

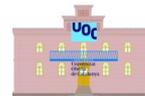


<https://flic.kr/p/ei5pSA> Attribution-ShareAlike 2.0 Generic
(CC BY-SA 2.0) - Se agrega el logotipo de la UOC

Declaración de Aplicabilidad del Ayuntamiento de la Universitat Oberta de Catalunya

Índice

1. OBJETIVO.....	3
2. SELECCIÓN DE MEDIDAS DE SEGURIDAD.....	3
3. DECLARACIÓN DE APLICABILIDAD PARA EL ENS.....	4
4. DECLARACIÓN DE APLICABILIDAD PARA ISO 27001:2013.....	23



1. Objetivo

El presente documento tiene por objeto dar cumplimiento al “Artículo 27. Cumplimiento de requisitos mínimos” del Capítulo 3 del ENS para el Ayuntamiento de la Universitat Oberta de Catalunya, entre los cuales se establece:

[...]

4. *La relación de medidas seleccionadas del Anexo II se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de seguridad.*

5. *Las medidas de seguridad referenciadas en el Anexo II podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos (Anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del real decreto. Como parte integral de la Declaración de Aplicabilidad se indicará de forma detallada la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II que compensan y el conjunto será objeto de la aprobación formal por parte del responsable de seguridad.*

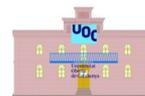
2. Selección de medidas de seguridad

Para la selección de las medidas de seguridad se ha tenido en cuenta lo indicado en el Anexo II Medidas de seguridad del ENS en su apartado 2, donde se establece:

1. *Para la selección de las medidas de seguridad se seguirán los pasos siguientes:*

- a) Identificación de los tipos de activos presentes.*
- b) Determinación de las dimensiones de seguridad relevantes, teniendo en cuenta lo establecido en el anexo I.*
- c) Determinación del nivel correspondiente a cada dimensión de seguridad, teniendo en cuenta lo establecido en el anexo I.*
- d) Determinación de la categoría del sistema, según lo establecido en el Anexo I.*
- e) Selección de las medidas de seguridad apropiadas de entre las contenidas en este Anexo, de acuerdo con las dimensiones de seguridad y sus niveles, y, para determinadas medidas de seguridad, de acuerdo con la categoría del sistema.*

Por tanto, para cada una de las medidas de seguridad, se indicará, las dimensiones de seguridad afectadas, su aplicación para nivel medio, según sea el caso, si aplica o no, con la justificación y el documento principal de referencia donde se explica cómo se encuentra implementada la medida. En caso, de utilizar medidas compensatorias se indicará en dicho campo.



3. Declaración de aplicabilidad para el ENS

A continuación, se muestra la Declaración de Aplicabilidad de los sistemas de información propiedad del Ayuntamiento de la Universitat Oberta de Catalunya.

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 específicos de algunas medidas (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		Dimensi ones Afectad as	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSIC A	MEDI A	ALTA	APLIC A	JUSTIFICACIÓN	APLIC A	JUSTIFICACIÓN	
						SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO	
org	Marco organizativo									
org.1	Política de seguridad	Todas	aplica	=	=	MEDIO	Designación de roles de seguridad y constitución de Comité Política de Seguridad Plan de Adecuación (categorización, plan de mejora, etc.)	MEDIO	Documento de designación de roles de seguridad y constitución de Comité y de Política de seguridad Plan de Adecuación (categorización, plan de mejora, etc.)	Cubierto por Conformidad ENS
org.2	Normativa de seguridad	Todas	aplica	=	=	MEDIO	Normativa de Uso de Recursos y Accesos a Sistemas de Información Curso normativa	MEDIO	Normativa de Uso de Recursos y Accesos a Sistemas de Información Curso normativa	Cubierto por Conformidad ENS
org.3	Procedimientos de seguridad	Todas	aplica	=	=	MEDIO	Procedimiento de Gestión de la documentación Inventario de documentos Repositorio de procedimientos, instrucciones técnicas y registros.	MEDIO	Procedimiento de Gestión de la documentación Inventario de documentos Repositorio de procedimientos, instrucciones técnicas y registros.	Cubierto por Conformidad ENS
org.4	Proceso de autorización	Todas	aplica	=	=	MEDIO	Procedimiento de Gestión de Autorizaciones Herramienta evidencias	MEDIO	Procedimiento de Gestión Autorizaciones Herramienta evidencias	Cubierto por Conformidad ENS
op	Marco operacional									
op.pl	Planificación									
op.pl.1	Análisis de riesgos	Todas	aplica	+	++	MEDIO	Procedimiento de análisis de riesgos Archivo análisis de riesgos (PILAR) Informe de análisis de riesgos Acta de aceptación de riesgos	BAJO*	Procedimiento de análisis de riesgos Archivo análisis de riesgos (PILAR) Informe de análisis de riesgos Acta de aceptación de riesgos	Cubierto por Conformidad ENS



Medidas de Seguridad		Dimensi ones Afectad as	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSIC A	MEDI A	ALTA	APLIC A	JUSTIFICACIÓN	APLIC A	JUSTIFICACIÓN	
						SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO		SISTEMA EXTERNALIZADO
op.pl.2	Arquitectura de Seguridad	Todas	aplica	=	=	MEDIO	Esquemas de red físicos y lógicos Sistema de Gestión de Seguridad de la Información (SGSI)	MEDIO	Esquemas de red físicos y lógicos Sistema de Gestión de Seguridad de la Información (SGSI)	Cubierto por Conformidad ENS Documentación proporcionada por el órgano competente sobre las comunicaciones con el Ayuntamiento, y con otros sistemas interconectados
op.pl.3	Adquisición de nuevos componentes	Todas	aplica	=	=	MEDIO	Procedimiento de adquisición de nuevos componentes Informes de estudios previos a la adquisición	MEDIO	Esquemas de red físicos y lógicos Sistema de Gestión de Seguridad de la Información (SGSI)	Cubierto por Conformidad ENS
op.pl.4	Dimensionamiento/ Gestión de capacidades	Todas	n/a	aplica	=	MEDIO	Procedimiento de dimensiones y gestión de la capacidad Informes de estudio de dimensionamiento y gestión de la capacidad	n/a	Medida que no aplica al sistema de información del Ayuntamiento	Cubierto por Conformidad ENS Documentación regular proporcionada por el órgano competente sobre los recursos disponibles y consumidos
op.pl.5	Componentes certificados	Todas	n/a	n/a	aplica	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a
op.acc	Control de acceso									
op.acc.1	Identificación	A T	aplica	=	=	MEDIO	Procedimiento de control de acceso Herramienta solicitudes	MEDIO	Procedimiento de control de acceso Herramienta solicitudes	Cubierto por Conformidad ENS Procedimientos documentados proporcionados por el órgano competente de configuración de los mecanismos de identificación de los



Medidas de Seguridad		Dimensi ones Afectad as	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSIC A	MEDI A	ALTA	APLIC A	JUSTIFICACIÓN	APLIC A	JUSTIFICACIÓN	
						SISTEMA AYUNTAMIENTO			SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
op.acc.2	Requisitos de acceso	I C A T	aplica	=	=	MEDIO	Procedimiento de control de acceso Herramienta solicitudes	MEDIO	Procedimiento de control de acceso Herramienta solicitudes	usuarios en los servicios Cubierto por Conformidad ENS Procedimientos documentados proporcionados por el órgano competente de configuración de roles/perfiles de acceso a los servicios
op.acc.3	Segregación de funciones y tareas	I C A T	n/a	aplica	=	MEDIO	Procedimiento de control de acceso Herramienta solicitudes y evidencias Definición de medida compensatoria en caso de sea necesario	n/a	Medida que no aplica al sistema de información del Ayuntamiento	Cubierto por Conformidad ENS Procedimientos documentados proporcionados por el órgano competente de configuración de roles/perfiles de acceso a los servicios
op.acc.4	Protección de gestión de derechos de acceso	I C A T	aplica	=	=	MEDIO	Procedimiento de control de acceso Herramienta solicitudes Evidencias de revisiones de accesos	MEDIO	Procedimiento de control de acceso Herramienta solicitudes Evidencias de revisiones de accesos	Cubierto por Conformidad ENS Procedimientos documentados proporcionados por el órgano competente de configuración de roles/perfiles de acceso a los servicios
op.acc.5	Mecanismo de autenticación	I C A T	aplica	+	++	MEDIO	Procedimiento de control de acceso Instrucciones Técnicas de bastionado de dominio y de aplicaciones	MEDIO	Procedimiento de control de acceso Instrucciones Técnicas de bastionado de dominio y de aplicaciones	Cubierto por Conformidad ENS Procedimientos documentados proporcionados por el



Medidas de Seguridad		Dimensi ones Afectad as	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSIC A	MEDI A	ALTA	APLIC A	JUSTIFICACIÓN	APLIC A	JUSTIFICACIÓN	
						SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO	
										órgano competente de los mecanismo de autenticación de acceso a los servicios
op.acc.6	Acceso local (local logon)	I C A T	aplica	+	++	MEDIO	Procedimiento de control de acceso Instrucciones Técnicas de bastionado de dominio y de aplicaciones	MEDIO	Procedimiento de control de acceso Instrucciones Técnicas de bastionado de dominio y de aplicaciones	Cubierto por Conformidad ENS 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
op.acc.7	Acceso remoto (remote login)	I C A T	aplica	+	=	MEDIO	Procedimiento de control de acceso Procedimiento de acceso remoto Instrucciones Técnicas de configuración de acceso remoto	MEDIO	Procedimiento de control de acceso Procedimiento de acceso remoto Instrucciones Técnicas de configuración de acceso remoto	Cubierto por Conformidad ENS
op.exp	Explotación									
op.exp.1	Inventario de activos	Todas	aplica	=	=	MEDIO	Procedimiento de Gestión de activos Herramienta de inventario de activos	MEDIO	Procedimiento de Gestión de activos Herramienta de inventario de activos	Cubierto por Conformidad ENS



Medidas de Seguridad		Dimensi ones Afectad as	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO			
			BÁSIC A	MEDI A	ALTA	APLIC A	JUSTIFICACIÓN	APLIC A	JUSTIFICACIÓN		
						SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO		
op.exp.2	Configuración de seguridad	Todas	aplica	=	=	MEDIO	Procedimiento de Gestión de la Configuración Instrucciones Técnicas de bastionado equipamiento, máquinas virtuales Informes CLARA Informes ROCIO	MEDIO	Procedimiento de Gestión de la Configuración Instrucciones Técnicas de bastionado equipamiento, máquinas virtuales Informes CLARA Informes ROCIO	Cubierto por Conformidad ENS	
op.exp.3	Gestión de la configuración de seguridad	Todas	n/a	aplica	=	MEDIO	Procedimiento de Gestión de la Configuración Herramienta solicitudes y evidencias	MEDIO	Procedimiento de Gestión de la Configuración Herramienta solicitudes y evidencias	Cubierto por Conformidad ENS	
op.exp.4	Mantenimiento	Todas	aplica	=	=	MEDIO	Procedimiento de mantenimiento Herramienta de solicitudes y evidencias	MEDIO	Procedimiento de mantenimiento Herramienta de solicitudes y evidencias	Cubierto por Conformidad ENS Procedimientos documentados de coordinación con el Ayuntamiento para realizar acciones de mantenimiento sobre el sistema que soportan los servicios	
op.exp.5	Gestión de cambios	Todas	n/a	aplica	=	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al sistema de información del Ayuntamiento	Cubierto por Conformidad ENS Procedimientos documentados de coordinación con el Ayuntamiento para realizar cambios sobre el sistema que soporta los servicios	
op.exp.6	Protección frente a código dañino	Todas	aplica	=	=	MEDIO	Procedimiento de Protección frente a Código dañino Consola antivirus e informes	MEDIO	Procedimiento de Protección frente a Código dañino Consola antivirus e informes	Cubierto por Conformidad ENS	



Medidas de Seguridad		Dimensi ones Afectad as	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO			
			BÁSIC A	MEDI A	ALTA	APLIC A	JUSTIFICACIÓN	APLIC A	JUSTIFICACIÓN		
						SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO		
op.exp.7	Gestión de incidentes	Todas	n/a	aplica	=	MEDIO	Procedimiento de Gestión de Incidentes Procedimiento de Gestión de Brechas de Seguridad Informes de incidentes Herramienta interna gestión incidencias Herramienta LUCIA	MEDIO	Procedimiento de Gestión de Incidentes Procedimiento de Gestión de Brechas de Seguridad Informes de incidentes Herramienta interna gestión incidencias	Cubierto por Conformidad ENS Procedimientos documentados de coordinación con el Ayuntamiento para la gestión incidentes y de comunicación de los mismos autoridades de control	
op.exp.8	Registro de la actividad de los usuarios	Todas	aplica	+	++	MEDIO	Procedimiento de Gestión de logs. Registros de actividad Informes de revisión	BAJO*	Registros de actividad Informes de revisión Sistema órgano competente que soporta los servicios cubierto por Conformidad ENS y Procedimientos de Gestión de logs.	Cubierto por Conformidad ENS 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)	



Medidas de Seguridad		Dimensi ones Afectad as	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO			
			BÁSIC A	MEDI A	ALTA	APLIC A	JUSTIFICACIÓN	APLIC A	JUSTIFICACIÓN		
						SISTEMA AYUNTAMIENTO			SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO	
op.exp.9	Registro de la gestión de incidentes	Todas	n/a	aplica	aplica	MEDIO	Procedimiento de Gestión de Incidentes Procedimiento de Gestión de Brechas de Seguridad Informes de incidentes Herramienta interna gestión incidencias Herramienta LUCIA	MEDIO	Procedimiento de Gestión de Incidentes Procedimiento de Gestión de Brechas de Seguridad Informes de incidentes Herramienta interna gestión incidencias	Cubierto por Conformidad ENS Procedimientos documentados de coordinación con el Ayuntamiento para la gestión incidentes y de comunicación de los mismos autoridades de control	
op.exp.10	Protección de los registro de actividad	T	n/a	n/a	aplica	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	
op.exp.11	Protección de claves criptográficas	Todas	aplica	+	=	MEDIO	Procedimiento de Protección de Claves Criptográficas	MEDIO	Procedimiento de Protección de Claves Criptográficas	Cubierto por Conformidad ENS Procedimientos documentados de protección de las claves criptográficas del Ayuntamiento que se encuentren alojadas en el sistema que soporta los servicios	



Medidas de Seguridad		Dimensi ones Afectad as	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSIC A	MEDI A	ALTA	APLIC A	JUSTIFICACIÓN	APLIC A	JUSTIFICACIÓN	
						SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO	
op.ext	Servicios externos									
op.ext.1	Contratación y acuerdos de nivel de servicio	Todas	n/a	aplica	=	MEDIO	Procedimiento de Gestión de Servicios Externos Clausulado de seguridad (confidencialidad, conformidad, ENS, comunicación incidente, etc.) pliegos Contratos y SLAs órgano competentes Certificados Conformidad ENS órgano competentes relacionados con el alcance	MEDIO	Procedimiento de Gestión de Servicios Externos Clausulado de seguridad (confidencialidad, conformidad, ENS, comunicación incidente, etc.) pliegos Contratos y SLAs Certificados Conformidad ENS servicios externalizados y de otros órgano competentes relacionados con el alcance	Cubierto por Conformidad ENS Certificados de Conformidad ENS de los servicios subcontratados por el órgano competente
op.ext.2	Gestión diaria	Todas	n/a	aplica	=	MEDIO	Procedimiento de Gestión de Servicios Externos Informes de revisión de SLA	MEDIO	Procedimiento de Gestión de Servicios Externos Informes de revisión de SLA	Cubierto por Conformidad ENS Informes/herramientas seguimiento SLA proporcionadas por el órgano competente
op.ext.9	Medios alternativos	Todas	n/a	n/a	aplica	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a
op.cont	Continuidad del servicio									
op.cont.1	Análisis de impacto	D	n/a	aplica	=	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a**	Medida que no aplica al sistema de información del Ayuntamiento	Cubierto por Conformidad ENS
op.cont.2	Plan de continuidad	D	n/a	n/a	aplica	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a
op.cont.3	Pruebas periódicas	D	n/a	n/a	aplica	n/a	Medida que no aplica al Perfil	n/a	Medida que no aplica al	n/a



Medidas de Seguridad	Dimensi ones Afectad as	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO			
		BÁSIC A	MEDI A	ALTA	APLIC A	JUSTIFICACIÓN	APLIC A	JUSTIFICACIÓN		
						SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO	
							de Cumplimiento Específico		Perfil de Cumplimiento Específico	
op.mon	Monitorización del sistema									
op.mon.1	Detección de intrusión	Todas	n/a	aplica	=	MEDIO	Procedimiento de Detección de Intrusión Herramientas IDS	MEDIO	Procedimiento de Detección de Intrusión Herramientas IDS	Cubierto por Conformidad ENS
op.mon.2	Sistema de métricas	Todas	aplica	+	++	MEDIO	Procedimiento de Métricas e Indicadores Registro de métricas e indicadores Registro de IM e IC	MEDIO	Procedimiento de Métricas e Indicadores Registro de métricas e indicadores Registro de IM e IC	Cubierto por Conformidad ENS
mp	Medidas de protección									
mp.if	Protección de las instalaciones e infraestructuras									
mp.if.1	Áreas separadas y con control de acceso	Todas	aplica	=	=	MEDIO	Procedimiento de Protección de las Instalaciones Planos instalaciones e infraestructuras	MEDIO	Procedimiento de Protección de las Instalaciones Planos instalaciones e infraestructuras	Cubierto por Conformidad ENS
mp.if.2	Identificación de las personas	Todas	aplica	=	=	MEDIO	Procedimiento de Protección de las Instalaciones Registros de los accesos Informes de revisión de los accesos	MEDIO	Procedimiento de Protección de las Instalaciones Registros de los accesos Informes de revisión de los accesos	Cubierto por Conformidad ENS
mp.if.3	Acondicionamiento de los locales	Todas	aplica	=	=	MEDIO	Procedimiento de Protección de las Instalaciones Herramientas sensores temperaturas e humedad Revisiones mantenimientos	MEDIO	Procedimiento de Protección de las Instalaciones Herramientas sensores temperaturas e humedad Revisiones mantenimientos	Cubierto por Conformidad ENS



Medidas de Seguridad		Dimensi ones Afectad as	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSIC A	MEDI A	ALTA	APLIC A	JUSTIFICACIÓN	APLIC A	JUSTIFICACIÓN	
						SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO	
mp.if.4	Energía eléctrica	D	aplica	+	=	MEDIO	Procedimiento de Protección de las Instalaciones Revisiones de SAI Revisiones mantenimientos Informes pruebas de capacidad	BAJO	Procedimiento de Protección de las Instalaciones Revisiones mantenimientos	Cubierto por Conformidad ENS
mp.if.5	Protección frente a incendios	D	aplica	=	=	MEDIO	Procedimiento de Protección de las Instalaciones Documentación medidas de prevención y extinción de incendios Revisiones de mantenimiento	MEDIO	Procedimiento de Protección de las Instalaciones Documentación medidas de prevención y extinción de incendios Revisiones de mantenimiento	Cubierto por Conformidad ENS
mp.if.6	Protección frente a inundaciones	D	n/a	aplica	=	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a**	Medida que no aplica al sistema de información del Ayuntamiento	Cubierto por Conformidad ENS
mp.if.7	Registro de entrada y salida de equipamiento	Todas	aplica	=	=	MEDIO	Procedimiento de Registro Entrada/Salida de equipamiento Herramienta evidencias entrada y salida de equipamiento	MEDIO	Procedimiento de Registro Entrada/Salida de equipamiento Herramienta evidencias entrada y salida de equipamiento	Cubierto por Conformidad ENS
mp.if.9	Instalaciones alternativas	Todas	n/a	n/a	aplica	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	
mp.per	Gestión del personal									
mp.per.1	Caracterización del puesto de trabajo	Todas	n/a	aplica	=	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a**	Medida que no aplica al sistema de información del Ayuntamiento	Cubierto por Conformidad ENS



Medidas de Seguridad		Dimensi ones Afectad as	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSIC A	MEDI A	ALTA	APLIC A	JUSTIFICACIÓN	APLIC A	JUSTIFICACIÓN	
						SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO	
mp.per.2	Deberes y obligaciones	Todas	aplica	=	=	MEDIO	Procedimiento de Gestión de Personal Política de Seguridad Normativa de Uso de Recursos y Accesos a Sistemas de Información Acuerdos de confidencialidad personal propio Acuerdos de confidencialidad con empresas órgano competentes, en caso de personal ajeno trabajando en las instalaciones	MEDIO	Procedimiento de Gestión de Personal Política de Seguridad Normativa de Uso de Recursos y Accesos a Sistemas de Información Acuerdos de confidencialidad personal propio Acuerdos de confidencialidad con empresas órgano competentes, en caso de personal ajeno trabajando en las instalaciones	Cubierto por Conformidad ENS
mp.per.3	Concienciación	Todas	aplica	=	=	MEDIO	Procedimiento de Gestión de Personal Plan de concienciación anual Cartelería/fondos de pantalla/cursos online	MEDIO	Procedimiento de Gestión de Personal Plan de concienciación anual	Cubierto por Conformidad ENS
mp.per.4	Formación	Todas	aplica	=	=	MEDIO	Procedimiento de Gestión de Personal Plan de formación anual Plataforma Vanesa Cursos online CCN	MEDIO	Procedimiento de Gestión de Personal Plan de concienciación anual Plataforma Vanesa Cursos online CCN	Cubierto por Conformidad ENS
mp.per.9	Personal alternativo	D	n/a	n/a	aplica	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a
mp.eq	Protección de los equipos									
mp.eq.1	Puesto de trabajo despejado	Todas	aplica	+	=	MEDIO	Procedimiento de Protección de los Equipos Normativa de Uso de Recursos	MEDIO	Procedimiento de Protección de los Equipos Normativa de Uso de	Cubierto por Conformidad ENS



Medidas de Seguridad		Dimensi ones Afectad as	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSIC A	MEDI A	ALTA	APLIC A	JUSTIFICACIÓN	APLIC A	JUSTIFICACIÓN	
						SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO	
							y Accesos a Sistemas de Información		Recursos y Accesos a Sistemas de Información	
mp.eq.2	Bloqueo de puesto de trabajo	A	n/a	aplica	+	MEDIO	Procedimiento de Protección de los Equipos Normativa de Uso de Recursos y Accesos a Sistemas de Información Instrucción Técnica de bastionado de dominio	MEDIO	Procedimiento de Protección de los Equipos Normativa de Uso de Recursos y Accesos a Sistemas de Información Instrucción Técnica de bastionado de dominio	Cubierto por Conformidad ENS
mp.eq.3	Protección de equipos portátiles	Todas	aplica	=	+	MEDIO	Procedimiento de Protección de los Equipos y equipamiento de red Normativa de Uso de Recursos y Accesos a Sistemas de Información Instrucción Técnica de bastionado de equipos portátiles Procedimiento de Autorización Procedimiento de Gestión de Activos Herramienta Inventario de Activos Herramienta Evidencias	MEDIO	Procedimiento de Protección de los Equipos y equipamiento de red Normativa de Uso de Recursos y Accesos a Sistemas de Información Instrucción Técnica de bastionado de equipos portátiles Procedimiento de Autorización Procedimiento de Gestión de Activos Herramienta Inventario de Activos Herramienta Evidencias	Cubierto por Conformidad ENS
mp.eq.9	Medios alternativos	D	n/a	n/a	aplica	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	
mp.com	Protección de las comunicaciones									
mp.com.1	Perímetro seguro	Todas	aplica	=	+	MEDIO	Procedimiento de Protección de las Comunicaciones Herramienta evidencias	MEDIO	Procedimiento de Protección de las Comunicaciones Herramienta evidencias	Cubierto por Conformidad ENS



Medidas de Seguridad		Dimensi ones Afectad as	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSIC A	MEDI A	ALTA	APLIC A	JUSTIFICACIÓN	APLIC A	JUSTIFICACIÓN	
						SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO		SISTEMA EXTERNALIZADO
mp.com.2	Protección de la confidencialidad	C	n/a	+	++	MEDIO	Procedimiento de Protección de las Comunicaciones	MEDIO	Procedimiento de Protección de las Comunicaciones	Cubierto por Conformidad ENS Documentos proporcionados por el órgano competente con información sobre los mecanismos de cifrado implementados en las comunicaciones
mp.com.3	Protección de la autenticidad y de la integridad	I A	aplica	+	++	MEDIO	Procedimiento de Protección de las Comunicaciones	MEDIO	Procedimiento de Protección de las Comunicaciones	Cubierto por Conformidad ENS Documentos proporcionados por el órgano competente con información sobre los mecanismos implementados para proteger la autenticidad y de la integridad
mp.com.4	Separación de redes	Todas	n/a	n/a	aplica	ALTO	Procedimiento de segmentación de redes Esquemas de red	ALTO	Procedimiento de segmentación de redes Esquemas de red	Cubierto por Conformidad ENS
mp.com.9	Medios alternativos	Todas	n/a	n/a	aplica	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	



Medidas de Seguridad		Dimensi ones Afectad as	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSIC A	MEDI A	ALTA	APLIC A	JUSTIFICACIÓN	APLIC A	JUSTIFICACIÓN	
						SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO	
mp.si	Protección de los soportes de información									
mp.si.1	Etiquetado	C	aplica	=	=	MEDIO ₁	Cuando sea de aplicación: Procedimiento de Gestión de Soportes de Información Procedimiento de Marcado de Soportes Normativa de Uso de Recursos y Accesos a Sistemas de Información Procedimiento de Autorización Herramienta Evidencias	MEDIO ₁	Procedimiento de Gestión de Soportes de Información Procedimiento de Marcado de Soportes Normativa de Uso de Recursos y Accesos a Sistemas de Información Herramienta Evidencias	Cubierto por Conformidad ENS
mp.si.2	Criptografía	I C	n/a	aplica	+	MEDIO ₁	Procedimiento de Gestión de Soportes de Información Normativa de Uso de Recursos y Accesos a Sistemas de Información Instrucción Técnica de Criptografía	MEDIO ₁	Procedimiento de Gestión de Soportes de Información Normativa de Uso de Recursos y Accesos a Sistemas de Información Instrucción Técnica de Criptografía	Cubierto por Conformidad ENS
mp.si.3	Custodia	Todas	aplica	=	=	MEDIO ₁	Procedimiento de Gestión de Soportes de Información Normativa de Uso de Recursos y Accesos a Sistemas de Información	MEDIO ₁	Procedimiento de Gestión de Soportes de Información Normativa de Uso de Recursos y Accesos a Sistemas de Información	Cubierto por Conformidad ENS
mp.si.4	Transporte	Todas	aplica	=	=	MEDIO ₁	Procedimiento de Gestión de Soportes de Información Normativa de Uso de Recursos y Accesos a Sistemas de Información Registro entrada/salida de soportes	MEDIO ₁	Procedimiento de Gestión de Soportes de Información Normativa de Uso de Recursos y Accesos a Sistemas de Información Registro entrada/salida de soportes	Cubierto por Conformidad ENS

1 Cuando contengan información relacionada con los servicios dentro del alcance del ENS o que forman parte del SGSI.



Medidas de Seguridad		Dimensi ones Afectad as	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSIC A	MEDI A	ALTA	APLIC A	JUSTIFICACIÓN	APLIC A	JUSTIFICACIÓN	
						SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO	
mp.si.5	Borrado y destrucción	D	aplica	+	=	MEDIO	Procedimiento de Gestión de Soportes de Información Normativa de Uso de Recursos y Accesos a Sistemas de Información Instrucción Técnica de borrado de soportes	MEDIO	Procedimiento de Gestión de Soportes de Información Normativa de Uso de Recursos y Accesos a Sistemas de Información Instrucción Técnica de borrado de soportes	Cubierto por Conformidad ENS
mp.sw	Protección de las aplicaciones informáticas									
mp.sw.1	Desarrollo de aplicaciones	Todas	n/a	aplica	=	n/a	Medida que no aplica al sistema de información del Ayuntamiento	MEDIO	Medida que no aplica al sistema de información del Ayuntamiento	Cubierto por Conformidad ENS
mp.sw.2	Aceptación y puesta en servicio	Todas	aplica	+	++	n/a	Procedimiento de Aceptación y Puesta en Servicio Plan de Pruebas- Informe resultados	MEDIO	Medida que no aplica al sistema de información del Ayuntamiento	Cubierto por Conformidad ENS 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



Medidas de Seguridad		Dimensi ones Afectad as	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSIC A	MEDI A	ALTA	APLIC A	JUSTIFICACIÓN	APLIC A	JUSTIFICACIÓN	
						SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO	
mp.info	Protección de la información									
mp.info.1	Datos de carácter personal	Todas	aplica	=	=	MEDIO	Registro de Actividades de Tratamiento (RAT) Delegado de Protección de Datos Análisis de Riesgo RGPD Evaluaciones de Impacto (EIPD) Regulación de la recogida de datos Regulación de terceros. Contratos de Encargado del Tratamiento. Deber de Diligencia	MEDIO	Registro de Actividades de Tratamiento (RAT) Delegado de Protección de Datos Análisis de Riesgo RGPD Evaluaciones de Impacto Regulación de la recogida de datos Regulación de terceros. Contratos de Encargado del Tratamiento. Deber de Diligencia	Cubierto por Conformidad ENS Documentos /plataformas online, proporcionados por el órgano competente, con evidencias de cumplimiento de la normativa de protección de datos
mp.info.2	Calificación de la información	C	aplica	+	=	MEDIO	Procedimiento de Calificación de la Información	MEDIO	Procedimiento de Calificación de la Información	Cubierto por Conformidad ENS
mp.info.3	Cifrado	C	n/a	n/a	+	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	
mp.info.4	Firma electrónica	I A	aplica	+	++	MEDIO	Cuando sea de aplicación: Procedimiento de Firma Electrónica Política de firma electrónica y certificados	MEDIO	Cuando sea de aplicación: Procedimiento de Firma Electrónica Política de firma electrónica y certificados	Cubierto por Conformidad ENS Documentos proporcionados por el órgano competente con información sobre las medidas de protección de la firma implementadas



Medidas de Seguridad		Dimensi ones Afectad as	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSIC A	MEDI A	ALTA	APLIC A	JUSTIFICACIÓN	APLIC A	JUSTIFICACIÓN	
						SISTEMA AYUNTAMIENTO			SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO
mp.info.5	Sellos de tiempo	T	n/a	n/a	aplica	ALTO	Procedimiento de Sellado de Tiempo	ALTO	Procedimiento de Sellado de Tiempo	Cubierto por Conformidad ENS 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	C	aplica	=	=	MEDIO	Normativa de Limpieza de Metadatos Instrucción Técnica de Limpieza de Metadatos	MEDIO	Normativa de Limpieza de Metadatos Instrucción Técnica de Limpieza de Metadatos	Cubierto por Conformidad ENS
mp.info.9	Copias de seguridad (backup)	D	aplica	=	=	MEDIO	Procedimiento de copias de respaldo y pruebas de restauración	MEDIO	Procedimiento de copias de respaldo y de restauración (si se tiene información en local en el sistema del Ayuntamiento)	Cubierto por Conformidad ENS Procedimientos documentados proporcionados por el órgano competente de la política de copias de seguridad y de restauración



Medidas de Seguridad		Dimensi ones Afectad as	CATEGORÍA			SERVICIO ALOJADO AYUNTAMIENTO		SERVICIO EXTERNALIZADO		
			BÁSIC A	MEDI A	ALTA	APLIC A	JUSTIFICACIÓN	APLIC A	JUSTIFICACIÓN	
						SISTEMA AYUNTAMIENTO		SISTEMA AYUNTAMIENTO	SISTEMA EXTERNALIZADO	
mp.s	Protección de los servicios									
mp.s.1	Protección del correo electrónico	Todas	aplica	=	=	MEDIO	Procedimiento de Protección del Correo Electrónico Instrucción Técnica de Bastionado del Correo Electrónico (si lo provee órgano competente externo solicitar conformidad con el ENS en categoría MEDIA y procedimiento de configuración del correo)	MEDIO	Procedimiento de Protección del Correo Electrónico Instrucción Técnica de Bastionado del Correo Electrónico (si lo provee órgano competente externo solicitar conformidad con el ENS en categoría MEDIA y procedimiento de configuración del correo)	n/a
mp.s.2	Protección de servicios y aplicaciones web	Todas	aplica	=	+	MEDIO	Procedimiento de Protección de los Servicios y Aplicaciones Web Instrucción Técnica de Bastionado de Servicios Web	n/a**	Medida que no aplica al sistema de información del Ayuntamiento	Cubierto por Conformidad ENS Informes proporcionados por el órgano competente con resultados de las inspecciones periódicas realizadas y plan de acción
mp.s.8	Protección frente a denegación de servicio	D	n/a	aplica	+	MEDIO	Procedimiento de protección frente a la denegación de servicio Instrucción técnica de bastionado de las tecnologías desplegadas para protegerse de la denegación de servicio	n/a**	Medida que no aplica al sistema de información del Ayuntamiento	Cubierto por Conformidad ENS
mp.s.9	Medios alternativos	D	n/a	n/a	+	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a	Medida que no aplica al Perfil de Cumplimiento Específico	n/a



4. Declaración de aplicabilidad para ISO 27001:2013

ISO 27001:2013 Controles de Seguridad				
Cláusula	Sección	Objetivo de control / control	Aplica	Justificación
5 Políticas de Seguridad	5,1	Dirección de la alta gerencia para la seguridad de la información		
	5.1.1	Políticas de seguridad de la información	Sí	Se corresponde con org.1 y org.2 de la declaración de aplicabilidad del ENS
	5.1.2	Revisión de las políticas de seguridad de la información	Sí	Se corresponde con org.1, org.2 y op.pl.2 de la declaración de aplicabilidad del ENS
6 Organización de la Seguridad de la Información	6,1	Organización interna		
	6.1.1	Roles y responsabilidad de seguridad de la información	Sí	Se corresponde con org.1 de la declaración de aplicabilidad del ENS
	6.1.2	Segregación de deberes	Sí	Se corresponde con org.4, op.acc.3 y op.exp.8 de la declaración de aplicabilidad del ENS
	6.1.3	Contacto con autoridades	Sí	Se corresponde con org.3 y op.exp.7 de la declaración de aplicabilidad del ENS
	6.1.4	Contacto con grupos de interés especial	Sí	Se corresponde con op.exp.7 de la declaración de aplicabilidad del ENS
	6.1.5	Seguridad de la información en la gestión de proyectos	Sí	Se corresponde con mp.sw.1 de la declaración de aplicabilidad del ENS
	6,2	Dispositivos móviles y teletrabajo		
	6.2.1	Política de dispositivos móviles	Sí	Se corresponde con org.4 y mp.eq.3 de la declaración de aplicabilidad del ENS (No es objetivo de este TFM)



ISO 27001:2013 Controles de Seguridad				
Cláusula	Sección	Objetivo de control / control	Aplica	Justificación
	6.2.2	Teletrabajo	Sí	Se corresponde con org.2 de la declaración de aplicabilidad del ENS
7 Seguridad en los Recursos Humanos	7,1	Previo al empleo		
	7.1.1	Verificación de antecedentes	No	Se corresponde con mp.per.1 de la declaración de aplicabilidad del ENS
	7.1.2	Términos y condiciones del empleo	Sí	Se corresponde con mp.per.2 de la declaración de aplicabilidad del ENS
	7,2	Durante el empleo		
	7.2.1	Responsabilidades de la Alta Gerencia	Sí	Se corresponde con mp.per.1 y mp.per.2 de la declaración de aplicabilidad del ENS
	7.2.2	Conciencia, educación y entrenamiento de seguridad de la información	Sí	Se corresponde con mp.per.3, mp.per.4 y mp.s.1 de la declaración de aplicabilidad del ENS
	7.2.3	Proceso disciplinario	Sí	Se corresponde con mp.per.2 de la declaración de aplicabilidad del ENS
	7,3	Terminación y cambio de empleo		
	7.3.1	Termino de responsabilidades o cambio de empleo	Sí	Se corresponde con mp.per.2 de la declaración de aplicabilidad del ENS
8 Gestión de Activos	8,1	Responsabilidad de los activos		
	8.1.1	Inventario de activos	Sí	Se corresponde con op.exp.1 y op.pl.2 de la declaración de aplicabilidad del ENS
	8.1.2	Propiedad de activos	Sí	Se corresponde con op.exp.1 y mp.info.2 de la declaración de



ISO 27001:2013 Controles de Seguridad				
Cláusula	Sección	Objetivo de control / control	Aplica	Justificación
				aplicabilidad del ENS
	8.1.3	Uso aceptable de los activos	Sí	Se corresponde con org.2 de la declaración de aplicabilidad del ENS
	8.1.4	Devolución de activos	Sí	Se corresponde con mp.per.2 de la declaración de aplicabilidad del ENS
	8,2	Clasificación de la información		
	8.2.1	Clasificación de la información	Sí	Se corresponde con mp.info.2 de la declaración de aplicabilidad del ENS
	8.2.2	Etiquetado de la información	Sí	Se corresponde con mp.info.2 y mp.si.1 de la declaración de aplicabilidad del ENS
	8.2.3	Manejo de activos	Sí	Se corresponde con mp.info.2 de la declaración de aplicabilidad del ENS
	8,3	Manejo de medios		
	8.3.1	Gestión de medios removibles	Sí	Se corresponde con org.4, mp.si.1, mp.si.2 y mp.si.3 de la declaración de aplicabilidad del ENS
	8.3.2	Eliminación de medios	Sí	Se corresponde con mp.si.5 de la declaración de aplicabilidad del ENS
	8.3.3	Transporte de medios físicos	Sí	Se corresponde con mp.si.4 de la declaración de aplicabilidad del ENS
9 Control de Acceso	9,1	Requerimientos de negocio para el control de acceso		
	9.1.1	Política de control de acceso	Sí	Se corresponde con op.acc.2 de la declaración de aplicabilidad del ENS
	9.1.2	Acceso a redes y servicios de red	Sí	Se corresponde con op.acc.2 y op.acc.7 de la declaración de



ISO 27001:2013 Controles de Seguridad				
Cláusula	Sección	Objetivo de control / control	Aplica	Justificación
				aplicabilidad del ENS
	9,2	Gestión de accesos de usuario		
	9.2.1	Registro y baja del usuario	Sí	Se corresponde con op.acc.1 y op.acc.5 de la declaración de aplicabilidad del ENS
	9.2.2	Provisión de acceso a usuarios	Sí	Se corresponde con op.acc.2, op.acc.4 y op.acc.5 de la declaración de aplicabilidad del ENS
	9.2.3	Gestión de derechos de acceso privilegiados	Sí	Se corresponde con op.acc.1 y op.acc.4 de la declaración de aplicabilidad del ENS
	9.2.4	Gestión de información de autenticación secreta de usuarios	Sí	Se corresponde con op.acc.5 de la declaración de aplicabilidad del ENS
	9.2.5	Revisión de derechos de acceso de usuarios	Sí	Se corresponde con op.acc.4 de la declaración de aplicabilidad del ENS
	9.2.6	Eliminación o ajuste de derechos de acceso	Sí	Se corresponde con op.acc.1, op.acc.4 y op.acc.5 de la declaración de aplicabilidad del ENS
	9,3	Responsabilidades del usuario		
	9.3.1	Uso de información de autenticación secreta	Sí	Se corresponde con op.acc.5 de la declaración de aplicabilidad del ENS
	9,4	Control de acceso de sistemas y aplicaciones		
	9.4.1	Restricción de acceso a la información	Sí	Se corresponde con op.acc.2 y op.acc.4 de la declaración de aplicabilidad del ENS
	9.4.2	Procedimientos de inicio de sesión seguro	Sí	Se corresponde con op.acc.5, op.acc.6 y op.acc.7 de la declaración de aplicabilidad del ENS
	9.4.3	Sistema de gestión de contraseñas	Sí	Se corresponde con op.acc.5 de la declaración de aplicabilidad del ENS



ISO 27001:2013 Controles de Seguridad				
Cláusula	Sección	Objetivo de control / control	Aplica	Justificación
	9.4.4	Uso de programas y utilidades privilegiadas	Sí	Se corresponde con op.acc.2 de la declaración de aplicabilidad del ENS
	9.4.5	Control de acceso al código fuente del programa	No	Se corresponde con op.acc.2 y mp.sw.1 de la declaración de aplicabilidad del ENS
10 Criptografía	10,1	Controles criptográficos		
	10.1.1	Política en el uso de controles criptográficos	Sí	Se corresponde con mp.si.2, mp.info.3, mp.info.4, op.acc.7, mp.com.2 y mp.com.3 de la declaración de aplicabilidad del ENS
	10.1.2	Gestión de llaves	Sí	Se corresponde con op.exp.11 de la declaración de aplicabilidad del ENS
11 Seguridad Física y del Entorno	11,1	Áreas seguras		
	11.1.1	Perímetro de seguridad físico	Sí	Se corresponde con mp.if.1 de la declaración de aplicabilidad del ENS
	11.1.2	Controles físicos de entrada	Sí	Se corresponde con mp.if.1 y mp.if.2 de la declaración de aplicabilidad del ENS
	11.1.3	Seguridad de oficinas, habitaciones y facilidades	Sí	Se corresponde con mp.if.1 de la declaración de aplicabilidad del ENS
	11.1.4	Protección contra amenazas externas y del ambiente	Sí	Se corresponde con mp.if.3, mp.if.5 y mp.if.6 de la declaración de aplicabilidad del ENS
	11.1.5	Trabajo en áreas seguras	Sí	Se corresponde con mp.if.1 y op.pl.2 de la declaración de aplicabilidad del ENS
	11.1.6	Áreas de entrega y carga	Sí	Se corresponde con mp.if.1 y op.pl.2 de la declaración de aplicabilidad del ENS
	11,2	Equipo		



ISO 27001:2013 Controles de Seguridad				
Cláusula	Sección	Objetivo de control / control	Aplica	Justificación
	11.2.1	Instalación y protección de equipo	Sí	Se corresponde con mp.if.1, mp.if.3, mp.if.5 y mp.if.6 de la declaración de aplicabilidad del ENS
	11.2.2	Servicios de soporte	Sí	Se corresponde con mp.if.3 y mp.if.4 de la declaración de aplicabilidad del ENS
	11.2.3	Seguridad en el cableado	Sí	Se corresponde con mp.if.3 de la declaración de aplicabilidad del ENS
	11.2.4	Mantenimiento de equipos	Sí	Se corresponde con op.exp.4 de la declaración de aplicabilidad del ENS
	11.2.5	Retiro de activos	Sí	Se corresponde con org.4, mp.if.7 y mp.si.4 de la declaración de aplicabilidad del ENS
	11.2.6	Seguridad del equipo y activos fuera de las instalaciones	Sí	Se corresponde con org.4, mp.if.7 y mp.eq.3 de la declaración de aplicabilidad del ENS
	11.2.7	Eliminación segura o reuso del equipo	Sí	Se corresponde con mp.si.5 de la declaración de aplicabilidad del ENS
	11.2.8	Equipo de usuario desatendido	Sí	Se corresponde con mp.eq.2 de la declaración de aplicabilidad del ENS
	11.2.9	Política de escritorio limpio y pantalla limpia	Sí	Se corresponde con mp.eq.1 de la declaración de aplicabilidad del ENS
12 Seguridad en las Operaciones	12,1	Procedimientos Operacionales y Responsabilidades		
	12.1.1	Documentación de procedimientos operacionales	Sí	Se corresponde con org.3 y mp.per.3 de la declaración de aplicabilidad del ENS
	12.1.2	Gestión de cambios	No	Se corresponde con op.exp.5 de la declaración de aplicabilidad del ENS



ISO 27001:2013 Controles de Seguridad				
Cláusula	Sección	Objetivo de control / control	Aplica	Justificación
	12.1.3	Gestión de la capacidad	Sí	Se corresponde con op.pl.4 de la declaración de aplicabilidad del ENS
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Sí	Se corresponde con mp.sw.1 y mp.sw.2 de la declaración de aplicabilidad del ENS
	12,2	Protección de Software Malicioso		
	12.2.1	Controles contra software malicioso	Sí	Se corresponde con op.exp.6 de la declaración de aplicabilidad del ENS
	12,3	Respaldo		
	12.3.1	Respaldo de información	Sí	Se corresponde con mp.info.9 de la declaración de aplicabilidad del ENS
	12,4	Bitácoras y monitoreo		
	12.4.1	Bitácoras de eventos	Sí	Se corresponde con op.exp.8 de la declaración de aplicabilidad del ENS
	12.4.2	Protección de información en bitácoras	No	Se corresponde con op.exp.10 de la declaración de aplicabilidad del ENS
	12.4.3	Bitácoras de administrador y operador	Sí	Se corresponde con op.exp.8 e la declaración de aplicabilidad del ENS
	12.4.4	Sincronización de relojes	Sí	Se corresponde con op.exp.8 y op.exp.10 de la declaración de aplicabilidad del ENS
	12,5	Control de software operacional		
	12.5.1	Instalación de software en sistemas operacionales	Sí	Se corresponde con org.4, op.exp.2 y mp.sw.2 de la declaración de aplicabilidad del ENS
	12,6	Gestión de vulnerabilidades técnicas		
	12.6.1	Gestión de vulnerabilidades	Sí	Se corresponde con op.exp.4 y mp.sw.2 de la declaración de



ISO 27001:2013 Controles de Seguridad				
Cláusula	Sección	Objetivo de control / control	Aplica	Justificación
		técnicas		aplicabilidad del ENS
	12.6.2	Restricciones en la instalación de software	Sí	Se corresponde con org.4 y op.acc.4 de la declaración de aplicabilidad del ENS
	12,7	Consideraciones de auditoria de sistemas de información		
	12.7.1	Controles de auditoría de sistemas de información	Sí	Se corresponde con el artículo 34 del anexo III del ENS aunque no tiene correspondencia de forma explícita con ninguno de los controles que propone el ENS por lo que será necesario revisar que este control se encuentre implantado para lograr la certificación en ISO/IEC 27001:2013
13 Seguridad en las Comunicaciones	13,1	Gestión de seguridad en red		
	13.1.1	Controles de red	Sí	Se corresponde con org.4, op.pl.2, op.acc.7, mp.com.2 y mp.com.3 de la declaración de aplicabilidad del ENS
	13.1.2	Seguridad en los servicios en red	Sí	Se corresponde con org.4, op.acc.7, op.mon.1, mp.com.1, mp.com.2 y mp.com.3 de la declaración de aplicabilidad del ENS
	13.1.3	Segregación en redes	Sí	Se corresponde con mp.com.4 de la declaración de aplicabilidad del ENS
	13,2	Transferencia de información		
	13.2.1	Políticas y procedimientos para la transferencia de información	Sí	Se corresponde con org.2, org.3 y mp.com.3 de la declaración de aplicabilidad del ENS
	13.2.2	Acuerdos en la transferencia de información	Sí	Se corresponde con op.ext.1 de la declaración de aplicabilidad del ENS
	13.2.3	Mensajería electrónica	Sí	Se corresponde con mp.s.1 de la declaración de aplicabilidad del ENS



ISO 27001:2013 Controles de Seguridad				
Cláusula	Sección	Objetivo de control / control	Aplica	Justificación
	13.2.4	Acuerdos de confidencialidad o no-revelación	Sí	Se corresponde con mp.per.2 de la declaración de aplicabilidad del ENS
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	14,1	Requerimientos de seguridad en sistemas de información		
	14.1.1	Análisis y especificación de requerimientos de seguridad	Sí	Se corresponde con op.pl.3 de la declaración de aplicabilidad del ENS
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas	Sí	Se corresponde con mp.com.2 y mp.com.3 de la declaración de aplicabilidad del ENS
	14.1.3	Protección de transacciones en servicios de aplicación	Sí	Se corresponde con mp.info.4 y mp.info.5 de la declaración de aplicabilidad del ENS
	14,2	Seguridad en el proceso de desarrollo y soporte		
	14.2.1	Política de desarrollo seguro	Sí	Se corresponde con mp.sw.1 de la declaración de aplicabilidad del ENS
	14.2.2	Procedimientos de control de cambios del sistema	Sí	Se corresponde con op.exp.5 y mp.sw.1 de la declaración de aplicabilidad del ENS
	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	No	Se corresponde con op.exp.5 de la declaración de aplicabilidad del ENS
	14.2.4	Restricción de cambios en paquetes de software	Sí	Se corresponde con org.4 y op.exp.5 de la declaración de aplicabilidad del ENS
	14.2.5	Principios de seguridad en la ingeniería de sistemas	Sí	Se corresponde con op.pl.2 y mp.sw.1 de la declaración de aplicabilidad del ENS
14.2.6	Entorno de desarrollo seguro	No	Se corresponde con mp.sw.1 de la declaración de aplicabilidad del ENS. El Ayto de la UOC no desarrolla software.	



ISO 27001:2013 Controles de Seguridad				
Cláusula	Sección	Objetivo de control / control	Aplica	Justificación
	14.2.7	Desarrollo tercerizado	Sí	Se corresponde con mp.sw.1, mp.sw.2, op.ext.1 y op.ext.2 de la declaración de aplicabilidad del ens
	14.2.8	Pruebas de seguridad del sistema	Sí	Se corresponde con mp.sw.1 y mp.sw.2 de la declaración de aplicabilidad del ens
	14.2.9	Pruebas de aceptación del sistema	Sí	Se corresponde con mp.sw.2 de la declaración de aplicabilidad del ENS
	14,3	Datos de prueba		
	14.3.1	Protección de datos de prueba	Sí	Se corresponde con mp.sw.1 y mp.sw.2 de la declaración de aplicabilidad del ENS
15 Relaciones con Proveedores	15,1	Seguridad de la información en relaciones con el proveedor		
	15.1.1	Política de seguridad de la información en las relaciones con el proveedor	Sí	Se corresponde con org.2, org.4 y op.ext.1 de la declaración de aplicabilidad del ENS
	15.1.2	Atención de tópicos de seguridad en los acuerdos con el proveedor	Sí	Se corresponde con op.ext.1 de la declaración de aplicabilidad del ENS
	15.1.3	Cadena de suministros de tecnologías de la información y comunicaciones	Sí	Se corresponde con op.ext.1 de la declaración de aplicabilidad del ENS
	15,2	Gestión de entrega de servicios de proveedor		
	15.2.1	Monitoreo y revisión de servicios del proveedor	Sí	Se corresponde con op.ext.2 de la declaración de aplicabilidad del ENS
	15.2.2	Gestión de cambios a los servicios del proveedor	Sí	Se corresponde con op.ext.2 y op.exp.5 de la declaración de aplicabilidad del ENS



ISO 27001:2013 Controles de Seguridad				
Cláusula	Sección	Objetivo de control / control	Aplica	Justificación
16 Gestión de Incidentes de Seguridad de la Información	16,1	Gestión de incidentes de seguridad de la información y mejoras		
	16.1.1	Responsabilidades y procedimientos	Sí	Se corresponde con org.2, org.3 y op.exp.7 de la declaración de aplicabilidad del ENS
	16.1.2	Reporte de eventos de seguridad de la información	Sí	Se corresponde con org.3, op.exp.9 y op.exp.7 de la declaración de aplicabilidad del ENS
	16.1.3	Reporte de debilidades de seguridad de la información	Sí	Se corresponde con org.3 y op.exp.7 de la declaración de aplicabilidad del ENS
	16.1.4	Valoración y decisión de eventos de seguridad de la información	Sí	Se corresponde con op.exp.7 de la declaración de aplicabilidad del ENS
	16.1.5	Respuesta a incidentes de seguridad de la información	Sí	Se corresponde con op.exp.7 y op.exp.9 de la declaración de aplicabilidad del ENS
	16.1.6	Aprendizaje de incidentes de seguridad de la información	Sí	Se corresponde con op.exp.7 de la declaración de aplicabilidad del ENS
	16.1.7	Colección de evidencia	Sí	Se corresponde con op.exp.7 y op.exp.9 de la declaración de aplicabilidad del ENS
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	17,1	Continuidad de la seguridad de la información		
	17.1.1	Planeación de la continuidad de la seguridad de la información	No	Se corresponde con op.cont.1 de la declaración de aplicabilidad del ENS
	17.1.2	Implementación de la continuidad de la seguridad de la información	No	Se corresponde con op.cont.2 de la declaración de aplicabilidad del ENS



ISO 27001:2013 Controles de Seguridad				
Cláusula	Sección	Objetivo de control / control	Aplica	Justificación
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	No	Se corresponde con op.cont.3 de la declaración de aplicabilidad del ENS
	17,2	Redundancias		
	17.2.1	Disponibilidad de facilidades de procesamiento de información	No	Se corresponde con mp.if.9, mp.per.9, mp.eq.9, mp.com.9 y mp.s.9 de la declaración de aplicabilidad del ENS
18 Cumplimiento				
	18,1	Cumplimiento con Requerimientos Legales y Contractuales		
	18.1.1	Identificación de legislación aplicable y requerimientos contractuales	Sí	Se corresponde con org.1 de la declaración de aplicabilidad del ENS
	18.1.2	Derechos de propiedad intelectual (IPR)	Sí	Se corresponde con org.2 y org.3 de la declaración de aplicabilidad del ENS
	18.1.3	Protección de registros	Sí	Se corresponde con los artículos 7, 21, 43 y el Anexo I del ENS y forma parte de los principios básicos del ENS.
	18.1.4	Privacidad y protección de información personal identificable (PIR)	Sí	Se corresponde con mp.info.1 de la declaración de aplicabilidad del ENS
	18.1.5	Regulación de controles criptográficos	Sí	Se corresponde con op.acc.7, mp.com.2, mp.info.3 y mp.info.4 de la declaración de aplicabilidad del ENS
	18,2	Revisiones de seguridad de la información		
	18.2.1	Revisión independiente de seguridad de la información	Sí	Se corresponde con el artículo 34 y el Anexo III.



ISO 27001:2013 Controles de Seguridad				
Cláusula	Sección	Objetivo de control / control	Aplica	Justificación
	18.2.2	Cumplimiento con políticas y estándares de seguridad	Sí	Se corresponde con org.2 de la declaración de aplicabilidad del ENS
	18.2.3	Revisión del cumplimiento técnico	Sí	Se corresponde con org.3 y mp.sw.2 de la declaración de aplicabilidad del ENS