
 DEPUTACION PROVINCIAL DE OURENSE	INFORME		INF
	PLAN DE ADECUACIÓN AL R.D. 3/2010 (ESQUEMA NACIONAL DE SEGURIDAD)		
	Nº edición: 01	Revisión: 01	Página 1 de 22


PLAN DE ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD



 DEPUTACION PROVINCIAL DE OURENSE	INFORME		INF
	PLAN DE ADECUACIÓN AL R.D. 3/2010 (ESQUEMA NACIONAL DE SEGURIDAD)		
	Nº edición: 01	Revisión: 01	Página 3 de 22

INDICE

1. INTRODUCCIÓN	4
2. CONTENIDO DEL PLAN DE ADECUACIÓN	6
2.1. PROPUESTA DE POLÍTICA DE SEGURIDAD	7
2.2. IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS	8
2.3. ANÁLISIS Y GESTIÓN DE RIESGOS.....	17
2.4. DECLARACIÓN DE APLICABILIDAD	18
2.5. INFORME DE INSUFICIENCIAS. PLAN DE MEJORA.	22

 <p>DEPUTACION PROVINCIAL DE OURENSE</p>	INFORME		INF
	PLAN DE ADECUACIÓN AL R.D. 3/2010 (ESQUEMA NACIONAL DE SEGURIDAD)		
	Nº edición: 01	Revisión: 01	Página 4 de 22

1. INTRODUCCIÓN

El objetivo principal del presente Plan de Adecuación de la Diputación de Ourense es la identificación del conjunto de acciones y proyectos que son necesarios afrontar para la implantación del Esquema Nacional de Seguridad (en adelante, ENS). El marco de referencia escogido para el desarrollo del presente Plan de Adecuación, ha sido el Reglamento de obligado cumplimiento dentro de las Administraciones Públicas (ENS), regulado por el Real Decreto 3/2010 de 8 de enero, publicado en el BOE número 25 del 29 de enero del 2010 y que establece las medidas mínimas de seguridad para proteger los sistemas de información de la Administración electrónica. Además, en este plan de adecuación se ha tenido en cuenta también el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y se incluyen novedades respecto del Real decreto 3/2010.

El ENS establece 3 tipos de medidas de seguridad:


- **Marco Organizativo:** Son medidas de carácter global referidas a la forma en que la Organización gestiona la seguridad y que tienen una componente puramente organizativa proporcionando el marco normativo y procedimental que debe regular la gestión y uso de los sistemas de información.

1. Marco Organizativo
1.1. Política de Seguridad
1.2. Normativa de Seguridad
1.3. Procedimientos de Seguridad
1.4. Proceso de Autorización

- **Marco Operacional:** Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.


2. Marco Operacional
2.1. Planificación
2.2. Control de Acceso
2.3. Explotación
2.4. Servicios Externos
2.5. Continuidad del Servicio
2.6. Monitorización del Sistema

- **Medidas de Protección:** Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas. Establece medidas de seguridad tangibles sobre cada uno de los tipos de activos que todo sistema de información va a contener.

 DEPUTACION PROVINCIAL DE OURENSE	INFORME		INF
	PLAN DE ADECUACIÓN AL R.D. 3/2010 (ESQUEMA NACIONAL DE SEGURIDAD)		
	Nº edición: 01	Revisión: 01	Página 5 de 22

3. Medidas de Protección
3.1. Protección de las instalaciones e infraestructuras
3.2. Gestión del Personal
3.3. Protección de los equipos
3.4. Protección de las comunicaciones
3.5. Protección de los soportes de información
3.6. Protección de las aplicaciones informáticas
3.7. Protección de la información
3.8. Protección de los servicios

Para la puesta en marcha del cumplimiento de las medidas de seguridad del ENS, se establece en el presente informe ejecutivo el plan de actuaciones a realizar contemplando las recomendaciones establecidas en el documento “Guía 804 Medidas de implantación del ENS”, publicado por el Centro Criptológico Nacional.


 DEPUTACION PROVINCIAL DE OURENSE	INFORME		INF
	PLAN DE ADECUACIÓN AL R.D. 3/2010 (ESQUEMA NACIONAL DE SEGURIDAD)		
	Nº edición: 01	Revisión: 01	Página 6 de 22

2. CONTENIDO DEL PLAN DE ADECUACIÓN

El plan de adecuación ha sido elaborado siguiendo las recomendaciones de la “Guía 806 - Plan de Adecuación del Esquema Nacional de Seguridad” y tal como expresa el citado documento, el contenido del plan debe contener la siguiente información:

1. la política de seguridad
2. información que se maneja, con su valoración
3. servicios que se prestan, con su valoración
4. datos de carácter personal, que deberá recogerse en el correspondiente Registro de Actividades del Tratamiento de la entidad, así como en la documentación vinculada a esta materia
5. categoría del sistema
6. análisis de riesgos
7. declaración de aplicabilidad de las medidas del Anexo II del ENS
8. insuficiencias del sistema (gap analysis)
9. plan de mejora seguridad.

El Plan de adecuación se compone de un conjunto de documentos o entregables que cubren todos los aspectos citados por la Guía 806 y que se nombran a continuación:

 <p>DEPUTACION PROVINCIAL DE OURENSE</p>	INFORME		INF
	PLAN DE ADECUACIÓN AL R.D. 3/2010 (ESQUEMA NACIONAL DE SEGURIDAD)		
	Nº edición: 01	Revisión: 01	Página 7 de 22

2.1. PROPUESTA DE POLÍTICA DE SEGURIDAD

Este documento debe, además, contemplar los requisitos establecidos por la medida “ORG.1. Política de Seguridad” que indica los contenidos mínimos que debe satisfacer una política de seguridad de acuerdo con el R.D. 3/2010.


ENTREGABLES:



1. Propuesta de Política de Seguridad



Política de Seguridad de la Información.doc

 <p>DEPUTACION PROVINCIAL DE OURENSE</p>	INFORME		INF
	PLAN DE ADECUACIÓN AL R.D. 3/2010 (ESQUEMA NACIONAL DE SEGURIDAD)		
	Nº edición: 01	Revisión: 01	Página 8 de 22

2.2. IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS


Este documento recoge la información que se trata junto a los servicios prestados, relacionados con la identificación de los sistemas de información que dan soporte a los procesos de administración electrónica sometidos al cumplimiento del R.D. 3/2010 de desarrollo del Esquema Nacional de Seguridad. En dicho documento, han sido identificados los siguientes puntos:

- información que se maneja, con su valoración
- servicios que se prestan, con su valoración

CRITERIOS DE VALORACIÓN

Cada activo se valorará con los criterios definidos en la guía **CCN-STIC-803, ESQUEMA NACIONAL DE SEGURIDAD, VALORACIÓN DE LOS SISTEMAS.**

- **D: Disponibilidad.** Propiedad o característica de los activos consistente en que los usuarios o los procesos autorizados tienen acceso a los mismos cuando lo requieran. Para valorar este criterio la pregunta a responder será: ¿Qué importancia tendría que el activo no estuviera disponible cuando se necesita?
- **I: Integridad.** Propiedad o característica consistente en la exactitud y completitud de la información y los métodos de su procesamiento. Para valorar este criterio la pregunta a responder será: ¿Qué importancia tendría que el activo fuera alterado sin control?
- **C: Confidencialidad.** Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos no autorizados. La pregunta a responder para valorar un activo en este criterio será: ¿Qué importancia tendría que el activo fuera revelado a personas no autorizadas?
- **T: Trazabilidad.** Propiedad o característica consistente en que las actuaciones llevadas a cabo pueden ser imputadas exclusivamente a quién las ha realizado. La valoración de este criterio responde a la pregunta de ¿qué importancia tendría no poder identificar a quien haya ejecutado una acción?
- **A: Autenticidad.** Propiedad o característica consistente en que, quien accede al activo, es quien dice ser o bien se garantiza la fuente de la que proceden los datos. La pregunta aquí sería, ¿qué importancia tendría que quién accede no es quién dice ser?

 DEPUTACION PROVINCIAL DE OURENSE	INFORME		INF
	PLAN DE ADECUACIÓN AL R.D. 3/2010 (ESQUEMA NACIONAL DE SEGURIDAD)		
	Nº edición: 01	Revisión: 01	Página 9 de 22

Para valorar los activos en cada uno de estos criterios se utiliza una escala de varios puntos, como sigue.

CRITERIOS PARA LA DISPONIBILIDAD DE SERVICIOS				
	No Adscrito (N/A)	BAJO	MEDIO	ALTO
RTO – Tiempo Objetivo de Recuperación	DIS.RTO.N La restauración de los niveles mínimos de servicio puede realizarse en un plazo superior a 5 días (RTO)	DIS.RTO.B La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 5 días (RTO)	DIS.RTO.M La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 1 día (RTO)	DIS.RTO.A La restauración de los niveles mínimos de servicio debe realizarse en un plazo máximo de 4 horas (RTO)

**PLAN DE ADECUACIÓN AL R.D. 3/2010
(ESQUEMA NACIONAL DE SEGURIDAD)**

Nº edición: 01

Revisión: 01

Página 10 de 22

**CRITERIOS COMUNES APLICABLES A TODAS LAS DIMENSIONES DE TIPOS DE INFORMACIÓN
Y SERVICIOS**

		No Adscrito (N/A)	BAJO	MEDIO	ALTO
Disposición legal o administrativa		COM.DIS.N No existe ninguna disposición legal que condicione su nivel.	COM.DIS.B Por disposición legal o administrativa: ley, decreto, orden, reglamento...	COM.DIS.M Por disposición legal o administrativa: ley, decreto, orden, reglamento...	COM.DIS.A Por disposición legal o administrativa: ley, decreto, orden, reglamento...
Perjuicio Directo al ciudadano		COM.PER.N No supone ningún perjuicio directo al ciudadano	COM.PER.B Algún perjuicio al ciudadano	COM.PER.M Daño importante, aunque subsanable al ciudadano	COM.PER.A Grave daño, de difícil o imposible reparación al ciudadano
Incumplimiento de una Norma	Legal	COM.LEG.N No implica incumplimiento de una norma jurídica	COM.LEG.B Incumplimiento formal leve de una norma jurídica, de carácter subsanable	COM.LEG.M Incumplimiento material de una norma jurídica, o incumplimiento formal no subsanable	COM.LEG.A Incumplimiento grave de una norma jurídica
	Regulatoria	COM.REG.N No implica incumplimiento de normativa de un regulador	COM.REG.B Implica incumplimiento de normativa de un regulador	COM.REG.M Implica sanción significativa de un regulador	COM.REG.A Implica sanción grave de un regulador y/o pérdida de licencia de operar
	Contractual	COM.CON.N No implica incumplimiento de una obligación contractual	COM.CON.B Incumplimiento leve de una obligación contractual	COM.CON.M Incumplimiento material o formal de una obligación contractual	COM.CON.A Incumplimiento grave de una obligación contractual
	Interna	COM.INT.N No implica incumplimiento de normativa interna	COM.INT.B Incumplimiento leve de una norma interna	COM.INT.M Incumplimiento material o formal de una norma interna	COM.INT.A Incumplimiento grave de una norma interna

**PLAN DE ADECUACIÓN AL R.D. 3/2010
(ESQUEMA NACIONAL DE SEGURIDAD)**

Nº edición: 01

Revisión: 01

Página 11 de 22

**CRITERIOS COMUNES APLICABLES A TODAS LAS DIMENSIONES DE TIPOS DE
INFORMACIÓN Y SERVICIOS**

	No Adscrito (N/A)	BAJO	MEDIO	ALTO
Pérdidas económicas	COM.ECO.N No implica pérdidas económicas	COM.ECO.B Pérdidas económicas apreciables (inferior a un 4% del presupuesto anual de la organización)	COM.ECO.M Pérdidas económicas importantes (igual o superior a un 4% e inferior a un 10% del presupuesto anual de la organización)	COM.ECO.A Pérdidas económicas o alteraciones financieras significativas (igual o superior a un 10% del presupuesto anual de la organización)
Reputación	COM.REP.N No implica daño reputacional	COM.REP.B Daño reputacional apreciable con los ciudadanos o con otras organizaciones	COM.REP.M Daño reputacional importante con los ciudadanos o con otras organizaciones	COM.REP.A Daño reputacional grave con los ciudadanos o con otras organizaciones
Protestas	COM.PRO.N No se prevé que pueda desembocar en protestas.	COM.PRO.B Múltiples protestas individuales.	COM.PRO.M Protestas públicas (alteración del orden público)	COM.PRO.A Protestas masivas (alteración seria del orden público)
Delitos	COM.DEL.N No facilitaría la comisión de delitos ni dificultaría su investigación.	COM.DEL.B Favorecería la comisión de delitos	COM.DEL.M Favorecería significativamente la comisión de delitos o dificultaría su investigación.	COM.DEL.A Incitaría a la comisión de delitos, constituiría en sí un delito, o dificultaría enormemente su investigación.


PLAN DE ADECUACIÓN AL R.D. 3/2010
(ESQUEMA NACIONAL DE SEGURIDAD)

Nº edición: 01

Revisión: 01

Página 12 de 22

CRITERIOS PARA TIPOS DE INFORMACIÓN CON DATOS PERSONALES EN FUNCIÓN DEL TIPO		
BAJO	MEDIO	ALTO
<p>PRI.TIP.B</p> <p>Datos de carácter personal con carácter general.</p>	<p>PRI.TIP.M</p> <p>Incluye datos de carácter personal:</p> <p>a) Relativos a la comisión de infracciones administrativas.</p> <p>b) Aquellos cuyo funcionamiento se rija por el artículo 29 de L.O. 15/1999, de 13 de diciembre.</p> <p>c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.</p> <p>d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.</p> <p>e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.</p> <p>f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.</p> <p>Datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y libertades fundamentales, incluidos:</p> <ul style="list-style-type: none"> • Origen étnico o racial (RGPD, art. 9). • Opiniones políticas (RGPD, art. 9). • Convicciones religiosas o filosóficas (RGPD, art. 9). • Afiliación sindical (RGPD, art. 9). • Datos genéticos (RGPD, art. 9). • Datos biométricos dirigidos a identificar de manera unívoca a una persona física (RGPD, art. 9). • Datos relativos a salud (RGPD, art. 9). • Datos relativos a la vida sexual u orientaciones sexuales (RGPD, art. 9). • Condenas e infracciones penales (RGPD, art. 10). 	

 DEPUTACION PROVINCIAL DE OURENSE	INFORME		INF
	PLAN DE ADECUACIÓN AL R.D. 3/2010 (ESQUEMA NACIONAL DE SEGURIDAD)		
	Nº edición: 01	Revisión: 01	Página 13 de 22

CRITERIOS PARA TIPOS DE INFORMACIÓN CON DATOS PERSONALES EN FUNCIÓN DEL TRATAMIENTO				
	N/A	BAJO	MEDIO	ALTO
Cantidad considerable de datos personales			PRI.CAN.M Operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañen probablemente un alto riesgo, por ejemplo, debido a su sensibilidad, cuando, en función del nivel de conocimientos técnicos alcanzado, se haya utilizado una nueva tecnología a gran escala (RGPD, 91)	
Importante riesgo para los derechos y libertades de los interesados			PRI.DER.M Operación de tratamiento que entraña un alto riesgo para los derechos y libertades de los interesados, en particular cuando esta operación hace más difícil para los interesados el ejercicio de sus derechos (RGPD, 91)	
Evaluación sistemática y exhaustiva de aspectos personales			PRI.ASP.M Operación de tratamiento para adoptar decisiones relativas a personas físicas concretas a raíz de una evaluación sistemática y exhaustiva de aspectos personales propios de personas físicas, basada en la elaboración de perfiles de dichos datos o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas (RGPD, 91)	
Control de zonas de acceso público a gran escala			PRI.ACC.M Operaciones de control de zonas de acceso público a gran escala, en particular cuando se utilicen dispositivos optoelectrónicos (RGPD, 91)	

CATEGORÍA DEL SISTEMA

Para categorizar el Sistema según el ENS, se detallan a continuación las valoraciones de cada uno de los activos esenciales. Como establece el ENS, el nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio. Consecuentemente, la categoría del Sistema viene dada por el valor máximo en cada dimensión.

A los distintos activos se les aplicará, como mínimo, aquellas medidas de seguridad estipuladas para su nivel en el Anexo II, Medidas de Seguridad, del ENS.

PLAN DE ADECUACIÓN AL R.D. 3/2010
(ESQUEMA NACIONAL DE SEGURIDAD)

Nº edición: 01

Revisión: 01

Página 14 de 22


CAPA	ACTIVO	DIMENSIONES				
		[D]	[I]	[C]	[A]	[T]
	[S] SERVICIOS					
	[S01] Registro General y Electrónico de Entrada y Salida	[M]				
	[S02] Expedientes Administrativos	[M]				
	[S03] Archivo	[M]				
	[S04] Licitación Electrónica y Perfil del Contratante	[M]				
	[S05] Carpeta Ciudadana	[M]				
	[S06] Quejas y Sugerencias	[B]				
	[S07] Gestión Sancionadora	[M]				
	[S08] Portal de Transparencia	[M]				
	[S09] Boletín Oficial de la Provincia	[M]				
	[S10] Avisos y Notificaciones	[B]				
	[S11] Atención de Derechos de Protección de Datos	[M]				
	[S12] Registro de Bienes e Intereses	[M]				
	[S13] Asesoría Jurídica	[M]				
	[S14] Gestión Patrimonial	[M]				
	[S15] Intervención	[M]				
	[S16] Gestión Tributaria	[M]				
	[S17] Tesorería	[M]				
	[S18] Presupuesto	[M]				
	[S19] Personal	[B]				
	[S20] Bolsa de Empleo Público	[M]				
	[S21] Agencia de Desarrollo Local	[B]				
	[S22] Instalaciones	[B]				
	[S23] Eventos y Actividades	[B]				
	[S24] Premios y Certámenes	[B]				
	[S25] Escuelas de la provincia (Gaitas, Oficios y Danza)	[B]				
	[S26] Biblioteca	[B]				
	[S27] Subvenciones	[M]				
	[S28] Oficina de Turismo (INORDE)	[B]				
	[S29] Registro de Entidades Ciudadanas	[B]				
	[S30] Planeamiento Urbanístico	[M]				
	[S31] Obras Públicas	[M]				
	[S32] Promoción Empresarial	[B]				
	[S33] Consorcio Provincial de Ourense para la prestación del servicio contra incendios y salvamento	[M]				
	[S34] Consorcio de aguas de Valdeorras	[M]				
	[S35] Video vigilancia de Edificios	[M]				
	[S36] Prevención y Salud	[M]				


PLAN DE ADECUACIÓN AL R.D. 3/2010
(ESQUEMA NACIONAL DE SEGURIDAD)

Nº edición: 01

Revisión: 01

Página 15 de 22

	[S37] Perreras	[B]				
	[S38] Asistencia a domicilio y Teleasistencia	[M]				
	[S39] Servicio de aguas, Limpieza y recogida de residuos	[M]				
	[S40] Web corporativa	[M]				
	[S41] Provincia Inteligente (Smart City)	[M]				
	[S42] Grabación y Retransmisión de Plenos, Comisiones, Aperturas de plicas y Sorteos	[M]				
	[S43] Notificación de Brechas de Seguridad	[M]				
	[S44] Programa de Termalismo	[B]				
	[S45] Servicio TIC	[B]				
	[IN] INFORMACIÓN					
	[IN01] Registro		[M]	[M]	[M]	[M]
	[IN02] Expedientes Administrativos		[M]	[M]	[M]	[M]
	[IN03] Personal		[M]	[M]	[B]	[B]
	[IN04] Bolsa de empleo		[M]	[M]	[M]	[M]
	[IN05] Contable, Económica, Financiera y Presupuestaria		[M]	[B]	[M]	[M]
	[IN06] Tributaria y Recaudación		[M]	[M]	[M]	[M]
	[IN07] Patrimonio		[M]	[B]	[M]	[M]
	[IN08] Responsabilidad Patrimonial		[M]	[M]	[M]	[M]
	[IN09] Contratación		[M]	[B]	[M]	[M]
	[IN10] Vías y Obras		[M]	[M]	[M]	[M]
	[IN11] Videovigilancia de Edificios		[M]	[B]	[M]	[M]
	[IN12] Promoción empresarial y emprendimiento		[B]	[B]	[B]	[B]
	[IN13] Actividades y Eventos Culturales y Deportivos		[B]	[B]	[B]	[B]
	[IN14] Subvenciones		[M]	[M]	[M]	[M]
	[IN15] Biblioteca y Archivos		[B]	[B]	[B]	[B]
	[IN16] Escuelas de la provincia (Gaitas, Oficios y Danza)		[B]	[B]	[B]	[B]
	[IN17] Actividades de Certámenes y Concursos		[B]	[B]	[B]	[B]
	[IN18] Asesoría Jurídica		[M]	[M]	[M]	[M]
	[IN19] Ayuda a domicilio y teleasistencia		[M]	[M]	[M]	[M]
	[IN20] Bienestar		[M]	[M]	[M]	[M]
	[IN21] Medio Ambiente		[M]	[M]	[M]	[M]
	[IN22] Información del consorcio contra incendios		[M]	[M]	[M]	[M]
	[IN23] Información del consorcio de aguas		[M]	[M]	[M]	[M]
	[IN24] Canal de Denuncias		[M]	[M]	[M]	[M]
	[IN25] Registro de Entidades Ciudadanas		[M]	[B]	[M]	[M]
	[IN26] Registro de Bienes e Intereses		[M]	[M]	[M]	[M]
	[IN27] Perreras		[B]	[M]	[M]	[M]
	[IN28] Gestión de la salud en el trabajo - PRL		[M]	[M]	[M]	[M]
	[IN29] Grabación y Retransmisión de Plenos, Comisiones, Aperturas de plicas y Sorteos		[M]	[0]	[M]	[M]
	[IN30] Información del servicio Provincia inteligente		[M]	[M]	[M]	[M]

 DEPUTACION PROVINCIAL DE OURENSE	INFORME		INF	
	PLAN DE ADECUACIÓN AL R.D. 3/2010 (ESQUEMA NACIONAL DE SEGURIDAD)			
	Nº edición: 01	Revisión: 01	Página 16 de 22	

[IN31] Publicaciones Web	[B]	[O]	[B]	[B]
[IN32] Instalaciones Municipales	[B]	[B]	[B]	[B]
[IN33] Carpeta Ciudadana	[M]	[M]	[M]	[M]
[IN34] Portal de Transparencia	[M]	[O]	[M]	[M]
[IN35] Boletín Oficial de la Provincia	[M]	[O]	[M]	[M]
[IN36] Quejas y Sugerencias	[B]	[B]	[B]	[B]
[IN37] Avisos y Notificaciones	[B]	[B]	[B]	[B]
[IN38] Gestión RGPD	[M]	[M]	[M]	[M]
[IN39] Turismo	[B]	[B]	[B]	[B]
[IN40] Información de Termalismo	[B]	[B]	[B]	[B]
[IN41] Información de departamento TIC	[B]	[B]	[B]	[B]


Tras lo cual, se determina que la categoría del sistema es: **MEDIA**.

ENTREGABLES:

2. Categorización de activos + dependencias

 Inventario y valoración de activos.xlsx

 Dependencias.xlsx

 <p>DEPUTACION PROVINCIAL DE OURENSE</p>	INFORME		INF
	PLAN DE ADECUACIÓN AL R.D. 3/2010 (ESQUEMA NACIONAL DE SEGURIDAD)		
	Nº edición: 01	Revisión: 01	Página 17 de 22

2.3. ANÁLISIS Y GESTIÓN DE RIESGOS

Uno de los requisitos de mayor importancia que establece el ENS para su cumplimiento, es la incorporación al plan de adecuación de un análisis de los riesgos a los que está sometida la organización, según lo descrito en su Anexo II, sección op.pl.1 para la categoría definida para el sistema.

En dicho análisis de riesgos se valoran las salvaguardas/medidas ya presentes en la fecha de aprobación del plan de adecuación para así obtener unos resultados lo más ajustados a la realidad y con el objetivo de identificar a posteriori medidas adicionales que permitan reducir en lo posible, los niveles de riesgos a los límites de aceptación previamente definidos.

ENTREGABLES:

3. Análisis de riesgos

 Informe sobre el Tratamiento de riesgos.pdf

 Análisis de riesgos.mgr

METODOLOGÍA DE ANÁLISIS DE RIESGOS


El Análisis de Riesgos sobre los sistemas de la Diputación de Ourense ha sido realizado de acuerdo a la metodología Magerit v.3, reconocida internacionalmente y que cubre todos los requisitos del ENS descritos en su sección op.pl.1.

En el presente documento se detalla todas las fases de la metodología, incluyendo los criterios de valoración y fórmulas de los cálculos realizados.

ENTREGABLES:

3. Análisis de riesgos

 Metodología Magerit v.3.pdf

 DEPUTACION PROVINCIAL DE OURENSE	INFORME		INF
	PLAN DE ADECUACIÓN AL R.D. 3/2010 (ESQUEMA NACIONAL DE SEGURIDAD)		
	Nº edición: 01	Revisión: 01	Página 18 de 22

2.4. DECLARACIÓN DE APLICABILIDAD

En la siguiente tabla se detallan las medidas de seguridad contenidas en el Anexo II del Esquema Nacional de Seguridad y la necesidad de aplicación de las mismas teniendo en cuenta las categorías de los sistemas identificados.

Cada medida de seguridad tendrá uno de los dos estados siguientes:

- No Aplica: Control no seleccionado debido a que no es obligatorio según la categoría del sistema.
- Aplica: Control seleccionado por requerimiento del ENS para la categoría del Sistema. La medida puede estar ya implantada a la fecha de realización del presente Documento o bien se prevé implementar en los plazos determinados por el ENS, tal y como se define en el Plan de Mejora de la seguridad.

Además, a continuación del estado, se indicará un código para indicar el nivel en el que tiene que aplicarse la medida (M – Medio; B – Bajo).

Dimensiones afectadas	Tipo de medida	Medida de seguridad	Sistema Nivel Medio
	ORG	MARCO ORGANIZATIVO	
categoría	org.1	Política de seguridad	Aplica – B
categoría	org.2	Normativa de seguridad	Aplica – B
categoría	org.3	Procedimientos de seguridad	Aplica – B
categoría	org.4	Proceso de autorización	Aplica – B
	OP	MARCO OPERACIONAL	
	op.pl	Planificación	
categoría	op.pl.1	Análisis de riesgos	Aplica – M
categoría	op.pl.2	Arquitectura de seguridad	Aplica – M
categoría	op.pl.3	Adquisición de nuevos componentes	Aplica – B
D	op.pl.4	Dimensionamiento /Gestión de capacidades	Aplica – M
categoría	op.pl.5	Componentes certificados	No Aplica
	op.acc	Control de acceso	
A T	op.acc.1	Identificación	Aplica - B
I C A T	op.acc.2	Requisitos de acceso	Aplica – B

**PLAN DE ADECUACIÓN AL R.D. 3/2010
(ESQUEMA NACIONAL DE SEGURIDAD)**

Nº edición: 01

Revisión: 01

Página 19 de 22

Dimensiones afectadas	Tipo de medida	Medida de seguridad	Sistema Nivel Medio
I C A T	op.acc.3	Segregación de funciones y tareas	Aplica – M
I C A T	op.acc.4	Acceso de gestión de derecho de acceso	Aplica – B
I C A T	op.acc.5	Mecanismo de autenticación	Aplica – M
I C A T	op.acc.6	Acceso local (local logon)	Aplica – M
I C A T	op.acc.7	Acceso remoto (remote login)	Aplica – M
	op.exp	Explotación	
categoría	op.exp.1	Inventario de activos	Aplica - B
categoría	op.exp.2	Configuración de seguridad	Aplica – B
categoría	op.exp.3	Gestión de la configuración	Aplica - M
categoría	op.exp.4	Mantenimiento	Aplica – B
categoría	op.exp.5	Gestión de cambios	Aplica – M
categoría	op.exp.6	Protección frente a código dañino	Aplica – B
categoría	op.exp.7	Gestión de incidencias	Aplica – M
T	op.exp.8	Registro de la actividad de los usuarios	Aplica – M
categoría	op.exp.9	Registro de la gestión de incidencias	Aplica – M
T	op.exp.10	Protección de los registros de actividad	No Aplica
categoría	op.exp.11	Protección de claves criptográficas	Aplica – M
	op.ext	Servicios externos	
categoría	op.ext.1	Contratación y acuerdos de nivel de servicio	Aplica – M
categoría	op.ext.2	Gestión diaria	Aplica – M
D	op.ext.9	Medios alternativos	No Aplica
	op.cont	Continuidad del servicio	
D	op.cont.1	Análisis de impacto	Aplica – M
D	op.cont.2	Plan de continuidad	No Aplica
D	op.cont.3	Pruebas periódicas	No Aplica
	op.mon	Monitorización del sistema	
categoría	op.mon.1	Detección de intrusión	Aplica – M
categoría	op.mon.2	Sistema de métricas	Aplica – M
	MP	MEDIDAS DE PROTECCIÓN	


**PLAN DE ADECUACIÓN AL R.D. 3/2010
(ESQUEMA NACIONAL DE SEGURIDAD)**

Nº edición: 01

Revisión: 01

Página 20 de 22

Dimensiones afectadas	Tipo de medida	Medida de seguridad	Sistema Nivel Medio
	mp.if	Protección de las instalaciones e infraestructuras	
categoría	mp.if.1	Áreas separadas y con control de acceso	Aplica – B
categoría	mp.if.2	Identificación de las personas	Aplica – B
categoría	mp.if.3	Acondicionamiento de los locales	Aplica – B
D	mp.if.4	Energía eléctrica	Aplica – M
D	mp.if.5	Protección frente a incendios	Aplica – B
D	mp.if.6	Protección frente a inundaciones	Aplica – M
categoría	mp.if.7	Registro de entrada y salida de equipamiento	Aplica – B
D	mp.if.9	Instalaciones alternativas	No Aplica
	mp.per	Gestión del personal	
categoría	mp.per.1	Caracterización del puesto de trabajo	Aplica – M
categoría	mp.per.2	Deberes y obligaciones	Aplica – B
categoría	mp.per.3	Concienciación	Aplica - B
categoría	mp.per.4	Formación	Aplica – B
D	mp.per.9	Personal alternativo	No Aplica
	mp.eq	Protección de los equipos	
categoría	mp.eq.1	Puesto de trabajo despejado	Aplica – M
A	mp.eq.2	Bloqueo de puesto de trabajo	Aplica – M
categoría	mp.eq.3	Protección de equipos portátiles	Aplica – B
D	mp.eq.9	Medios alternativos	Aplica – M
	mp.com	Protección de las comunicaciones	
categoría	mp.com.1	Perímetro seguro	Aplica – B
C	mp.com.2	Protección de la confidencialidad	Aplica – M
I A	mp.com.3	Protección de la autenticidad y de la integridad	Aplica – M
categoría	mp.com.4	Segregación de redes	No Aplica
D	mp.com.9	Medios alternativos	No Aplica
	mp.si	Protección de los soportes de información	


 DEPUTACION PROVINCIAL DE OURENSE	INFORME		INF
	PLAN DE ADECUACIÓN AL R.D. 3/2010 (ESQUEMA NACIONAL DE SEGURIDAD)		
	Nº edición: 01	Revisión: 01	Página 21 de 22

Dimensiones afectadas	Tipo de medida	Medida de seguridad	Sistema Nivel Medio
C	mp.si.1	Etiquetado	Aplica – B
I C	mp.si.2	Criptografía	Aplica – M
categoría	mp.si.3	Custodia	Aplica - B
categoría	mp.si.4	Transporte	Aplica – B
C	mp.si.5	Borrado y destrucción	Aplica – M
	mp.sw	Protección de las aplicaciones informáticas	
categoría	mp.sw.1	Desarrollo	Aplica – M
categoría	mp.sw.2	Aceptación y puesta en servicio	Aplica – M
	mp.info	Protección de la información	
categoría	mp.info.1	Datos de carácter personal	Aplica – B
C	mp.info.2	Calificación de la información	Aplica – M
C	mp.info.3	Cifrado	No Aplica
I A	mp.info.4	Firma electrónica	Aplica – M
T	mp.info.5	Sellos de tiempo	No aplica
C	mp.info.6	Limpieza de documentos	Aplica – B
D	mp.info.9	Copias de seguridad (back Up)	Aplica – B
	mp.s	Protección de los servicios	
categoría	mp.s.1	Protección del correo electrónico	Aplica – B
categoría	mp.s.2	Protección de servicios y aplicaciones web	Aplica – B
D	mp.s.8	Protección frente a la denegación de servicio	Aplica – M
D	mp.s.9	Medios alternativos	No Aplica

ENTREGABLES:

4. Plan de mejora

 Informe Análisis diferencial ENS.pdf

 <p>DEPUTACION PROVINCIAL DE OURENSE</p>	INFORME		INF
	PLAN DE ADECUACIÓN AL R.D. 3/2010 (ESQUEMA NACIONAL DE SEGURIDAD)		
	Nº edición: 01	Revisión: 01	Página 22 de 22

2.5. INFORME DE INSUFICIENCIAS. PLAN DE MEJORA

Estos documentos establecen cual es la situación de partida respecto al contenido de cada una de las medidas de seguridad establecidas por el R.D. 3/2010, considerando de aplicación la categoría establecida de nivel **MEDIO**.

De igual modo, estos documentos establecen qué tareas son necesarias llevar a cabo para solventar las deficiencias detectadas.

ENTREGABLES:

4. Plan de mejora

 Informe de insuficiencias.pdf

 Informe Análisis diferencial ENS.pdf