

ASUNTO: Erratas en la publicación del R.D 951/2015, de 23 de octubre.

En ningún caso se está introduciendo modificación alguna en el texto a corregir a excepción de simples erratas al existir discordancia entre la tabla recopilatorio y el apartado correspondiente donde se explica el alcance y aplicación concreta de la medida de seguridad concernida, como a continuación se detalla:

Errata 1: Arquitectura de seguridad [op.pl.2]

(Discordancia entre la tabla recopilatorio y el apartado falta un + en el apartado 4.1.2 al existir incremento de exigencias como se indica en el desarrollo del apartado indicado)

Página 104250

Dice la tabla:

Trece. La tabla del apartado 2.4 del anexo II, queda redactada como sigue:

categoria	básica	media	alta		
medida	aplica	+	++	Op.pl.2	Arquitectura de seguridad

.....

página 104252

Dice el apartado 4.1.2

«4.1.2 Arquitectura de seguridad [op.pl.2].

dimensiones	todas		
categoria	básica	media	alta
medida	aplica	+	+

...La seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:

Categoría BÁSICA

a) Documentación de las instalaciones:

1. Áreas.

2. Puntos de acceso.

b) Documentación del sistema:

1. Equipos.

2. Redes internas y conexiones al exterior.

3. Puntos de acceso al sistema (puestos de trabajo y consolas de administración).

c) Esquema de líneas de defensa:

1. Puntos de interconexión a otros sistemas o a otras redes, en especial si se trata de Internet o redes públicas en general.

2. Cortafuegos, DMZ, etc.

3. Utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

d) Sistema de identificación y autenticación de usuarios:

1. Uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga.

2. Uso de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso.

Categoría MEDIA

e) Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información.

Categoría ALTA

f) Sistema de gestión de seguridad de la información con actualización y aprobación periódica.

g) Controles técnicos internos:

1. Validación de datos de entrada, salida y datos intermedios.

Debe decir el apartado 4.1.2

dimensiones	todas		
categoría	básica	media	alta
medida	aplica	+	++

Toda vez que existen incremento de exigencia en la aplicación de medidas específicas para los sistemas de categoría ALTA y así debe reflejarse como se indica en el apartado 4. letra d del punto 2. Selección de Medidas de Seguridad con dos + en cuadro en rojo.

....En las tablas del presente Anexo se emplean las siguientes convenciones:

a) Para indicar que una determinada medida de seguridad se debe aplicar a una o varias dimensiones de seguridad en algún nivel determinado se utiliza la voz «aplica».

b) «n.a.» significa «no aplica».

c) Para indicar que las exigencias de un nivel son iguales a los del nivel inferior se utiliza el signo «=».

d) Para indicar el incremento de exigencias graduado en función de del nivel de la dimensión de seguridad, se utilizan los signos «+» y «++»....

e) Para indicar que una medida protege específicamente una cierta dimensión de seguridad, ésta se explicita mediante su inicial.

f) En las tablas del presente anexo se han empleado colores verde, amarillo y rojo de la siguiente forma: el color verde para indicar que una cierta medida se aplica en sistemas de categoría BÁSICA o superior; el amarillo para indicar las medidas que empiezan a aplicarse en categoría MEDIA o superior; el rojo para indicar las medidas que sólo son de aplicación en categoría ALTA.

Errata 2: Componentes certificados [op.pl.5]

(discordancia entre la tabla recopilatorio y el apartado en el color de la celda debe ser rojo cuando la medida solo aplica a esta categoría ALTA según se indica en las observaciones a pie de tabla en el mismo texto legal apartado 4.1etra f del punto 2. Selección de Medidas de Seguridad)

Página 104250

Dice la tabla:

Trece. La tabla del apartado 2.4 del anexo II, queda redactada como sigue:

categoría	básica	media	alta		
medida	n.a	n.a.	aplica	Op.pl.5	Componentes certificados

.....

página 104253

Dice el apartado 4.1.5

«4.1.5 Componentes certificados[op.pl.5].

dimensiones	todas		
categoría	básica	media	alta
medida	n.a.	n.a.	aplica

Debe decir el apartado 4.1.5

dimensiones	Todas		
categoría	básica	media	alta
medida	n.a.	n.a.	aplica

Errata 3: Sistema de métricas [op.mon.2]

(discordancia entre la tabla recopilatorio y el apartado)

página 104259

Dice el apartado 4.6.2

«4.6.2 Sistema de métricas [op.mon.2].

dimensiones	Todas		
categoría	básica	media	alta
medida	aplica	+	++

.....(Y sigue la explicación de la aplicación de medidas concretas en las tres categorías BÁSICA, MEDIA y ALTA).....

.....Categoría BÁSICA:

Se recopilarán los datos necesarios atendiendo a la categoría del sistema para conocer el grado de implantación de las medidas de seguridad que apliquen de las detalladas en el Anexo II y, en su caso, para proveer el informe anual requerido por el artículo 35.

Categoría MEDIA:

Además, se recopilarán datos para valorar el sistema de gestión de incidentes, permitiendo conocer

- Número de incidentes de seguridad tratados.
- Tiempo empleado para cerrar el 50% de los incidentes.
- Tiempo empleado para cerrar el 90% de los incidentes.

Categoría ALTA

Se recopilarán datos para conocer la eficiencia del sistema de seguridad TIC:

- Recursos consumidos: horas y presupuesto.

Página 104250

Dice la tabla:

Trece. La tabla del apartado 2.4 del anexo II, queda redactada como sigue:

categoría	básica	media	alta		
medida	n.a.	n.a.	aplica	op.mon.2	Sistema de métricas

Debe decir la tabla:

categoría	básica	media	alta		
medida	aplica	+	++	op.mon.2	Sistema de métricas

Errata 4: Borrado y destrucción [mp.si.5]

(discordancia entre la tabla recopilatorio y el apartado)

Página 104251

Dice la tabla:

Trece. La tabla del apartado 2.4 del anexo II, queda redactada como sigue:

nivel	bajo	medio	alto		
C	aplica	+	=	mp.si.5	Borrado y destrucción

.....

página 104262

Dice el apartado 5.5.5

«5.5.5 Borrado y destrucción [mp.si.5].

dimensiones	D		
nivel	bajo	medio	alto
medida	n.a.	+	=

La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

Nivel BAJO

- a) Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su contenido.

Nivel MEDIO

- b) Se destruirán de forma segura los soportes, en los siguientes casos:
1. Cuando la naturaleza del soporte no permita un borrado seguro.
 2. Cuando así lo requiera el procedimiento asociado al tipo de información contenida.
- c) Se emplearán productos certificados conforme a lo establecido en ([op. pl.5]).

Debe decir el apartado 5.5.5

dimensiones	C		
nivel	bajo	medio	alto
medida	aplica	+	=

Errata 5: Desarrollo de aplicaciones [mp.sw.1]

(Donde dice categoría bajo, medio, alto debe decir categoría básica, media, alta)

página 104262

Dice el apartado 5.6.1

«5.6.1 Desarrollo de aplicaciones [mp.sw.1].

dimensiones	Todas		
categoría	bajo	medio	alto
	n.a.	aplica	=

Debe decir:

dimensiones	Todas		
categoría	básica	media	alta
	n.a.	aplica	=

Toda vez que la categorización de un sistema se clasifica en BÁSICA, MEDIA Y ALTA Y NO EN BAJO, MEDIO y ALTO que se reserva para definir niveles de las dimensiones de seguridad

Errata 6: Protección de servicios y aplicaciones web [mp.s.2]

(donde dice nivel debe decir categoría)

página 104264

Dice el apartado 5.8.2

«5.8.2 protección de servicios y aplicaciones web [mp.s.2].

dimensiones	Todas		
nivel	básica	media	alta
	aplica	=	+

Debe decir:

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	+

Toda vez que la clasificación de niveles de las dimensiones de seguridad son: BAJO, MEDIO y ALTO y no BÁSICA, MEDIA Y ALTA que se utiliza para la categorización de un sistema.

Fin de erratas.