberincidentes.**
Integración con herramientas del CCN-CERT - A2 – implantación de la herramienta micro Claudia	**Implementar MicroCLAUDIA es una capacidad basada en el motor de CLAUDIA que proporciona protección contra código dañino de tipo ransomware a los equipos de una entidad. Para ello, hace uso de un agente ligero para sistemas Windows que se encarga del despliegue** **y ejecución de vacunas.**
Ampliación de control de seguridad en los accesos a los sistemas - A1 – Implantación de herramientas de seguridad perimetral conforme a catálogo **CCN-STIC 105**	**Para el cumplimiento con la normativa de seguridad conforme al Esquema Nacional de Seguridad, se deberán implantar y bastionar dos niveles de Cortafuegos para la** **protección tanto del perímetro exterior de la red como de las infraestructuras internas que proporcionan servicio al personal del ayuntamiento y a los ciudadanos**
Ampliación de control de seguridad en los accesos a los sistemas A2 – Adecuación de la herramienta SIEM LogICA disponible	**Para el cumplimiento con la normativa de seguridad conforme al Esquema Nacional de Seguridad, se procederá a la adecuación de la herramienta existente SIEM a la normativa vigente.**
Formación técnica en materia de ciberseguridad -	**Mediante las actividades de formación y concienciación se**

A1 – Actividades de concienciación	**consigue promover y reforzar la cultura de seguridad de la entidad a través del desarrollo e implementación** **de un Plan de concienciación y Sensibilización, y formación, en el que se transformarán e interiorizarán comportamientos y hábitos en seguridad en el día a día de los empleados**
Formación técnica en materia de ciberseguridad - **A2 – Actividades de formación**	**Mediante las actividades de formación y concienciación se consigue promover y reforzar la cultura de seguridad de la entidad a través del desarrollo e implementación** **de un Plan de concienciación y Sensibilización, y formación, en el que se transformarán e interiorizarán comportamientos y hábitos en seguridad en el día a día de los empleados**

10.-DESCRIPCIÓN DE LOS INDICADORES ASOCIADOS AL PROYECTO

Nombre del indicador y descripción. Se deberá tener en cuenta las tipologías de actuaciones subvencionables para cada línea estratégica de acuerdo con los apartados 6 a 10 de la Guía de requisitos

NOMBRE DEL INDICADOR

ICI: Indicadores de control de implantación del proyecto

IR: Indicadores de resultados finales tras el período que consideramos que es suficiente como para ver de forma efectiva la utilidad del proyecto.

Tipo indicador	**Tipo desviación**	**Grado cumplimiento**	**Medida correctiva**
ICI	Tiempo de implantación	% desviación	M1, M3, M4
ICI	Falta de información de los ítems aplicados y conseguidos	Nº informes actualizados	M2

IR	Test de conocimientos insuficiente tras formación recibida	Deben de al menos tener calificación de un 7	M2, M3,M5
IR	Número de sistemas de categoría media a los que aplica las nuevas medidas encaminadas a la certificación ENS	10 sistemas con medidas adicionales	M2,M3,M4

MEDIDAS CORRECTIVAS

Tipo de medida	**Corrección aplicada**
M1	Asignación personal por parte del adjudicatario
M2	Cambio de técnico gestor o del personal de formación
M3	Revisión del plan de implantación para añadir/modificar/eliminar puntos de control y consecución de objetivos
M4	Revisión de recursos disponibles para gestión de incidencias
M5	Ampliación de formación a técnicos

11.-COLECTIVO OBJETIVO DEL PROYECTO

Por ejemplo, empresas en general, pequeñas y mediana empresas [pymes], sectores específicos, población en general, familias, estudiantes, trabajadores de un sector determinado...

Las mejoras que se implantan en este proyecto están orientadas a afianzar la seguridad de cara al público en general y en particular a los empleados, dando un mayor nivel de cumplimiento en lo refereido a las dimensiones recogidas en el ENS (disponibilidad, confidencialidad, trazabilidad, integridad y autenticidad)

12.-IMPLEMENTACIÓN DEL PROYECTO

Desarrollar cada fase de ciclo de vida de proyecto con una planificación de fechas estimadas

1. **Licitación: 01/01/2022-30/04/2022.**
2. **Implantación y ejecución asociadas a los hitos:**
   - **Integración con herramientas del ccn-cert: 01/05/2022 al 15/08/2022.**
   - **Ampliación de control de seguridad en los accesos a los sistemas: 01/05/2022-15/05/2022.**
3. **Plan de pruebas**
   - **Integración con herramientas del ccn-cert: 15/08/2022-15/08/2022**
   - **Ampliación de control de seguridad en los accesos a los sistemas:15/05/2022-01/06/2022**
4. **Documentación y generación de informes:**
   - **Integración con herramientas del ccn-cert: 15/08/2022-31/08/2022**
   - **Ampliación de control de seguridad en los accesos a los sistemas: 01/06/2022-01/07/2022.**
5. **Formación 01/05/2022-31/10/2022**
6. **Pago y justificación del proyecto: Hasta 31/12/2022.**

13.-DISTRIBUCIÓN ANUAL DEL COSTE TOTAL ESTIMADO DEL PROYECTO

COSTE TOTAL	2020	2021	2022
	0	**0**	**107.049,50€**

14.-CRONOGRAMA GENERAL DEL PROYECTO

Se adjunta el cronograma de las principales tareas a realizar y su temporización

	MES 1	MES 2	MES 3	MES 4	MES 5	MES 6	MES 7	MES 8	MES 9	MES 10	MES 11	MES 12
Publicación de actuaciones												
Licitación												
Reunión de lanzamiento												

Hito 1. Actuación A1												
1. Instalación y despliegue de herramienta LUCIA												
1.1Insalación de instancia, configuración de políticas y perffiles												
1.2. Integración con SIEM y test de integración												
2. Despliegue herramienta microClaudia												
Hito 2. Actuación A1												
3.1. Suministro e instalación firewall												
3.2. Configuración y pruebas												
3.3. Documentación y formación												
Hito 2. Actuación A2												
4. Actualización y adecuación herramienta logICA												
4.1. Identificación de fuentes y arquitectura												
4.2. Elaboración de catálogo de reglas personalizadas												
4.3. Despliegue de configuración actualizada												
4.4. Plan de pruebas												
4.5. Generación de informes												
Hito 3. Actuación A1												

6.1.Plan de concienciación												
6.2. Plan de formación												
Campaña de difusión y comunicación												
Pago y justificación de la actuación												

15.-OBJETIVOS QUE PRETENDE ALCANZAR	
Objetivos del PRTR (marcar con una X)	Descripción de cómo desarrolla el proyecto los objetivos señalados
Obj 1. Promueve la cohesión económica, social y territorial de la UE (X)	El proyecto enmarcado en la línea 5 de Ciberseguridad contribuye a la protección tanto de la Entidad como a nivel nacional y europeo frente a amenazas de ciberseguridad, reforzando así las capacidades de prevención y reacción a nivel de la UE ante incidentes de seguridad, incrementando la capacidad de vigilancia y detección de ciberamenazas de un modocentralizado más eficiente promoviendo así la cohesión económica y territorial, al gestionar la seguridad de todas las entidades de manera centralizada
Obj 2. Fortalecer la resiliencia y la capacidad de ajuste de los Estados miembros (X)	Este proyecto va a contribuir a aumentar la resiliencia ante amenazas cibernéticas cada vez mayores y a mantener la seguridad y protección de la sociedad y de la economía digital, mejorando la resiliencia y las capacidades de respuesta ante incidentes tanto del sector público como del privado y de la UE en su conjunto.
Obj 3. Mitigar las repercusiones sociales y	La pandemia ha provocado en las AALL la aceleración de la transformación digital de

económicas de la crisis de la COVID 19 (X)	sus procesos y trámites, ya que la digitalización de los servicios públicos es clave para seguir atendiendo a los ciudadanos en todas sus necesidades sin necesidad de presencialidad. En este sentido está aumentando la probabilidad que tienen las AALL de ser víctimas de ciberataques y de que estos puedan tener un impacto sustancial, debido a que los ciberdelincuentes están aprovechando la incertidumbre actual de este escenario sin precedentes, por ello este proyecto va a permitir a la Entidad dotarse de instrumentos de protección frente a amenazas de ciberseguridad, reforzar las capacidades de prevención y reacción ante incidentes de seguridad e incrementar la capacidad de vigilancia y detección de ciberamenazas de un modo centralizado más eficiente , garantizado que los trámites que realiza con sus ciudadanos y empresas son seguros.
Obj 4. Apoya las transiciones ecológica y digital (X)	La seguridad es pieza clave, en el proceso de transición digital, ya que a través de los canales digitales se expone información sensible. Este Proyecto es clave para la Entidad ya que en su proceso de transición digital debe proteger los datos asegurando el cumplimiento normativo en materia de protección de datos y seguridad, además de protegerse frente a las ciberamenazas incorporando sistemas de almacenamiento seguro de la información y backups, así como desplegar aplicaciones de protección de la red corporativa, y de navegación segura de los empleados, para que la transición se realice en un entorno confiable y seguro.

Objetivos del Componente 11 del PRTR (marcar con una X)	Descripción de cómo desarrolla el proyecto los objetivos señalados
Obj 1. Mejora la accesibilidad de los servicios públicos digitales a los ciudadanos y empresas (X)	Este proyecto supone una iniciativa que va a mejorar el acceso y la accesibilidad de los servicios del Ayuntamiento a los ciudadanos/empresas, ya que cualquier intercambio de información estará securizado, dependiendo de forma transversal de la infraestructura tanto a nivel físico como lógico A nivel físico cualquier conexión con el Ayuntamiento entrante o saliente será analizada para evitar intrusiones y aislar conexiones potencialmente peligrosas y prever posibles tiempos de indisponibilidad mediante asignación de cuotas de servicios (QoS - Quality of service).
Obj 2. Reduce la brecha digital (X)	Este proyecto va a capacitar a empleados públicos en materia de ciberseguridad, dotándolos de las competencias necesarias para afrontar con garantías los nuevos retos planteados por los escenarios novedosos en Ciberseguridad, reduciendo así la brecha digital existente en esta materia en la Entidad.
Obj 3. Mejora la eficiencia y eficacia de los empleados públicos (X)	Implementar un modelo integral de ciberseguridad que centralice y favorezca la coordinación interdepartamental ante incidentes de seguridad, mejorar las capacidades de vigilancia, prevención, detección, análisis y respuesta ante incidentes de ciberseguridad, aumentar la compartición e intercambio de inteligencia de ciberseguridad y mejorar la formación/conocimiento de los empleados, va a reforzar las capacidades de la Entidad/empleados, haciéndolos más

	eficientes y eficaces en el desempeño de su trabajo.
Obj 4. Reutiliza los servicios y soluciones digitales construidas (X)	El proyecto enmarcado en esta línea, es una iniciativa que pivota sobre soluciones que ya existen en el mercado y que sólo requerirían una adaptación a las necesidades concretas de nuestra Entidad, procediéndose a la adecuación de la herramienta existente SIEM a la normativa vigente.

OBJETIVOS DEL PLAN DE DIGITALIZACIÓN DE LAS AAPP (PDAP)	
Objetivos del PDAP (marcar con una X)	**Descripción de cómo desarrolla el proyecto los objetivos señalados**
Obj 1. Incrementar el número de procedimientos digitales (X)	
Obj 2. Incremento del número de servicios públicos para implementar en app ()	
Objetivos del Eje 3 del PDAP (marcar con una X)	**Descripción de cómo desarrolla el proyecto los objetivos señalados**
Obj 1. Administración Orientada a la ciudadanía ()	
Obj 2. Automatización inteligente de procesos ()	
Obj 3. Transparencia y política basadas en datos ()	
Obj 4. Entornos Digitales Líquidos ()	
Obj 5. Ciberseguridad **(X)**	El Ayuntamiento va a implementar medidas e instrumentos que le van a ayudar a reforzar las capacidades de prevención y reacción ante incidentes de seguridad, incrementando su capacidad de vigilancia y

	detección de ciberamenazas mediante la implementación de un modelo integral y centralizado más eficiente que implique un ahorro significativo de dinero, esfuerzo y tiempo, garantizando la seguridad de las infraestructuras, comunicaciones y servicios digitales prestados por la Entidad, unido a las mejores capacidades y competencias de sus empleados en la materia, lo que va a ayudar también a mejorar su capacidad de comunicación de incidentes de seguridad con el Centro Criptológico Nacional

ALINEAMIENTO CON LOS HITOS Y OBJETIVOS DEL COMPONENTE 11.I3 DEL PRTR	
Propuesta de Objetivos	**Descripción**
OES1- Garantizar la seguridad de las infraestructuras, comunicaciones y servicios digitales prestados por la Entidad y mejorar las capacidades de prevención, detección y respuesta ante incidentes de ciberseguridad.	Incorporación de servicios horizontales de ciberseguridad que aumenten la capacidad de vigilancia y detección de amenazas en las transacciones de los sistemas de información y comunicaciones de la Entidad, mejora de su capacidad de respuesta ante posibles ataques y protección en el ámbito de la seguridad perimetral frente a ciberamenazas, así como su correcta configuración, administración, control y gestión.
OES2 – Implementar un modelo integral de Ciberseguridad en la Entidad.	Implantación de herramientas, procesos y servicios de vigilancia, prevención, detección, análisis, respuesta y asesoramiento que favorezcan la coordinación interdepartamental ante incidentes de seguridad complejos y la compartición e intercambio de inteligencia de ciberseguridad.
OES3 - Mejorar la situación de seguridad de la	Cumplimiento de la regulación en materia

Entidad y su grado de conocimiento.	de seguridad de la información, concretamente del Esquema Nacional de Seguridad (ENS) y poder habilitar mecanismos para obtener más visibilidad e información sobre vulnerabilidades, fallos de configuración e incidentes, a la vez que se mejoren las capacidades de protección y respuesta.
OES4- Mejorar la comunicación de incidentes de seguridad al Centro Citológico Nacional,	Implantación de herramientas de comunicación de incidencias que permitan la interrelación con el Centro Citológico Nacional.
OES5- Mejorar la formación y conocimientos de los técnicos del Ayuntamiento en materia de ciberseguridad	Desarrollo de un plan de sensibilización y formación para afrontar con garantías los nuevos retos planteados por los escenarios novedosos en Ciberseguridad
Propuesta de Hitos	**Descripción**
Hito 1- Integración con herramientas del CCN-CERT	Monitorización de Operaciones de Seguridad siendo necesario apoyarse en herramientas puestas a disposición por el CCN que aseguren las comunicaciones y los sistemas con las herramientas de reporte a tal efecto desplegadas.
Hito 2- Ampliación de control de seguridad en los accesos a los sistemas	Implantación de herramientas de seguridad perimetral en dos niveles de Cortafuegos (el cortafuegos de nivel uno se ocupa de la protección frente a las redes públicas y el cortafuegos de segundo nivel dos protege las infraestructuras de cómputo internas) para la protección tanto del perímetro exterior de la red como de las infraestructuras internas que proporcionan servicio al personal del ayuntamiento y a los ciudadanos, así como la adecuación de la herramienta existente SIEM de monitorización (gestor de eventos de

	seguridad) LogICA disponible
Hito 3- Plan de Formación técnica en materia de ciberseguridad	Desarrollo e implementación de un Plan de concienciación y Sensibilización, y formación, en el que se transformarán e interiorizarán comportamientos y hábitos en seguridad en el día a día de los empleados.