Plan de mejora de la seguridad del Ayuntamiento de la Universitat Oberta de Catalunya

Índice

1. Informe de Insuficiencias

A continuación, se muestra el grado de cumplimiento de las medidas del Anexo II del Real Decreto ENS a fecha 6 de Noviembre de 2020.

Las medidas se han evaluado conforme a la escala CMM:

CMM	DESCRIPCIÓN	EFECTIVIDAD
L0	Inexistente	0%
L1	Inicial / Ad hoc	10%
L2	Reproducible, pero intuitivo	50%
L3	Proceso definido	80%
L4	Gestionado y medible	90%
L5	Optimizado	100%

Se establecen los siguientes supuestos:

- **Servicios proporcionados directamente por el Ayuntamiento**, donde el Perfil de Cumplimiento Específico será de aplicación al sistema de información del Ayuntamiento.
- **Servicios del Ayuntamiento proporcionados por la Diputación Provincial, Cabildo, Consejo Insular o el órgano competente equivalente** (en adelante para referirse a estos, se indicará órgano competente), **o por proveedores contratados en la modalidad de software como servicio (SaaS), infraestructura como servicio (IaaS) o Plataforma como Servicio (PaaS)**. En este caso, será necesario que el órgano competente disponga de la conformidad del sistema de información que soporta los servicios en esta modalidad y el Perfil de Cumplimiento Específico se aplicará al Sistema de Información del Ayuntamiento desde el que se accede a los servicios.

Criterios de aplicación de medidas específicos (se marcan con asteriscos):

* En el caso de servicios del Ayuntamiento que son proporcionados por el órgano o proveedor competente, serán de aplicación al sistema de información del Ayuntamiento los requisitos de nivel BAJO, mientras que en el sistema de información del órgano o proveedor competente esta medida estará aplicada, al disponer éste de la conformidad ENS en categoría MEDIA.

** En el caso de servicios del Ayuntamiento que son proporcionados por el órgano o proveedor competente, no serán de aplicación al sistema de información del Ayuntamiento, mientras que en el sistema de información del órgano o proveedor competente esta medida estará aplicada al disponer éste de la conformidad ENS en categoría MEDIA.

Medidas de Seguridad		SERVICIO AYUNTAMIENTO		SERVICIO DEL AYUNTAMIENTO PROPORCIONADO POR ÓRGANO COMPETENTE		
		APLICA	SISTEMA AYUNTAMIENTO NIVEL DE MADUREZ ALCANZADO	APLICA	SISTEMA AYUNTAMIENTO NIVEL DE MADUREZ ALCANZADO	SISTEMA ÓRGANO COMPETENTE NIVEL DE MADUREZ ALCANZADO (MÍNIMO)
org.1	Política de seguridad	MEDIO	L0	MEDIO	L0	L3[1]
org.2	Normativa de seguridad	MEDIO	L0	MEDIO	L0	L3
org.3	Procedimientos de seguridad	MEDIO	L1	MEDIO	L1	L3
org.4	Proceso de autorización	MEDIO	L1	MEDIO	L1	L3
op.pl.1	Análisis de riesgos	MEDIO	L1	BAJO*	L1	L3
op.pl.2	Arquitectura de Seguridad	MEDIO	L1	MEDIO	L1	L3
op.pl.3	Adquisición de nuevos componentes	MEDIO	L2	MEDIO	L2	L3
op.pl.4	Dimensionamiento/ Gestión de capacidades	MEDIO	L2	n/a	-	L3
op.pl.5	Componentes certificados	n/a	-	n/a	-	-
op.acc.1	Identificación	MEDIO	L2	MEDIO	L2	L3
op.acc.2	Requisitos de acceso	MEDIO	L2	MEDIO	L2	L3
op.acc.3	Segregación de funciones y tareas	MEDIO	L1	n/a	-	L3
op.acc.4	Protección de gestión de derechos de acceso	MEDIO	L2	MEDIO	L2	L3
op.acc.5	Mecanismo de autenticación	MEDIO	L2	MEDIO	L2	L3
op.acc.6	Acceso local (local logon)	MEDIO	L2	MEDIO	L2	L3
op.acc.7	Acceso remoto (remote login)	MEDIO	L2	MEDIO	L2	L3
op.exp.1	Inventario de activos	MEDIO	L1	MEDIO	L1	L3
op.exp.2	Configuración de seguridad	MEDIO	L2	MEDIO	L2	L3
op.exp.3	Gestión de la configuración de seguridad	MEDIO	L1	MEDIO	L1	L3
op.exp.4	Mantenimiento	MEDIO	L2	MEDIO	L2	L3
op.exp.5	Gestión de cambios	n/a	-	n/a	-	L3

1 L3 en todos los controles, si el sistema dispone de la conformidad ENS en categoría MEDIA.

Medidas de Seguridad		SERVICIO AYUNTAMIENTO		SERVICIO DEL AYUNTAMIENTO PROPORCIONADO POR ÓRGANO COMPETENTE		
		APLICA	SISTEMA AYUNTAMIENTO NIVEL DE MADUREZ ALCANZADO	APLICA	SISTEMA AYUNTAMIENTO NIVEL DE MADUREZ ALCANZADO	SISTEMA ÓRGANO COMPETENTE NIVEL DE MADUREZ ALCANZADO (MÍNIMO)
op.exp.6	Protección frente a código dañino	MEDIO	L2	MEDIO	L2	L3
op.exp.7	Gestión de incidentes	MEDIO	L1	MEDIO	L1	L3
op.exp.8	Registro de la actividad de los usuarios	MEDIO	L1	BAJO*	L1	L3
op.exp.9	Registro de la gestión de incidentes	MEDIO	L2	MEDIO	L2	L3
op.exp.10	Protección de los registros de actividad	n/a	-	n/a	-	-
op.exp.11	Protección de claves criptográficas	MEDIO	L1	MEDIO	L1	L3
op.ext.1	Contratación y acuerdos de nivel de servicio	MEDIO	L2	MEDIO	L3	L3
op.ext.2	Gestión diaria	MEDIO	L2	MEDIO	L3	L3
op.ext.9	Medios alternativos	n/a	-	n/a	-	-
op.cont.1	Análisis de impacto	n/a	-	n/a**	-	L3
op.cont.2	Plan de continuidad	n/a	-	n/a	-	-
op.cont.3	Pruebas periódicas	n/a	-	n/a	-	-
op.mon.1	Detección de intrusión	MEDIO	L3	MEDIO	L3	L3
op.mon.2	Sistema de métricas	MEDIO	L1	MEDIO	L1	L3
mp.if.1	Áreas separadas y con control de acceso	MEDIO	L1	MEDIO	L1	L3
mp.if.2	Identificación de las personas	MEDIO	L1	MEDIO	L1	L3
mp.if.3	Acondicionamiento de los locales	MEDIO	L2	MEDIO	L2	L3
mp.if.4	Energía eléctrica	MEDIO	L2	BAJO	L2	L3
mp.if.5	Protección frente a incendios	MEDIO	L2	MEDIO	L2	L3
mp.if.6	Protección frente a inundaciones	n/a	-	n/a**	-	L3
mp.if.7	Registro de entrada y salida de equipamiento	MEDIO	L2	MEDIO	L2	L3
mp.per.1	Caracterización del	n/a	-	n/a**	-	L3

Medidas de Seguridad		SERVICIO AYUNTAMIENTO		SERVICIO DEL AYUNTAMIENTO PROPORCIONADO POR ÓRGANO COMPETENTE		
		APLICA	SISTEMA AYUNTAMIENTO NIVEL DE MADUREZ ALCANZADO	APLICA	SISTEMA AYUNTAMIENTO NIVEL DE MADUREZ ALCANZADO	SISTEMA ÓRGANO COMPETENTE NIVEL DE MADUREZ ALCANZADO (MÍNIMO)
	puesto de trabajo					
mp.per.2	Deberes y obligaciones	MEDIO	L3	MEDIO	L3	L3
mp.per.3	Concienciación	MEDIO	L1	MEDIO	L1	L3
mp.per.4	Formación	MEDIO	L1	MEDIO	L1	L3
mp.per.9	Personal alternativo	n/a	-	n/a	-	-
mp.eq.1	Puesto de trabajo despejado	MEDIO	L1	MEDIO	L1	L3
mp.eq.2	Bloqueo de puesto de trabajo	MEDIO	L2	MEDIO	L2	L3
mp.eq.3	Protección de dispositivos portátiles	MEDIO	L1	MEDIO	L1	L3
mp.eq.9	Medios alternativos	n/a	-	n/a	-	-
mp.com.1	Perímetro seguro	MEDIO	L3	MEDIO	L3	L3
mp.com.2	Protección de la confidencialidad	MEDIO	L1	MEDIO	L1	L3
mp.com.3	Protección de la autenticidad y de la integridad	MEDIO	L1	MEDIO	L1	L3
mp.com.4	Separación de redes	ALTO	L2	ALTO	L2	L3
mp.com.9	Medios alternativos	n/a	-	n/a	-	-
mp.si.1	Etiquetado	MEDIO	L1	MEDIO	L1	L3
mp.si.2	Criptografía	MEDIO	L1	MEDIO	L1	L3
mp.si.3	Custodia	MEDIO	L1	MEDIO	L1	L3
mp.si.4	Transporte	MEDIO	L1	MEDIO	L1	L3
mp.si.5	Borrado y destrucción	MEDIO	L1	MEDIO	L1	L3
mp.sw.1	Desarrollo de aplicaciones	n/a	-	MEDIO	L2	L3
mp.sw.2	Aceptación y puesta en servicio	n/a	-	MEDIO	L2	L3
mp.info.1	Datos de carácter personal	MEDIO	L1	MEDIO	L1	L3
mp.info.2	Calificación de la información	MEDIO	L1	MEDIO	L1	L3
mp.info.3	Cifrado	n/a	-	n/a	-	-
mp.info.4	Firma electrónica	MEDIO	L1	MEDIO	L1	L3
mp.info.5	Sellos de tiempo	ALTO	L1	ALTO	L1	L3
mp.info.6	Limpieza de documentos	MEDIO	L1	MEDIO	L1	L3
mp.info.9	Copias de	MEDIO	L2	MEDIO	L2	L3

		SERVICIO AYUNTAMIENTO		SERVICIO DEL AYUNTAMIENTO PROPORCIONADO POR ÓRGANO COMPETENTE		
Medidas de Seguridad		APLICA	SISTEMA AYUNTAMIENTO NIVEL DE MADUREZ ALCANZADO	APLICA	SISTEMA AYUNTAMIENTO NIVEL DE MADUREZ ALCANZADO	SISTEMA ÓRGANO COMPETENTE NIVEL DE MADUREZ ALCANZADO (MÍNIMO)
	seguridad					
mp.s.1	Protección del correo electrónico	MEDIO	L1	MEDIO	L1	L3
mp.s.2	Protección de servicios y aplicaciones web	MEDIO	L2	n/a**	-	L3
mp.s.8	Protección frente a denegación de servicio	MEDIO	L2	n/a**	-	L3
mp.s.9	Medios alternativos	n/a	-	n/a	-	-

2. Plan de mejora de la seguridad

2.1. Objeto del documento

El propósito de este documento es proponer un plan de medidas de seguridad (“Plan de Mejora de la Seguridad) a llevar a cabo para subsanar las desviaciones de cumplimiento de lo dispuesto en el Esquema Nacional de Seguridad.

La responsabilidad de su ejecución y la provisión de recursos recaen sobre el Ayuntamiento de la Universitat Oberta de Catalunya ya sean propios o mediante externalización. El RSEG se encargará de la supervisión de su ejecución. Las tareas realizar se organizan en tres grupos:

- **Tareas priorizadas:** tareas que se deben abordar inicialmente, ya sea fruto del análisis de riesgos, o porque presentan un cumplimiento muy bajo, o por tratarse de un incumplimiento normativo.
- **Tareas de implantación ENS:** resto de tareas que es necesario llevar a cabo para realizar la implantación efectiva del ENS. Para ello, se irán revisando/implantando y documentando las medidas de seguridad, siguiendo el orden establecido en el anexo II del Real Decreto ENS. De esta manera, se va implantado el Sistema de Gestión que dará cumplimiento a estas medidas.
- **Tareas periódicas:** tareas para llevar a cabo aquellas medidas de seguridad que se deben realizar de forma periódica.

2.2. Plan de Mejora de la Seguridad

2.2.1. Tareas Prioritarias

Leyenda: RINFSER (Responsable/s de Información y Servicio/s); RSEG (Responsable de Seguridad); RSIS (Responsable del Sistema); CSI (Comité de Seguridad de la Información); T (Trimestre); RESPONSABLE (Responsable de que la tarea se lleve a cabo).

Las siguientes tareas se abordarán de forma prioritaria, son las que se exponen a continuación.

TAREAS PRIORITARIAS	CONTROL/ CUMPLIMIENTO	RESPONSABLE	T1	T 2	T 3	T 4
Desarrollar la Política de seguridad (pertenece al plan de adecuación): designación de roles de seguridad y constituir el CSI. Publicar en el Boletín Oficial de la Provincia, sede electrónica/portales internos vinculados con la difusión de iniciativas de seguridad. En caso de servicios externalizados en órgano competente designar Responsable/s de la Información y Responsable de Servicio/s, acogerse a la Política de seguridad del órgano competente.	Política de seguridad de la Información [org.1]	CSI	X			
Categorizar el sistema (pertenece al plan de adecuación): realizar y aprobar la valoración de los Servicios y la Información. Determinar la categoría del sistema	Artículo 43. Categorías y 44. Facultades del Real Decreto ENS	RINFSER/RSIS	X			
Realizar el Análisis de Riesgos (pertenece al plan de adecuación) informes asociados y aceptar los riesgos residuales	Análisis de riesgos [op.pl.1]	RINFSER RSEG,RSIS	X			
Realizar la Declaración de aplicabilidad (pertenece al plan de adecuación)	Artículo 27. Cumplimiento de requisitos mínimos. 2. Selección de medidas de seguridad - ANEXO II Medidas de seguridad	RSEG	X			
Realizar al Informe de Insuficiencias (pertenece al plan de adecuación) y el Plan de mejora de la seguridad	Disposición transitoria. *Adecuación de sistemas*	RSEG,RSIS/CSI	X			

TAREAS PRIORITARIAS	CONTROL/ CUMPLIMIENTO	RESPONSABLE	T1	T 2	T 3	T 4
Desarrollar y aprobar la normativa de seguridad de los recursos TIC (correo, internet, etc.) puestos a disposición del personal que regule también, entre otros, el uso de dispositivos portátiles, soportes extraíbles, la necesidad de que los usuarios bloqueen su puesto de trabajo ante las ausencias, la necesidad de limpiar los documentos de metadatos no necesarios, etc. Aprobar formalmente y difundir a todo personal: publicación en el portal del empleado. Elaborar de plan anual de difusión/sensibilización y de formación.	Normativa de seguridad [org.2] Puesto de trabajo despejado [mp.eq.1] Bloqueo de puesto de trabajo [mp.eq.2] Protección de dispositivos portátiles [mp.eq.3] Protección de los soportes [mp.si] Limpieza de metadatos [mp.info.6] Concienciación [mp.per.3] Formación [mp.per.4]	RSEG/CSI	X	X		
Desarrollar e implantar un procedimiento de gestión de la seguridad con terceros: antes, durante y después de la contratación: Requisitos de solvencia técnica. Exigencia de declaración/certificación de conformidad con el ENS, contratos de encargado del tratamiento de datos personales y/o confidencialidad, acuerdos de nivel de servicio, etc. Inventariar terceros y regular su situación. En caso de servicios externalizados: completar con certificados de Conformidad ENS de los servicios subcontratados por el órgano competente. Para la gestión diaria completar con los Informes/herramientas seguimiento SLA proporcionadas por el órgano competente	Contratación y acuerdos de nivel de servicio [op.ext.1] Gestión diaria [op.ext.2]	CSI	X	X		
Revisar las medidas de protección frente a código dañino, en todo el equipamiento incluido: el de las sedes, portátiles, etc. Se recomienda implementar soluciones medidas EDR (Endpoint Defense and Response) Desarrollar un procedimiento que describa la forma en cual se gestiona y se mantiene la solución de protección frente a código dañino	Protección frente a código dañino [op.exp.6]	RSIS	X			
Segmentar las redes de tal forma que cada equipo solamente tenga acceso a la información que necesita, se compartimenten los diferentes grupos de usuarios para evitar la propagación de malware y las redes inalámbricas disponga de su propio segmento de red. Desarrollar los procedimientos asociados	Segregación de redes [mp.com.4]	RSIS	X	X		

TAREAS PRIORITARIAS	CONTROL/ CUMPLIMIENTO	RESPONSABLE	T1	T 2	T 3	T 4
Asegurarse de que todos los usuarios o procesos disponen de un identificador único. Establecer un “periodo de retención” de las cuentas. Desarrollar un procedimiento de control de acceso detallando los mecanismos de identificación implementados En caso de servicios externalizados: completar con los procedimientos documentados proporcionados por el órgano competente de configuración de roles/perfiles de acceso a los servicios	Identificación [op.acc.1]	RSIS	X	X		
Desarrollar e implementar una Política de acceso desarrollando un procedimiento de gestión de los derechos de acceso cumpliendo el requisito de “mínimo privilegio”. Realizar controles aleatorios de cumplimiento. Registrar estas acciones y sus resultados. Desarrollar un procedimiento de gestión de los derechos de acceso, que garantice que se asignan los mínimos privilegios y que son acordes a los establecidos para el control Requisitos de acceso [op.acc.2] y establecer tareas periódicas de revisión de los permisos otorgados. En caso de servicios externalizados: completar con los procedimientos documentados proporcionados por el órgano competente de configuración de roles/perfiles de acceso a los servicios	Requisitos de acceso [op.acc.2] Proceso de gestión de los derechos de acceso [op.acc.4]	RSIS, CSI	X	X		
Desarrollar Instrucciones Técnicas de configuración segura (bastionado) de los principales componentes del sistema: equipamiento (seguridad perimetral, electrónica de red, servidores (físicos, virtuales), bases de datos), equipos de usuarios (PC, portátiles, Smartphone, tabletas), dispositivos conectados a la red (impresoras, etc.) Migrar los sistemas obsoletos (Windows XP, 2003 Server, etc.) a sistemas que dispongan de soporte de seguridad	op.exp.2 Configuración de Seguridad op.exp.3 Gestión de la configuración Protección de equipos portátiles [mp.eq.3]	RSIS		X	X	
Revisar el procedimiento de copias y asegurarse que las políticas implementadas respaldan toda la información, aplicaciones, logs, etc. En caso de servicios externalizados: completar con procedimientos documentados proporcionados por el órgano competente de la política de copias de seguridad y de restauración	mp.info.9 Copias de seguridad (back up)	RSIS	X			
Instalar la herramienta Lucia herramienta desarrollada por el CCN-CERT para la Gestión de Ciberincidentes. Completar la instalación con las sondas que ofrece (Internet y Red SARA). Instalar un IDS de red Desarrollar un procedimiento integral de gestión de incidentes de seguridad con las obligaciones establecidas por el ENS y RGPD En caso de servicios externalizados: completar con los procedimientos documentados de coordinación con el Ayuntamiento para la gestión incidentes y de comunicación de los mismos a las autoridades de control	Gestión de incidentes [op.exp.7] Registro de la gestión de incidentes [op.exp.9] op.mon.1 Detección de Intrusión	RSEG	X	X		

TAREAS PRIORITARIAS	CONTROL/ CUMPLIMIENTO	RESPONSABLE	T1	T 2	T 3	T 4
Implementar un mecanismo de acceso al CPD que permita identificar a las personas (incluido el acceso de terceros). Desarrollar el procedimiento asociado Revisar las medidas de acondicionamiento del CPD. Implantar un registro de entrada/salida de equipamiento al CPD. Desarrollar el procedimiento asociado.	Identificación de las personas [mp.if.2] Acondicionamiento de los locales [mp.if.3] Registro de entrada y salida de equipamiento [mp.if.7]	RSIS		X		
Habilitar registros de las actividades de los usuarios realizadas sobre el Sistema, de forma que Indique quien las realiza, cuándo y sobre qué información. Desarrollar procedimiento asociado. Especialmente los de los administradores del sistema para monitorizar su actividad como medida compensatoria de op.acc.3 (en caso de que sea de aplicación). En caso de servicios externalizados: completar con procedimientos documentados de configuración de los registros de actividad de los usuarios a los servicios Información/plataforma de visualización proporcionada por el órgano competente de los accesos de los administradores del sistema que soporta los servicios (en caso de que se hayan requerido) Implantar un sistema automático de recolección de eventos de seguridad. Valorar que permita la correlación de los mismos. (herramienta GLORIA CCN)	Registros de la actividad de los usuarios [op.exp.8] Segregación de funciones y tareas [op.acc.3]	RSIS		X	X	
Para servicios proporcionados directamente por el Ayuntamiento: • En caso de realizar desarrollo de Software utilizar metodologías de desarrollo reconocido y seguro. Desarrollar los procedimientos asociados. Realizar acciones formativas. • En caso de que se encargue a terceros desarrollo de software, solicitar que se utilicen metodologías de desarrollo seguro y que satisfagan los requisitos necesarios para cumplir con el ENS. • En caso de adquirir software para instalación en modo local solicitad la conformidad con el ENS, en categoría MEDIA, y los requisitos adicionales requeridos por el “Abstract- Requisitos de Seguridad Adicionales para Soluciones en la Nube (SaaS) implementadas en Modo Local”	Desarrollo [mp.sw.1] Formación [mp.per.4]	CSI			X	X

TAREAS PRIORITARIAS	CONTROL/ CUMPLIMIENTO	RESPONSABLE	T1	T 2	T 3	T 4
Para servicios proporcionados directamente por el Ayuntamiento: • Desarrollar e implantar un procedimiento donde se definan las pruebas, a realizar antes de la puesta en producción de las aplicaciones o bien solicitar al órgano competente en caso de que estos proporcionen este servicio. • Se recomienda realizar test de intrusión y análisis de vulnerabilidades, para todas las aplicaciones que ya están puestas en producción. • Para los servicios y las aplicaciones web, además realizar pruebas de las amenazas que son propias de este entorno, realizar test de intrusión. • Para los servicios web y aplicaciones web emplear "certificados de autenticación de sitio web" acordes a la normativa europea en la materia. En caso de servicios externalizados: recopilar los procedimientos documentados proporcionados por el órgano competente de coordinación con el Ayuntamiento para la realización de pruebas de aceptación y puesta en servicio. Informes resultados pruebas y plan de acción y los Informes proporcionados por el órgano competente con resultados de las inspecciones periódicas realizadas y plan de acción	Aceptación y puesta en servicio [mp.sw.2] Protección de los servicios y aplicaciones web [mp.s.2]	RSIS			X	X
Identificar los mecanismos de autenticación de cada recurso y documentar como se encuentra implementado el doble factor de autenticación. Desarrollar el procedimiento asociado. Si se utilizan contraseñas: utilizar contraseñas seguras, definir una política de caducidad. Inventariar los accesos remotos. Realizar un procedimiento que permita mantener este inventario, cómo se autorizan, etc. Realizar unas normas para los accesos remotos que regulen las condiciones en las cuales debe realizare este acceso. Revisar que los accesos remotos, se realizan, implementando doble factor de autenticación En caso de servicios externalizados: completar con pprocedimientos documentados proporcionados por el órgano competente de los mecanismos de autenticación de acceso a los servicios	Mecanismo de autenticación [op.acc.5] Acceso remoto (remote login) [op.acc.7]	RSIS	X	X		
Configurar las directivas de acceso al dominio de forma que: • Se establezca una limitación de intentos de acceso. • Solo se muestre información, una vez validado en el dominio, por tanto, no se guardará la información del último usuario validado. • Se informe al usuario de sus obligaciones. • Se muestre la información sobre el último acceso con éxito y los posibles intentos de acceso. En caso de servicios externalizados: completar con procedimientos documentados proporcionados por el órgano competente de configuración de los requisitos del control: limitación de intentos de acceso, aviso de obligaciones, información sobre el último acceso	Acceso local (local logon) [op.acc.6]	RSIS	X	X		

2.2.2. Tareas de implantación del ENS

Durante los siguientes ciclos se procederá a implantar y documentar el resto de medidas. Descripción detallada de la tareas:

TAREAS	CONTROL	RESPONSABLE	T1	T2	T3	T4
MARCO ORGANIZATIVO						
POLÍTICA DE SEGURIDAD-(incluido en medidas priorizadas)	org.1					
NORMATIVA DE SEGURIDAD-(incluido en medidas priorizadas)	org.2					
PROCEDIMIENTOS DE SEGURIDAD- Desarrollar procedimientos operativos que recojan las principales tareas sobre el sistema. Indicando los responsables de su realización y cómo identificar y reportar comportamientos anómalos. Integrar en un Sistema de Gestión de Seguridad de la Información que de soporte al cumplimiento del ENS. (SGSIENS)	org.3	RSEG RSIS	X	X	X	X
PROCESOS DE AUTORIZACIÓN- Implantar y documentar un proceso de autorización para la introducción de elementos en el sistema: instalaciones, equipos, aplicaciones, medios de comunicación, utilización de soportes, portátiles, móviles, etc. y servicios de terceros.	org.4	RSIS		X		
MARCO OPERACIONAL - PLANIFICACIÓN						
ANÁLISIS DE RIESGOS ENS – (incluido en medidas priorizadas). Desarrollar el procedimiento de análisis de riesgos acorde a la categoría del sistema	op.pl.1	RSEG RSIS				X
ARQUITECTURA DE SEGURIDAD- Recopilar, organizar, completar y mantener actualizada documentación sobre: áreas y puntos de acceso, del sistema, líneas de defensa, identificación y autenticación, controles técnicos, relaciones con terceros, para que formen parte del SGSENS. En caso de servicios externalizados: completar con la documentación proporcionada por el órgano competente sobre las comunicaciones con el Ayuntamiento, y con otros sistemas interconectados comunicaciones con el Ayuntamiento, y con otros sistemas interconectados	op.pl.2	RSIS		X	X	
ADQUISICIÓN DE NUEVOS COMPONENTES- Implantar un procedimiento que analice los riesgos, evalúe la necesidad de requisitos antes de la adquisición de nuevos componentes. Registrar estas acciones y sus resultados.	op.pl.3	RSIS		X		
DIMENSIONAMIENTO Y GESTIÓN DE LA CAPACIDAD - - Implantar un procedimiento para la realización de un estudio de estos parámetros antes de la entrada en producción de nuevos elementos. En caso de servicios externalizados: completar con la documentación regular proporcionada por el órgano competente sobre los recursos disponibles y consumidos	op.pl.4	RSIS		X		
MARCO OPERACIONAL – CONTROL DE ACCESO						
IDENTIFICACIÓN- (incluido en medidas priorizadas)	op.acc.1					
REQUISITOS DE ACCESO- (incluido en medidas priorizadas)	op.acc.2					
SEGREGACIÓN DE FUNCIONES Y TAREAS- (en caso de que sea de aplicación)- Elaborar un procedimiento documento de asignación de tareas con indicación de las tareas críticas y la incompatibilidad entre estas. – Medida compensatoria en caso de que sea necesario incluido en incluido en medidas priorizadas	op.acc.3	RSIS				X

TAREAS	CONTROL	RESPONSABLE	T1	T2	T3	T4
PROCESO DE GESTIÓN DE LOS DERECHOS DE ACCESO-(incluido en medidas priorizadas).	op.acc.4					
MECANISMOS DE AUTENTICACIÓN- (incluido en medidas priorizadas).	op.acc.5					
ACCESO LOCAL (local logon)- (incluido en medidas priorizadas).	op.acc.6					
ACCESO REMOTO (remote login)- (incluido en medidas priorizadas).	op.acc.7					
MARCO OPERACIONAL – EXPLOTACIÓN						
INVENTARIO DE ACTIVOS- Desarrollar un procedimiento que describa la forma en la que se gestionan los activos. Realizar un inventario de software (se recomienda utilizar una herramienta que realice un inventario de activos hardware, software de forma automática).	op.exp.1	RSIS			X	
CONFIGURACIÓN DE SEGURIDAD)- (incluido en medidas priorizadas). Elaborar un procedimiento de bastionado que recoja la configuración básica de seguridad del equipamiento (seguridad perimetral, electrónica de red, servidores (físicos, virtuales), bases de datos), equipos de usuarios (PC, portátiles, Smartphone, tabletas), dispositivos conectados a la red (impresoras, etc.), antes de entrar en operación.	op.exp.2	RSIS		X	X	X
GESTIÓN DE LA CONFIGURACIÓN DE SEGURIDAD- (incluido en medidas priorizadas). Establecer revisiones periódicas de la configuración de la seguridad: identificar vulnerabilidades, incidencias, etc. Registrar estas acciones y sus resultados.	op.exp.3	RSIS			X	
MANTENIMIENTO - Documentar todas las acciones de mantenimiento (físico y lógico). Registrar estas acciones y sus resultados. Desarrollar un procedimiento para analizar, prioridad la aplicación de actualizaciones de seguridad, parches, mejoras, etc. En caso de servicios externalizados: completar con procedimientos documentados de coordinación con el Ayuntamiento para realizar acciones de mantenimiento sobre el sistema.	op.exp.4	RSIS			X	
GESTIÓN DE CAMBIOS – En caso de servicios externalizados: recopilar la información aportada por el la órgano competente de coordinación con el Ayuntamiento para realizar cambios sobre el sistema que soporta los servicios	op.exp.5	RSIS			X	
PROTECCIÓN FRENTE A CÓDIGO DAÑINO- (incluido en medidas priorizadas).	op.exp.6					
GESTIÓN DE INCIDENTES- (incluido en medidas priorizadas).	op.exp.7					
REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS – [Incluido en medidas priorizadas}	op.exp.8					
REGISTRO DE LA GESTIÓN DE INCIDENCIAS- (incluido en medidas priorizadas).	op.exp.9					
PROTECCIÓN DE LAS CLAVES CRIPTOGRÁFICAS- Documentar las medias de seguridad implementadas para garantizar la protección de las claves criptográficas durante todo su ciclo de vida. Para sistemas de categoría media se asegurará la utilización de programas evaluados o dispositivos criptográficos evaluados que empleen algoritmos acreditados por el CCN. En caso de servicios externalizados: completar con procedimientos documentados de protección de las claves criptográficas del Ayuntamiento que se encuentren alojadas en el sistema que soporta los servicios	op.exp.11	RSIS				X
MARCO OPERACIONAL – SERVICIOS EXTERNOS						
CONTRATACIÓN Y ACUERDOS DE NIVEL DE SERVICIO - (incluido en medidas priorizadas)	op.ext.1					
GESTIÓN DIARIA - (incluido en medidas priorizadas)	op.ext.2					
MARCO OPERACIONAL – MONITORIZACIÓN DEL SISTEMA						
DETECCIÓN DE INTRUSIÓN – (incluido en medidas priorizadas)	op.mon.1					
MARCO OPERACIONAL – SISTEMA DE MÉTRICAS						
SISTEMA DE MÉTRICAS – Realizar un procedimiento que establezca los indicadores, métrica asociada y designación de responsables para su recopilación de los elementos para dar respuesta a la encuesta INES (re-querido por el artículo 35).	op.mon.2	RSIS				X
MARCO DE PROTECCIÓN – PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURAS						

TAREAS	CONTROL	RESPONSABLE	T1	T2	T3	T4
ÁREAS SEPARADAS Y CONTROL DE ACCESO- Realizar un procedimiento que contengan un inventario de todas las áreas donde se concentra el sistema de información y que detalle los mecanismos implementados en cada caso para controlar el acceso a las mismas y las autorizaciones pertinentes en caso de que sea necesario	mp.if.1	RSIS				X
IDENTIFICACIÓN DE LAS PERSONAS- (incluido en medidas priorizadas).	mp.if.2					
ACONDICIONAMIENTO DE LOS LOCALES- Documentar las medidas implementadas para asegurar el acondicionamiento del CPD: sensores de temperatura, humedad, protección del cableado, etc. Cómo se monitorizan y responsables. -(incluido en medidas priorizadas).	mp.if.3	RSIS				X
ENERGÍA ELÉCTRICA- Documentar las medidas implementadas para garantizar el suministro eléctrico en el CPD. En caso de que sea de aplicación describir las medidas adicionales implementadas (SAI, grupo electrónico, la forma y cuando entran en funcionamiento, pruebas de contingencia realizadas para determinar los cálculos de tiempo.)	mp.if.4	RSIS				X
PROTECCIÓN FRENTE A INCENDIOS- Desarrollar un procedimiento que recoja la forma en la cual se protegen los locales conforme a la normativa industrial, la ubicación de los carteles, extintores, materiales no inflamables, etc. Los controles periódicos realizados, etc. Mantener de forma centralizada toda la documentación relacionada Mantener de forma centralizada toda la documentación relacionada)	mp.if.5	RSIS				X
REGISTRO DE ENTRADA Y SALIDA DE EQUIPAMIENTO- (incluido en medidas priorizadas)	mp.if.7					
MARCO DE PROTECCIÓN – GESTIÓN DE PERSONAL						
DEBERES Y OBLIGACIONES- Desarrollar un procedimiento de gestión de personal que describa la forma en la cual se trasladan los deberes al personal propio o de terceros.	mp.per.2	CSI				X
CONCIENCIACIÓN- (incluido en medidas priorizadas) Desarrollar un procedimiento que describa la cómo se desarrollará el Plan Concienciación en materia de seguridad de la información para todo el personal, con periodicidad anual. (Incluido también en medidas periodicidad anual)	mp.per.3	RSEG CSI				
FORMACIÓN– (incluido en medidas priorizadas) Desarrollar un procedimiento que describa la cómo se desarrollará el Plan de Formación específica en seguridad de la información para el personal con responsabilidad en la operación del sistema, con periodicidad anual. (Incluido también en medidas periodicidad anual)	mp.per.4	RSEG CSI				
MARCO DE PROTECCIÓN – PROTECCIÓN DE LOS EQUIPOS						
PUESTO DE TRABAJO DESPEJADO – (incluido en medidas priorizadas) Obligación recogida en la Normativa de seguridad [org.2]	mp.eq.1					
BLOQUEO DE PUESTO DE TRABAJO– (incluido en medidas priorizadas) Obligación recogida en la Normativa de seguridad [org.2]	mp.eq.2					
PROTECCIÓN DE LOS EQUIPOS PORTÁTILES-– (incluido en medidas priorizadas) Desarrollar un procedimiento que describa la forma en la que realizar el inventario de los equipos portátiles (incluido Smartphone, tabletas, etc.)	mp.eq.3	RSIS			X	
MARCO DE PROTECCIÓN – PROTECCIÓN DE LAS COMUNICACIONES						
PERÍMETRO SEGURO- Documentar la seguridad perimetral y las excepciones implementadas en los firewalls. Proceso de autorización y que describa la separación de flujos implementada.	mp.com.1	RSIS				X
PROTECCIÓN DE LA CONFIDENCIALIDAD- Realizar un procedimiento que describa la forma en la cual se protege la confidencialidad de la información cuanto esta discurre por redes fuera del propio dominio de seguridad. En caso de servicios externalizados: completar con documentos proporcionados por el órgano competente con información sobre los mecanismos de cifrado implementados en las comunicaciones.	mp.com.2	RSIS				X

TAREAS	CONTROL	RESPONSABLE	T1	T2	T3	T4
PROTECCIÓN DE LA AUTENTICIDAD Y DE LA INTEGRIDAD - Realizar un procedimiento/norma que establezca la necesidad de utilizar redes privadas virtuales para garantizar la autenticidad y la integridad de la información antes de su intercambio. En caso de servicios externalizados: completar con documentos proporcionados por el órgano competente con información sobre los mecanismos implementados para proteger la autenticidad y de la integridad	mp.com.3	RSIS				X
SEGMENTACIÓN DE REDES - (incluido en medidas priorizadas)	mp.com.4					
MARCO DE PROTECCIÓN – PROTECCIÓN DE LOS SOPORTES DE INFORMACIÓN						
ETIQUETADO–- Desarrollar un procedimiento para el etiquetado de soportes extraíbles conforme a la calificación de la información que contienen. Difundir al personal afectado.	mp.si.1	RSIS		X		
CUSTODIA- - Desarrollar un procedimiento para la custodia de soportes de información. Difundir al personal afectado.	mp.si.3	RSIS		X		
TRANSPORTE- - Desarrollar un procedimiento que describa las medidas de seguridad a aplicar durante el transporte a los soportes de información. Difundir al personal afectado.	mp.si.4	RSIS		X		
BORRADO Y DESTRUCCIÓN- Desarrollar un procedimiento que describa el procedimiento a seguir para el borrado y destrucción en función del soporte. Elaborar instrucción técnica de borrado y de destrucción	mp.si.5	RSIS		X		
MARCO OPERACIONAL – PROTECCIÓN DE LAS APLICACIONES INFORMÁTICAS						
DESARROLLO- - (incluido en medidas priorizadas)	mp.sw.1					
ACEPTACIÓN Y PUESTA EN SERVICIO-- (incluido en medidas priorizadas)	mp.sw.2					
MARCO OPERACIONAL – PROTECCIÓN DE LA INFORMACIÓN						
DATOS DE CARÁCTER PERSONAL – Desarrollar las acciones de seguridad necesarias para llevar a cabo la implantación de la normativa de protección de datos (RAT, designación DPD, Análisis de Riegos RGPD, Evaluación de Impacto, contratos de encargado del tratamiento, alinear medidas de seguridad con las del ENS). En caso de servicios externalizados: recopilar documentos /plataformas online, proporcionados por el órgano competente, con evidencias de cumplimiento de la normativa de protección de datos	mp.info.1	CSI	X	X	X	X
CALIFICACIÓN DE LA INFORMACIÓN - Desarrollar e implantar un procedimiento de calificación de la información. Elaborar procedimientos que definan la forma que hay que tratar la documentación en consideración al nivel de seguridad requerido	mp.info.2	CSI				X
FIRMA ELECTRÓNICA – - Desarrollar, aprobar y dar publicidad a la Política de Firma Electrónica. Realizar un procedimiento que recoja los requisitos que deben cumplir los mecanismos de firma electrónica En caso de servicios externalizados: completar con documentos proporcionados por el órgano competente con información sobre las medidas de protección de la firma implementadas	mp.info.4	CSI			X	X
SELLOS DE TIEMPO –- Realizar un procedimiento que recoja los requisitos que deben cumplir los mecanismos de sello electrónico En caso de servicios externalizados: recopilar documentos proporcionados por el órgano competente con información sobre las medidas de seguridad implementadas para proteger el sello de tiempo	mp.info.6					
LIMPIEZA DE DOCUMENTOS- Desarrollar e Implantar un procedimiento donde se establezca la forma en la cual se ha de proceder para la limpieza de los documentos electrónicos.	mp.info.6	CSI			X	
COPIA DE SEGURIDAD- (incluido en medidas priorizadas)	mp.info.9					
MARCO OPERACIONAL – PROTECCIÓN DE LOS SERVICIOS						

TAREAS	CONTROL	RESPONSABLE	T1	T2	T3	T4
PROTECCIÓN DEL CORREO ELECTRÓNICO- Desarrollar un procedimiento que describa la forma en la cual se protege el correo.	mp.s.1	RSIS			X	
PROTECCIÓN DE SERVICIOS Y APLICACIONES WEB - (incluido en medidas priorizadas)	mp.s.2	RSIS				X
PROTECCIÓN FRENTE A LA DENEGACIÓN DE SERVICIO- – Documentar las medidas de seguridad implementadas. Realizar el procedimiento asociado.	mp.s.8	RSIS				X

2.2.3. Tareas Periódicas

TAREAS PERIODICIDAD ANUAL	CONTROL	PERIODICIDAD
Revisión de la Política de Seguridad de la Información	Política de Seguridad de la Información [org.1]	Anual
Elaboración del Plan de Concienciación y Plan de Formación	Concienciación [mp.per.3] Formación [mp.per.4]	Anual
Revisión de la Normativa de seguridad,	Normativa de seguridad [org.2]	Anual
Revisión de la Información y lo Servicios, su valoración y proceso de categorización del sistema	Artículo 43. Categorías y 44. Facultades del Real Decreto ENS	Permanente
Actualización del análisis de Riesgos	Análisis de riesgos [op.pl.1]	Anual/ cambios relevantes
Revisión de la Declaración de aplicabilidad o del Perfil de Cumplimiento	Artículo 27. Cumplimiento de requisitos mínimos. 2. Selección de medidas de seguridad -ANEXO II Medidas de seguridad	Anual
Realización de auditorías internas. Revisión de medidas de seguridad y procedimientos	Todos	Al menos anual
Revisión del Plan de Mejora de la Seguridad		Mensual/ Trimestral
Revisión del Estado de la Seguridad. INÉS	Artículo 35 Sistema de Métricas [op.mon.2]	Anual
Auditoría ENS (certificación conformidad ENS).	Artículo 34. Auditoría de la seguridad.	Bienal