VECTOR CYBERSECURITY.

Informe de Cumplimiento para ENS Servicio HUB-Efact para AOC (Consorcio Administración Abierta de Cataluña)

- Fecha de publicación: 03/12/2018
- Importancia: Alta
- Destinatarios: SERES
- Ámbito de aplicación: General
- Contacto: VectorSOC / 91.183.03.00
- Email: info@vectorcybersecurity.com

Índice

1.Introducción.

El **Esquema Nacional de Seguridad**, en adelante **ENS** o **Esquema**, en su Anexo II, establece para cada nivel (BASICO,MEDIO,ALTO) una serie de medidas en los siguientes ámbitos:

a) Marco organizativo

b) Marco operacional

c) Medidas de protección

El presente documento tiene por **finalidad confirmar el cumplimiento en el Nivel Básico del ENS tras la implementación de medidas correctivas aplicadas** en el **Servicio HUB-Efact** de la **Administración Abierta de Cataluña** (**AOC**) prestado por la **Sociedad de Explotación de Redes Electrónicas y Servicios S.A.** en adelante **SERES**,

1.1 Servicio que se evalúa, HUB-Efact de AOC.

El HUB-Efact de AOC es el nexo de unión entre las numerosas plataformas de facturación existentes en el mercado, y las diferentes administraciones catalanas.

En el Anexo II del ENS, se realiza una revisión acerca del estado en el que se encuentra SERES respecto a los Artículos 29,35,36,43 y 44 del RD 3/2010, se muestra en la siguiente tabla:

RD 3/2010	REQUISITO	OBSERVACIONES REQUISITOS
Art. 29	**Instrucciones Técnicas de Seguridad y Guías de Seguridad**	• Hay conocimiento de la relación de instrucciones Técnicas de Seguridad y guías de Seguridad publicadas en www.ccn-cert.cni.es. • Se dispone de documento de instrucciones Técnicas de Seguridad **PRI1303 - Procedimiento para la gestión de incidentes de seguridad**
Art.35	**Informe del Estado de la Seguridad**	• Se conoce la existencia de la herramienta INES • No se dispone de acceso a la herramienta INES. Para ello es necesario ser empresa colaboradora y poseer la correspondiente Habilitación de Seguridad • Se dispone de Políticas de Seguridad **POL0103-Política de Seguridad , POL0202 Política de seguridad Física, POL1202 Política de Seguridad de Información en las Relaciones con Proveedores , POL1701 , Política de seguridad de la Información,**
Art. 36	**Capacidad de Respuesta a Incidentes de Seguridad de la Información**	• Se conoce la existencia de la herramienta LUCIA • No aplica uso de LUCIA en nivel BÁSICO.
Art. 43 y 44	**Categorías y Facultades**	• Existe un proceso definido como **POL1501C - Política de Seguridad para los servicios a las AA.PP**

		• Existe un proceso definido de control de cambios **PRI1202 Cambios de Componentes de Red , MAR0207 Procedimiento de control de documentos.**

2. Tabla de cumplimiento de controles del ENS.

Se incluye a continuación una tabla resumen de las medidas de seguridad, los criterios de aplicación y el nivel de cumplimiento previo vs actual en el **Servicio HUB-Efact** de la **Administración Abierta de Cataluña** (**AOC)** prestado por SERES.

- Situación previa vs actual de cumplimiento utilizando el siguiente código de colores y de iniciales para cada una de las medidas de seguridad, así como documentación relacionada :
  - **Verde** y "**C**" de Cumplimiento, si cumple con todo lo especificado por el ENS.
  - **Naranja** y "**R**" de Recomendaciones, si cumple parcialmente.
  - **Rojo** e "**I**" de Incumplimiento, si la medida de control es inexistente o no está implementada.
  - En blanco, cuando la medida no aplica para el servicio HUB-Efact.

DIMENSION	NIVEL BAJO	Medidas de Seguridad		Cumplimiento 08/01/2018	Cumplimiento 03/12/2018
		org	**Marco Organizativo**		
C,A,T	aplica	org.1	Política de seguridad	I	C POL1504-Politica de Seguridad ara los servicios a alas AAPP
C,A,T	aplica	org.2	Normativa de seguridad	R	C PRI2602 Proceso de Autorizacion ENS PRI2902-Procedimientos Operacionales ENS PRI2910B Procedimiento para la Gestion de Usuarios PRI2501 Procedimiento de copias de Seguridad POL1102 Politica de Uso Aceptable
C,A,T	aplica	org.3	Procedimientos de seguridad	I	C PRI2501-Procedimiento de Copia de Seguridad.pdf PRI2602 Proceso de Autorizacion.pdf PRI2801-Procedimiento para Gestión de Usuarios ENS.pdf PRI2901-Procedimientos Operacionales ENS.pdf
C,A,T	aplica	org.4	Proceso de autorización	I	C PRI2602-Proceso de Autorizacion ENS
		Op	**Marco Operacional**		
		op.pl	Planificación		
C,A,T	aplica	op.pl.1	Análisis de Riesgos	I	C ENS - Análisis de Riesgos 2018-01.
C,A,T	aplica	op.pl.2	Arquitectura de seguridad	I	C Arquitectura de Seguridad ENS v2018-01

C,A,T	aplica	op.pl.3	Adquisición de nuevos componentes	I	C PRI2902-Procedimientos Operacionales ENS
		op.acc	Control de acceso		
A T	aplica	op.acc.1	Identificación	R	C PRI2902-Procedimientos Operacionales ENS
I C A T	aplica	op.acc.2	Requisitos de acceso	I	C PRI2902-Procedimientos Operacionales ENS
I C A T	aplica	op.acc.4	Proceso de gestión de derechos de acceso	I	C PRI2902-Procedimientos Operacionales ENS
I C A T	aplica	op.acc.5	Mecanismo de autenticación	I	C PRI2902-Procedimientos Operacionales ENS
I C A T	aplica	op.acc.6	Acceso local (local login)	R	C PRI2902-Procedimientos Operacionales ENS
I C A T	aplica	op.acc.7	Acceso remoto (remote login)	R	C PRI2902-Procedimientos Operacionales ENS
		op.exp	Explotación		
C,A,T	aplica	op.exp.1	Inventario de activos	R	C PRI2902-Procedimientos Operacionales ENS
C,A,T	aplica	op.exp.2	Configuración de seguridad	R	C PRI2902-Procedimientos Operacionales ENS
C,A,T	aplica	op.exp.4	Mantenimiento	I	C PRI2902-Procedimientos Operacionales ENS
C,A,T	aplica	op.exp.6	Protección frente a código dañino	I	C PRI2902-Procedimientos Operacionales ENS
T	aplica	op.exp.8	Registro de la actividad de los usuarios	R	C PRI2902-Procedimientos Operacionales ENS
C,A,T	aplica	op.exp.11	Protección de claves criptográficas	C	C PRI2902-Procedimientos Operacionales ENS
C,A,T	aplica	op.mon.2	Sistema de métricas	I	C PRI2902-Procedimientos Operacionales ENS
		mp	**Medidas de Protección**		
		mp.if	Protección de las instalaciones e infraestructuras		
C,A,T	aplica	mp.if.1	Áreas separadas y con control de acceso	C	C POL0202 Politica de Seguridad Fisica
C,A,T	aplica	mp.if.2	Identificación de las personas	R	C POL0202 Politica de Seguridad Fisica PRI0605 Procedimiento Control de Acceso(Madrid)
C,A,T	aplica	mp.if.3	Acondicionamiento de los locales	C	C
D	aplica	mp.if.4	Energía eléctrica	C	C
D	aplica	mp.if.5	Protección frente a incendios	C	C
C,A,T	No aplica para HUB-Efact	mp.if.7	Registro de entrada y salida de equipamiento		
		mp.per	Gestión del personal		
C,A,T	aplica	mp.per.2	Deberes y obligaciones	R	C POL1102 Politica de uso aceptable
C,A,T	aplica	mp.per.3	Concienciación	R	C

					SERES Concienciacion 2018
C,A,T	aplica	mp.per.4	Formación	I	C Lo gestiona RRHH Solicitud de necesidades de formación 2018.msg
		mp.eq	Protección de los equipos		
C,A,T	aplica	mp.eq.1	Lugar de trabajo ordenado	R	C POL1102 Politica de uso aceptable
C,A,T	aplica	mp.eq.3	Protección de equipos portátiles	R	C POL1102 Politica de uso aceptable
		mp.com	Protección de las comunicaciones		
C,A,T	aplica	mp.com.1	Perímetro seguro	C	C
I A	aplica	mp.com.3	Protección de la autenticidad y de la integridad	R	C POL1501C Politica de Seguridad para los Servicios a las AAPP
		mp.si	Protección de los soportes de información		
C	No aplica para HUB-Efact	mp.si.1	Etiquetado		
C,A,T	No aplica para HUB-Efact	mp.si.3	Custodia		
C,A,T	No aplica para HUB-Efact	mp.si.4	Transporte		
C	aplica	mp.si.5	Borrado y destrucción	C	C PRI2401 Procedimiento para la eliminación y destrucción de equipos y soportes
C,A,T	aplica	mp.sw.2	Aceptación y puesta en servicio	R	C PRI2602 Proceso de Autorización ENS
		mp.info	Protección de la información		
C,A,T	No aplica para HUB-Efact	mp.info.1	Datos de carácter personal		
C	aplica	mp.info.2	Calificación de la información	R	C POL1701 Politica de Clasificación de la Información
I A	aplica	mp.info.4	Firma electrónica	R	C AOC-Cuestionario ENS apartado mp.s2
C	aplica	mp.info.6	Limpieza de documentos	I	C Para Este servicio no se incorporan metadatos
D	aplica	mp-info.9	Copias de seguridad (backup)	R	C PRI2501 Procedimiento de Copias Seguridad
		mp.s	Protección de los servicios		
C,A,T	aplica	mp.s.1	Protección del correo electrónico	C	C PRI2201 Hardering de Servidores SERES
C,A,T	aplica	mp.s.2	Protección de servicios y aplicaciones web	R	C PRI2201 Hardering de Servidores SERES AOC-Cuestionario ENS apartado mp.s2

3. Índice de Cumplimiento HUB-Efact vs ENS.

Tras la reevaluación de los controles de seguridad del ENS tanto en marco organizativo , como operacional, como de implementación de medidas de protección , podemos concluir que el servicio **Servicio HUB-Efact** de la **Administración Abierta de Cataluña (AOC) cumple que los requisitos del nivel BÁSICO del ENS.**

4. Documentación revisada.

Para la evaluación se revisó la siguiente documentación:

Documentación de **POLITICAS** SERES:

- AAPS0401 .-Gestión de usuarios para Seguridad y accesos.
- MAR0113 Listado Maestro de Documentación.
- MAR0207 Procedimiento de control de documentos.
- POL0103 Política de Seguridad
- POL0202 Política de Seguridad Física
- POL1102 Política de Uso Aceptable
- POL1701 Política de Clasificación de la Información
- POL1201.- Política de Seguridad de la Información en las Relaciones con Proveedores.
- POL1501C.- Política de Seguridad para los Servicios a las A.A.P.P.
- PRI0605 Procedimiento Control de Acceso (Madrid)
- PRI2201 Hardering de servidores SERES
- PRI2401 Procedimiento para la eliminación y destrucción de equipos y soportes
- POL1201 Política de Seguridad de la Información en las Relaciones con los Proveedores
- POL1501C Política de Seguridad para los servicios a las AA.PP
- PRI1202 Procedimiento de Control de Cambios en Componentes de Red
- PRI1303 Procedimiento para la gestión de incidentes de seguridad
- PRI2501 - Procedimiento de Copias de Seguridad
- PRI2602.- Proceso de Autorización ENS
- PRI2801.- Procedimiento de Gestión de Usuarios
- PRI2902 .- Procedimientos Operacionales.
- PRI1302.- Procedimiento de entrada y salida de equipamiento.
- SERES.- Concienciación sobre seguridad

Madrid 3 de Diciembre del 2018.