Informe de Auditoría del Esquema Nacional de Seguridad del Servicio HESTIA

Consorci Administració Oberta de Catalunya (AOC)

8 de mayo de 2018

Documento de uso interno

Consorci AOC

Informe de Auditoría del ENS del Servicio Hèstia

(Basado en el Real Decreto 3/2010, de 8 de enero)

Mayo 2018

CONTENIDO

Rafael Calvo, 18
28010 Madrid · España

t: +34 914 364 190
f: +34 914 364 191/92

www.bdo.es

Servicio Hèstia, Consorcio AOC

Informe de Auditoría del ENS del Servicio Hèstia

(Basado en el Real Decreto 3/2010, de 8 de enero)

1. INFORME DE AUDITORÍA

1.1. INTRODUCCIÓN

De acuerdo con los términos de nuestra propuesta de servicios profesionales de fecha septiembre de 2017 solicitada por Consorci AOC, les presentamos nuestro informe de la auditoría del Esquema Nacional de Seguridad a nivel Alto de los Sistemas de Información que dan cobertura a servicio Hestia de Consorci, en cumplimiento del artículo 34 y de acuerdo con lo previsto en el anexo III del Real Decreto 3/2010, de 8 de enero.

Este informe de auditoría ha sido preparado para uso exclusivo del Consorci AOC, con CIF: Q0801175A y situada en Carrer de Tànger, 98, bajo, 08018 Barcelona (en adelante AOC o la Organización), por lo que no deberá ser utilizado para fines distintos al descrito a continuación ni ser distribuido a terceros, salvo requerimiento de la autoridad competente.

1.2. OBJETIVO

Para dar cumplimiento a la normativa vigente, y de conformidad con el artículo 34 y con el Anexo III del RD 3/2010, y su modificación mediante el Real Decreto 951/2015, de 23 de octubre, hemos procedido, a solicitud del Consorci AOC, a revisar el cumplimiento de los requisitos a nivel Alto establecidos en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en los capítulos II y III y en los Anexos I y II.

Nuestra responsabilidad es la emisión de un informe que exprese un dictamen sobre la adecuación de AOC a las medidas y controles definidos a nivel Alto en el Esquema Nacional de Seguridad, identificar sus deficiencias. Adicionalmente, nuestro informe a nivel Alto incluye los datos, hechos y observaciones en que se basan los dictámenes alcanzados.

1.3. ALCANCE

El alcance de la revisión ha contemplado los elementos necesarios para el desarrollo del servicio Hestia del Consorci AOC.

A continuación, se detalla la descripción de dicho servicio:

- El servicio Hestia permite gestionar buena parte de las actividades que se llevan a cabo desde una Área de Servicios Sociales básicos. Está formado por una serie de módulos que dan respuesta al primer nivel del sistema público. Los módulos de los que consta actualmente el Hestia son:
    - Atención Primaria.
    - Servicios de Información y Atención a la Mujer (SIAD).
    - Servicios de gestión de los Planes de Ciudadanía e Inmigración.
    - Servicios Gestores del Ayudas de Vivienda.
    - Servicio de Atención Domiciliaria (SAD).
    - Servicio de Atención a la Infancia y la Adolescencia (EAIA).
    - Gestión de la agenda de los profesionales.
    - Buscador.
    - Gestión de trámites.
    - Extracción de datos para informes y memorias.

En el momento de la realización de esta revisión el servicio se presta desde el DataCenter de MediaCloud ubicado en Barcelona.

A continuación, se enumera el detalle de los requisitos que no forman parte del alcance de la revisión del servicio:

- Medidas de protección\Protección de la Información:
    - mp.info.2 - Calificación de la información.
    - mp.info.4 – Firma Electrónica.
    - mp.info.5 – Sellos de tiempo.

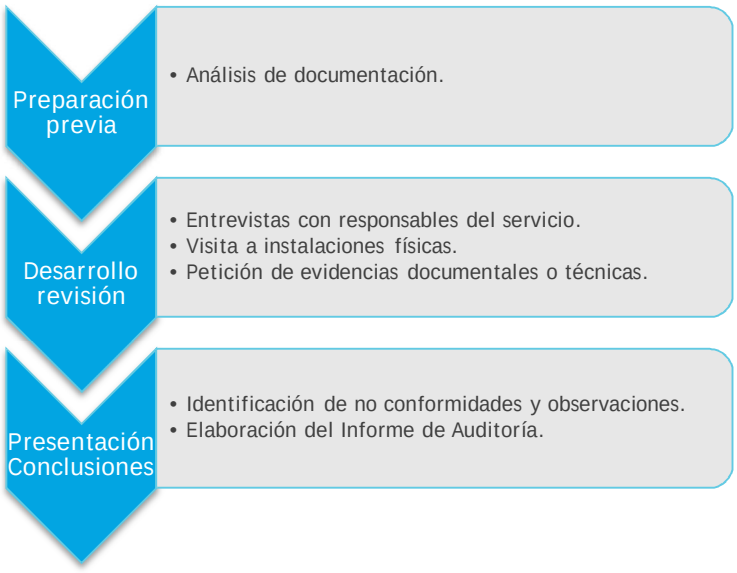
1.4. EQUIPO AUDITOR

A continuación, se indican los componentes del equipo responsable de la auditoría, así como su función:

EQUIPO AUDITOR	
Valentín Faura	Auditor Jefe
Roger Pérez	Auditor
Juan Gordo	Auditor

1.5. METODOLOGÍA

La metodología empleada para la realización del presente trabajo, ha consistido en:



- Preparación previa: el trabajo de revisión se ha iniciado con un análisis de la documentación facilitada por la Organización, a partir de la que se ha planificado la revisión conjuntamente con los responsables del proyecto de la Organización.

- Desarrollo de la revisión: se han validado los procedimientos descritos y se han realizado las pruebas y comprobaciones necesarias para asegurar que se adecuan a la normativa vigente.

- Entrevistas: las personas de BDO que han participado en la revisión se han entrevistado con diferentes responsables de la Organización con la finalidad de revisar el cumplimiento del ENS.

- Visita a las instalaciones: se ha realizado una revisión in-situ de los siguientes tipos de dependencias:

    - Sede central: se ha visitado la sede central ubicada en Carrer de Tànger, 98, bajo, 08018 Barcelona, donde se han realizado entrevistas con los responsables del servicio y unidades organizativas.

    - Centros de Procesamiento de Datos (CPD): se ha revisado la sede del Centro de Procesamiento de Datos (aquella que alberga sistemas de la Organización) ubicado en el MediaCloud con dirección Diagonal, 177, 08018 Barcelona, realizando verificaciones de cumplimiento sobre las medidas de seguridad del Esquema Nacional de Seguridad.

- Presentación conclusiones: en la última fase de la metodología, se ha procedido a la validación de la información y se han presentado a la Organización las conclusiones y observaciones derivadas del trabajo realizado.

1.6. CONCLUSIONES

Las principales conclusiones obtenidas de nuestro trabajo de revisión de las medidas y controles de seguridad conforme al nivel Alto de los Sistemas de Información que dan cobertura al servicio Hèstia del Consorci AOC son las que se indican a continuación:

a) AOC dispone de la preceptiva Política de Seguridad. Todo ello permitiendo un proceso de la gestión de la seguridad conforme a lo establecido en los principios básicos y requisitos mínimos del Esquema Nacional de Seguridad.

b) Se definen los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de información respectando el principio de "separación de funciones".

No obstante, a lo anterior, en la comprobación de la adecuación de las medidas y controles de seguridad conforme al nivel Alto del Real Decreto 3/2010, del 8 de enero, de aquellos aspectos de aplicación para el servicio revisado, se han identificado algunos puntos de mejora, y en consecuencia, la necesidad de introducir algunas medidas adicionales en el proceso de seguridad actual.

c) Estas medidas de mejora son conocidas por la Organización, que ya está trabajando para su implementación. Se concretan en los siguientes aspectos:

Declaración de Aplicabilidad

Respecto a la Declaración de Aplicabilidad, se ha observado que:

B1) [No Conformidad Menor]: No se ha realizado una adecuada valoración de la aplicabilidad de los requisitos del ENS en relación con el servicio.

Marco Organizativo

Respecto a la Normativa y Procedimientos de seguridad (org.2 y org.3), se ha observado que:

B1) [No Conformidad Menor]: La Organización está trabajando aún en su Marco Normativo de Seguridad. Algunos procedimientos como el de copias de seguridad y recuperación o de altas de usuarios están en proceso de aprobación.

Respecto al Proceso de autorización (org.4), se ha observado que:

B1) [No Conformidad Menor]: No se dispone de un proceso formal de autorizaciones en el entorno productivo que cubra todos los elementos del sistema de información (entradas equipos, elementos de red o aplicaciones en el entorno productivo, nuevos proveedores de servicios con acceso a producción)

Marco Operacional

Planificación

Respecto al Análisis de riesgos (op.pl.1), se ha observado que:

B1), M1), A1) [No Conformidad Mayor]: No se realiza una identificación y gestión de riesgos incluyendo la identificación de escenarios de riesgo, el análisis de las consecuencias y su probabilidad, y la evaluación de su aceptabilidad o inaceptabilidad para la Organización, con revisión y aprobación regular, según lo establecido en las medidas aplicables del Anexo II del RD 3/2010.

Respecto a la Arquitectura de seguridad (op.pl.2) se ha observado que:

M1), A1) [No Conformidad Mayor]: No se dispone de un sistema de gestión de seguridad de la información documentado y aprobado por Dirección, cual sistema ofrece un proceso de mejora continua de la gestión de la seguridad conforme a lo establecido en los principios básicos y requisitos mínimos del Esquema Nacional de Seguridad.

Control de acceso

Respecto a la Identificación (op.acc.1), se ha observado que:

B1) [No Conformidad Menor]: Se ha identificado el uso de cuentas genéricas no asociadas a un usuario individual como por ejemplo el usuario Admin dado de alta en las 81 áreas que utiliza el servicio Hestia. Este usuario genérico con máximo privilegios es utilizado por los administradores de AOC. En una revisión de una muestra de áreas, se han identificado otros usuarios genéricos como Tests8 – administrador, Testsis7, Testsistemas5 o Ts49. Se ha identificado también el uso de usuarios genéricos en los servidores y para los accesos remotos de proveedores.

Respecto a Mecanismos de autenticación (op.acc.5), se ha observado que:

B1) [No Conformidad Menor]: No se puede asegurar que las credenciales del acceso al servicio están bajo el control exclusivo del usuario. A cada nuevo usuario, se le asigna la misma contraseña por defecto. A su vez, es responsabilidad del cliente del servicio Hestia aplicar la funcionalidad de cambio automático de contraseña a la primera conexión. La responsabilidad recae en el cliente.

M1, A1) [Observación]: El servicio Hestia ofrece la posibilidad de autenticarse al servicio por usuario y contraseña o por certificado electrónico y contraseña. El uso de usuario/contraseña no cumple con los requerimientos de mecanismos de autenticación de nivel medio y alto. Es responsabilidad del cliente autenticarse con certificado electrónico y contraseña para cumplir con el requerimiento.

B1) [No Conformidad Menor]: Para los accesos remotos por parte de empleados y proveedores a los servidores del servicio Hestia no se utiliza doble factor de autenticación.

Respecto al Acceso local (op.acc.6), se ha observado que:

B1), M1), A1) [No Conformidad Menor]: No se informa al usuario cuando se conecta al servicio Hestia de sus obligaciones inmediatamente después de obtener el acceso. Tampoco se ha identificado alguna restricción de acceso al servicio por horario, fechas y lugar desde donde se accede.

Respecto al Acceso remoto (op.acc.7), se ha observado que:

M1) [No Conformidad Menor]: No se ha establecido una política específica de lo que puede hacerse remotamente. No se requiere utilizar un dispositivo de AOC para conectarse remotamente a la red interna. Los usuarios acceden a un escritorio remoto por lo que tendrá el mismo acceso que en local. No hay restricciones de accesos específicos ni tampoco se requiere autorizaciones especiales. Cualquier usuario de AOC tiene acceso remoto a la red interna.

Explotación

Respecto a la Configuración de seguridad (op.exp.2), se ha observado que:

B1) [No Conformidad Menor]: Se han identificado aspectos de mejora en la configuración de servidores (servicios innecesarios con vulnerabilidades reconocidas y usuarios locales genéricos).

Respecto a la Protección frente a código dañino (op.exp.5), se ha observado que:

B1) [No Conformidad Menor]: No se dispone de soluciones de protección antivirus instalada en los 3 servidores que compone el servicio.

Respecto al Registro de la actividad de los usuarios (op.exp.10), se ha observado que:

A1) [No Conformidad Menor]: No se han identificado controles de seguridad específicos para asegurar la integridad de los registros de auditoria. Hemos sido informados que, para otros servicios, AOC está implementando una solución desarrollada internamente para asegurar la integridad de los registros de auditoria.

Servicios Externos

Respecto a Contratación y acuerdos de nivel de servicio (op.ext.1), se ha observado que:

M1) [Observación]: No se incluye en los pliegos de condiciones de productos y servicios externalizados relacionados con el servicio Hestia la obligatoriedad por parte del proveedor de presentar a petición de AOC un certificado de cumplimiento de los requerimientos del ENS por una entidad independiente.

Continuidad del servicio

Respecto a Análisis de impacto (op.cont.1), se ha observado que:

M1) [No Conformidad Menor]: No se ha realizado un análisis de impacto cuyo objetivo es conocer las consecuencias de una interrupción en la realización de las actividades del servicio Hestia. Un análisis de impacto permite identificar las necesidades y requerimientos existentes, y consecuentemente, diseñar una adecuada estrategia de recuperación.

Respecto a Plan de Continuidad (op.cont.2), se ha observado que:

A1) [No Conformidad Mayor]: Se dispone de una única sala de servidores dónde se ubican los servidores que componen el servicio Hestia. En caso de incidente mayor que afecte al CPD, el servicio Hestia quedaría afectado. Tampoco se incluyen los datos de los servidores que soportan el servicio Hestia en las copias de seguridad que externaliza AOC. Las copias del servicio Hestia se hacen en disco y en cintas pero que se ubican en el mismo DataCenter de MediaCloud.

A2) [No Conformidad Mayor]: No se dispone de un Plan de Continuidad de Negocio ni un Plan de Recuperación ante desastre del servicio Hestia. Tomamos en consideración que AOC está trabajando para otros servicios en el desarrollo de estos planes y podría aplicarlo para el servicio Hestia.

Respecto a Pruebas periódicas (op.cont.3), se ha observado que:

A1) [Observación] Existe una falta de documentación y registro de las pruebas de contingencias tecnológicas.

Monitorización del sistema

Respecto a la Detección de intrusión(op.mon.2), se ha observado que:

M1) [Observación]: Pese a disponer y tener implementado un sistema de detección de intrusión, no se ha establecido un procedimiento de revisión y monitorización del sistema de detección. No se dispone de alertas preventivas, sino que es tarea del equipo asignado verificar y comprobar los registros y alertas del IDS.

Respecto al Sistema de métricas (op.mon.2), se ha observado que:

A1) [No Conformidad Menor]: AOC no dispone de las métricas requeridas por el Centro Criptográfico Nacional de la herramienta INES para monitorizar el cumplimiento del ENS de la Organización o de los servicios que ofrece a entidades públicas y en el alcance del Esquema Nacional de Seguridad. Los indicadores definidos y medidos por el departamento de Seguridad de AOC no cubren todos los dominios de seguridad del Esquema Nacional de Seguridad.

Medidas de Protección

Gestión del personal

Respecto a Concienciación (mp.per.3), se ha observado que:

B1) [No Conformidad Menor]: Se ha identificado una falta de iniciativas de concienciación en materia de Seguridad de la Información y Confidencialidad para los empleados.

Respecto a Formación (mp.per.4), se ha observado que:

B1) [Observación]: Falta de Formación específica en Seguridad de la Información y sobre el Esquema Nacional de Seguridad para el personal con responsabilidad sobre los sistemas de información que soportan el servicio Hestia.

Protección de las comunicaciones

Respecto al Perímetro seguro (mp.com.1), se ha observado que:

B1) [No conformidad Menor]: Se utilizan firewalls lógicos no redundados ni certificados para la separación de la red interna y externa.

Respecto a la Protección de la confidencialidad (mp.com.2), se ha observado que:

Protección de las aplicaciones informáticas

Respecto a Desarrollo de aplicaciones (mp.sw.1) y aceptación y puesta en servicio (mp.sw.2), se ha observado que:

M1) [No Conformidad Menor]: No se toman en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida de desarrollo (toma de requerimientos, desarrollo seguro, pruebas de seguridad).

M2) [No Conformidad Mayor]: Durante la auditoria, debido a una incidencia prolongada, no se disponía de entornos diferenciados para producción y test con los evidentes riesgos de seguridad asociados.

Protección de la información

Respecto al Cifrado de la información (mp.info.3), se ha observado que:

A1) [No Conformidad Menor]: La información con un nivel alto en confidencialidad del servicio Hestia no se almacena cifrada en Base de Datos.

Protección de los servicios

Respecto a la Protección de servicios y aplicaciones web (mp.s.2) y Protección frente a la denegación de servicio (mp.s.8), se ha observado que:

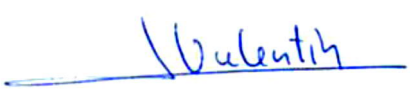
M1), A1) [No Conformidad Menor]: No se incluye previo a la entrada en servicio de nuevos cambios en el servicio Hestia de los siguientes controles:

- Análisis de vulnerabilidades. Los análisis que se ejecutan no incluyen en su alcance los 3 servidores del Servicio Hestia.
- Pruebas de penetración.
- Auditorias del código fuente.

d) Excepto por todo lo indicado en el punto c) anterior, las medidas y controles de seguridad a nivel Alto de los Sistemas de Información que dan cobertura al servicio Héstia del Consorci AOC, sus Sistemas de Información e instalaciones de tratamiento de datos cumplen con lo dispuesto en el Real Decreto 3/2010, del 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica para el servicio.

e) El dictamen final del informe de auditoría es: Desfavorable

BDO Auditores, S.L.P.



Valentín Faura
Auditor Jefe

Barcelona, 08 de Mayo de 2018

CUADRO RESUMEN MEDIDAS DE SEGURIDAD

Informe de Auditoría del ENS del Servicio Hèstia

Consorcio AOC

2. CUADRO RESUMEN MEDIDAS DE SEGURIDAD

La tabla a continuación proporciona un resumen de los Sistemas de Información que dan cobertura al Servicio Hésteria del Consorci AOC en cumplimiento del alcance al nivel "Alto" del "Esquema Nacional de Seguridad".

MARCO ORGANIZATIVO

Categoría	Tipo	Dimensión		
		Básico	Medio	Alto
(org)	1 - Política de Seguridad	✓		
	2 - Normativa de seguridad	×		
	3 - Procedimientos de seguridad	×		
	4 - Proceso de autorización	×		

Leyenda	✓ Cumple	× NC Mayor	× NC Menor	- No Aplica

MARCO OPERACIONAL

Categoría	Tipo	Dimensión		
		Básico	Medio	Alto
Planificación (op.pl)	1 - Análisis de Riesgos	×	×	×
	2 - Arquitectura de Seguridad	✓	×	×
	3 - Adquisición de nuevos componentes	✓		
	4 - Dimensionamiento / gestión de capacidades		✓	
	5 - Componentes certificados			✓
Control de acceso (op.acc)	1 - Identificación	×		
	2 - Requisitos de acceso	✓		
	3 - Segregación de funciones y tareas		✓	
	4 - Proceso de gestión de derechos de acceso	✓		
	5 - Mecanismo de autenticación	×	✓	✓
	6 - Acceso local	✓	✓	✓
	7 - Acceso remoto	✓	×	
Explotación (op.exp)	1 - Inventario de activos	✓		
	2 – Configuración de seguridad	×		
	3 - Gestión de la configuración		✓	
	4 - Mantenimiento	✓		
	5 - Gestión de cambios		✓	
	6 - Protección frente a código dañino	×		
	7 - Gestión de incidentes	✓	✓	
	8 - Registro de la actividad de los usuarios	✓	✓	✓
	9 - Registro de la gestión de incidentes	✓	✓	
	10 - Protección de los registros de actividad			×
	11 - Protección de claves criptográficas	×	×	×

Categoría	Tipo	Dimensión		
		Básico	Medio	Alto
Servicios externos (op.ext)	1 - Contratación y acuerdos de nivel de servicio		✓	
	2 - Gestión diaria		✓	
	9 - Medios alternativos			✓
Continuidad del servicio (op.cont)	1 - Análisis del impacto		×	
	2 - Plan de continuidad			×
	3 - Pruebas periódicas			✓
Monitorización del sistema (op.mon)	1 - Detección de intrusión		✓	
	2 - Sistema de métricas	✓	✓	×

MEDIDAS DE PROTECCIÓN

Categoría	Tipo	Dimensión		
		Básico	Medio	Alto
Protección de las instalaciones e infraestructuras (mp.if)	1 - Áreas separadas y con control de acceso	✓	✓	✓
	2 - Identificación de las personas	✓		
	3 - Acondicionamiento de los locales	✓		
	4 - Energía eléctrica	✓	✓	
	5 - Protección frente a incendios	✓		
	6 - Protección frente a inundaciones		✓	
	7 - Registro de entrada y salida de equipamiento	✓		
	9 - Instalaciones alternativas	✓		
Gestión del personal (mp.per)	1 - Caracterización del puesto de trabajo		✓	
	2 - Deberes y obligaciones	✓		
	3 - Concienciación	×		
	4 - Formación	✓		
	9 - Personal alternativo			✓
Protección de los equipos (mp.eq)	1 - Puesto de trabajo despejado	✓	✓	
	2 - Bloqueo de puesto de trabajo	✓		
	3 - Protección de equipos portátiles	✓		
	9 - Medios alternativos		✓	
Protección de las comunicaciones (mp.com)	1 - Perímetro seguro	✓	✓	
	2 - Protección de la confidencialidad		✓	✓
	3 - Protección de la autenticidad y de la integridad	✓	✓	✓
	4 - Segregación de redes		✓	
	9 - Medios alternativos		✓	

Leyenda	✓ Cumple	✓ Compartido	× NC Mayor	× NC Menor	- No Aplica

Categoría	Tipo	Dimensión		
		Básico	Medio	Alto
Protección de los soportes de información (mp.si)	1 - Etiquetado	✓		
	2 - Criptografía		✓	
	3 - Custodia	✓		
	4 - Transporte			
	5 – Borrado y destrucción	✓	✓	
Protección de las aplicaciones inf. (mp.sw)	1 - Desarrollo de aplicaciones		×	
	2 - Aceptación y puesta en servicio	✓	×	
Protección de la información (mp.info)	1 - Datos de carácter personal	✓	✓	
	2 - Calificación de la información	✓	✓	
	3 - Cifrado			×
	4 - Firma electrónica			
	5 - Sellos de tiempo			
	6 - Limpieza de documentos	✓		
	9 - Copias de seguridad	✓	✓	
Protección de los servicios (mp.s)	1 - Protección del correo electrónico	✓		
	2 - Protección de servicios y aplicaciones web	✓	×	✓
	8 - Protección frente a la denegación de servicio		×	
	9 - Medios alternativos		✓	

Leyenda	✓ Cumple	✓ Compartido	× NC Mayor	× NC Menor	- No Aplica

DETALLE DE LAS PRUEBAS REALIZADAS
Informe de Auditoría del ENS del Servicio Hèstia

Consorci AOC

3. DETALLE DE LAS PRUEBAS REALIZADAS

3.1. DEFINICIÓN DE LA PLANTILLA

En las siguientes páginas se detalla cada una de las pruebas efectuadas a lo largo del análisis de grado de cumplimiento del ENS, de acuerdo con la siguiente estructura:

Marco	Marco afectado
Medidas	Controles

Descripción
Descripción de la prueba diseñada.

Trabajo realizado y Observaciones
Documentación revisada, evidencias obtenidas y hechos detectados.

(1): Para la valoración de los diferentes dominios se ha utilizado la escala de valores mostrada anteriormente en el apartado 1.4.

3.2. GRADO DE CUMPLIMIENTO DE CONTROLES ENS

A continuación, se presenta el detalle del trabajo de campo realizado para verificar y revisar el cumplimiento de los controles del Esquema Nacional de Seguridad en el Consorcio AOC, así como las observaciones realizadas y las recomendaciones encaminadas a subsanar dichas observaciones, en el caso de que las hubiese.

Marco	Marco organizativo
Medidas	Org.1 Política de seguridad Org.2 Normativa de seguridad Org.3 Procedimientos de seguridad Org.4 Proceso de autorización

Descripción
Se debe disponer de una Política de Seguridad documentada y coherente con lo establecido en el Documento de Seguridad, exigible por el Real Decreto 1720/2007. Dicha política ha sido aprobada por el órgano superior de la Organización, además de ser accesible por todos los miembros de la misma. La Normativa de Seguridad se debe encontrar a disposición de todos los miembros de la Organización siendo de obligado cumplimiento. Establecerá las obligaciones y responsabilidades de los miembros de la Entidad respecto a aspectos de Seguridad de la Información. La Organización debe contar con un proceso para la autorización a los sistemas de información. En él se incluyen las instalaciones, las configuraciones sobre equipos y aplicaciones en preproducción, las comunicaciones con otros sistemas, así como los medios de comunicación, los soportes de información y los dispositivos móviles que pudieran ser utilizados. Además, dicho procedimiento se difunde dentro de la Organización.

Trabajo realizado
En relación a la Política de Seguridad, se ha revisado la información proporcionada y se ha comprobado que: • Disponen de una Política de Seguridad escrita y aprobada por la Comisión Ejecutiva. Queda evidenciado con el documento "PDS_ Política de Seguretat v 1 1". Este documento incluye los siguientes aspectos relevantes concernientes al ENS: o Marco legal y regulatorio (Apartado 2.3) o Roles, funcionalidades, deberes, responsabilidades y procedimientos de asignación y baja de cargo de los responsables de seguridad (Apartado 3.1). o Estructura de la Comisión Ejecutiva del Consorcio AOC, Comité Ejecutivo de Seguridad de la Información, Responsable de Seguridad de la Información, Comité Operativo de Seguridad de la Información y Responsable de Sistemas (Apartado 3.1). o Directrices de Seguridad de la Información (Apartado 3.2). Se ha revisado la información proporcionada en relación con las Normativas y Procedimientos de Seguridad y se ha comprobado: • La Normativa de Seguridad del Consorcio AOC es un conjunto de documentos que establecen la forma de afrontar ciertos temas en materia de seguridad. La Normativa del Consorcio AOC se compone de la Política de Seguridad y las normas concretas que la desarrollen y aprueben. La Normativa se desarrolla mediante procedimientos específicos para cada caso. • La Normativa tiene carácter de obligado cumplimiento y su incumplimiento da lugar a medidas disciplinarias. • El Consorcio AOC dispone de diversas normativas y procedimientos que poseen control de versiones, lista de distribución histórica de cambios, así como los apartados descriptivos concernientes a la norma. A continuación, se exponen cuatro ejemplos de normas de seguridad con sus objetivos y un procedimiento:

- AOC_NOR_01_acces internet v1.0. El objetivo de esta Norma es regular el acceso a Internet por parte de los usuarios de los Sistemas de Información del Consorcio AOC, posibilitando la homogeneización de criterios dentro de la organización y definiendo unas reglas de uso que deberán ser conocidas y practicadas por todos los usuarios.
- AOC_NOR_02_Contrasenyes_V1.1. El objetivo de esta Norma es regular la creación y el uso de contraseñas robustas, cuando éste sea el mecanismo de autenticación utilizado para acceder a determinados sistemas o servicios del Consorcio AOC. objetivo
- AOC_NOR_03_Treball fora instal·lacions_V 1.1. El objetivo de esta Norma es regular el trabajo del personal del Consorcio AOC cuando desarrolle su actividad profesional fuera de los edificios, dependencias e instalaciones del Consorcio AOC.
- AOC_NOR_04_Control acces_V2.0. El objetivo de esta Norma es regular el control de acceso a los Sistemas de información, a las instalaciones e infraestructuras del Consorcio AOC.
- AOC_PROC_01_incidents seguretat: El objeto de este Procedimiento se indicó cómo proceder en la gestión de los incidentes de seguridad y de las debilidades detectadas en los elementos de los sistemas de información del Consorcio AOC.

- Estas Normativas y Procedimientos de Seguridad precisan cómo llevar a cabo las tareas habituales y quién debe hacer cada tarea
- Además, existe un documento que hace referencia a lo concerniente en tratamiento de datos de carácter personal donde se especifican normas y procedimientos de seguridad específicos para este tipo de datos. Este documento es "Document de Seguretat.2017 3.0"

No obstante, se han identificado las siguientes deficiencias:

- De la revisión de la Política de seguridad del Consorcio AOC, destacamos que no incluye de manera clara los objetivos de la Organización en cuanto a Seguridad de la Información.
- Respecto a la revisión de Normativas y Procedimientos de seguridad, se destaca que la Organización está trabajando aún en su Marco Normativo de Seguridad.
  - Los procedimientos de copias de Seguridad y recuperación o de altas de usuarios están en proceso de aprobación. Poner la típica frase que me faltan procedimientos tipo (accesos remotos, configuración segura,)
- No se posee evidencia de los procesos de autorización en relación a los cambios en producción. Pese que todos los cambios al entorno productivo requieren aprobación de Sistemas o de Dirección, no queda siempre evidencia de dichas autorizaciones previo a su pase a producción. Tampoco queda documentado ni procedimentado un proceso formal de autorizaciones que cubra todos los elementos del sistema de información (entradas equipos, elementos de red o aplicaciones en el entorno productivo, nuevos proveedores de servicios con acceso a producción)

Marco	Marco operacional (Planificación)
Medidas	Op.pl.1 Análisis de riesgos Op.pl.2 Arquitectura de seguridad Op.pl.3 Adquisición de nuevos componentes Op.pl.4 Dimensionamiento / Gestión de capacidades Op.pl.5 Componentes certificados

Descripción

Sobre la base de una metodología definida y generalmente aceptada, se dispondrá de un análisis de riesgos, identificando y valorando sus activos, amenazas, vulnerabilidades, salvaguardas y el riesgo residual que la Organización está dispuesta a asumir.

Se exige documentación sobre las instalaciones y sus áreas de seguridad, en la cuales se precise de puntos de acceso, de las redes de comunicaciones internas y sus medios de conexión al exterior.

Se debe disponer de un inventario que recoja los Sistemas de Información, así como los procedimientos que los gestionan, y los Sistemas de Seguridad. Además, requiere documentación precisa sobre la gestión y control de los Sistemas de Identificación.

Se exige un procedimiento formal para la adquisición de nuevos componentes del sistema, acorde con las conclusiones del análisis de riesgos, así como con la arquitectura de seguridad. En dicho procedimiento se debe tener en cuenta las necesidades de formación y financiación.

La normativa requiere que exista un plan que contemple las necesidades de dimensionamiento previa a la puesta en explotación. Se deben cubrir aspectos como las nuevas necesidades de procesamiento, almacenamiento, comunicaciones, personal, instalaciones y medios auxiliares.

Trabajo realizado

En relación al análisis de riesgos, no se ha realizado a nivel de Organización como a nivel de servicio Hestia ningún análisis de riesgos para identificar y cuantificar los riesgos de seguridad que puedan afectar el servicio. Hemos sido informados por AOC que se está trabajando en las siguientes actividades:

- Estudio de la metodología de análisis de riesgos del CESICAT para valorar su aplicación para los servicios de AOC y en particular del servicio Hestia.
- Desde el departamento de Seguridad de AOC se está realizando formación sobre la herramienta PILAR con el objetivo de utilizarla para la ejecución y seguimiento del análisis de riesgos.
- Se están identificado e inventariado los activos Hardware y Software que soportan el servicio Hestia, cuales activos formarán parte del análisis

En relación a la arquitectura de Seguridad, se ha verificado lo siguiente:

- Se dispone de documentación técnica sobre los sistemas que dan soporte al servicio Hestia y la infraestructura de red en la que se encuentra.
    - la evidencia “AOC - AOC-NetworkingBackbone” incluye un diagrama de red con nombres inequívocos e IPs los Servidores de Aplicación, las Bases de Datos y los discos duros de almacenamiento, así como la interconexión que existe entre los sistemas.
    - Los sistemas operativos de los entornos de Producción y Preproducción están identificados en la evidencia “Digrama xarxa II”. Estos sistemas son:
        - Para el entorno de preproducción:
            - VM00917 - AOC - Eacat PRE FP2IIS - Frontal - Windows server 2008 r2 standard
            - VM00922 - AOC - Eacat PRE FP2SQL - DB - Windows server 2008 r2 standard
        - Para el entorno de producción:

- AOC-W-HESTIA-PRO-FP1 - Frontal - Windows server 2008 r2 standard
- AOC-W-HESTIA-PRO-FP2 - Frontal - Windows server 2008 r2 standard
- HESTIA-PRO-SQL1 - DB - Windows server 20012 r2 standard
- HESTIA-PRO-SQL2 - DB - Windows server 20012 r2 standard
- eacatTR64-SQL01 - Antic DB migrat al cluster - Windows server 2008 r2 enterprise

  - Se han identificado en la evidencia "Digrama xarxa II", algunas de las salvaguardas del servicio Hestia, en concreto se ha identificado:
    - Firewall PaloAlto
    - Balanceador de carga AOC-ASA-FW

- Se posee evidencia de la documentación de la arquitectura de comunicaciones del Consorcio AOC. En concreto se describe lo concerniente a:
  - Áreas y puntos de acceso lógico
  - Equipos
  - Redes internas y las distintas conexiones al exterior.
- En el diagrama de red facilitado en la evidencia "AOC-NetworkingBackbone", se identifican las líneas de defensa donde queda especificado la interconexión entre las redes internas, otras redes corporativas (red Badalona, red Callus, red SARA y red Xcat), internet y las DMZ.
- Queda evidenciado el uso de cortafuegos en la documentación "AOC-NetworkingBackbone"

Sistemas y Seguridad suelen estar involucrados en todos los proyectos tecnológicos. Eso sí, cada sponsor de proyectos debe especificar claramente que el nuevo proyecto debe ser revisado por Seguridad en la hoja de información de justificación del proyecto. A nivel operativo, este hecho significa que intervienen en los pliegos de condiciones introduciendo los requerimientos de seguridad a aplicar. Dichos requerimientos incluyen:

- Inventario de Normas y procedimientos a cumplir por el servicio objeto de la contratación.
- Controles específicos de Seguridad a cumplir. Seguridad AOC tiene un inventario de unos 140 controles que afectan a varios dominios de seguridad (comunicaciones, control de acceso, desarrollo, explotación) que se van incluyendo al pliego según las necesidades del servicio y la revisión realizada por Seguridad. Se ha obtenido varios pliegos en el que se ha podido validar este control.

La adquisición de nuevos componentes sigue los procesos actuales de contratación del AOC. Cualquier compra de componentes que se instala en el entorno productivo de Hestia involucra a Sistemas y Seguridad AOC. El esquema nacional de seguridad obliga a que los componentes estén certificados. Se ha identificado que los componentes que intervienen en el servicio Hestia cumplen con estas características.

En vistas de asegurar la capacidad de los sistemas, se ha observado que sistemas utiliza Nagios OP5 Monitor como sistema de monitorización de redes y servidores. Se utiliza este dispositivo para la realización de estimaciones futuras de capacidad, con la finalidad de predecir y evitar sobrecargas del sistema. AOC emplea una estrategia de escala horizontal. Se utilizan entornos de características similares que se van añadiendo según las necesidades y el presupuesto.

Se posee evidencia de la notificación por correo de la falta de capacidades en la base de datos SQL del servicio de producción. En dicha evidencia se aprecia un correo automático que informa al operario de la falta de espacio en el disco detallando ambos de forma precisa y otro correo donde el operario informa de forma clara de lo sucedido.

En lo que concierne a componentes certificados, se solicita los pliegos de condiciones técnicas que cumplan con los requisitos mínimos de seguridad para el servicio Hèstia. Ha quedado evidenciado que el servicio se encuentra tras un alinea de firewall estando estos incluidos en la lista de componentes certificados facilitado por el CCN y son:

- Cisco ASA: Cisco Systems 5520 8.2 OS
- Palo Alto's: PAN-3020 6.1 OS

No obstante, se han observado las siguientes deficiencias:

- Se ha evidenciado que no se ha ejecutado nunca un análisis de riesgos sobre el servicio Hestia ni tampoco se dispone de una metodología aprobada de gestión de riesgos.
- No se dispone de un Sistema de Gestión de Seguridad de la Información que permita generar un compromiso con la seguridad de la información, permitir una adecuada gestión de riesgos de TI, cumplir con los requerimientos legales y normativos. El Departamento de Seguridad está finalizando su Marco Normativo de Seguridad.

Marco	Marco operacional (Control de acceso)
Medidas	Op.acc.1 Identificación Op.acc.2 Requisitos de acceso Op.acc.3 Segregación de funciones y tareas Op.acc.4 Proceso de gestión de derechos de acceso Op.acc.5 Mecanismo de autenticación Op.acc.6 Acceso local (local logon) Op.acc.7 Acceso remoto (remote login)

Descripción

El control de accesos obliga a que cada usuario que accede al sistema utilice un identificador único. La Organización debe tener la capacidad para conocer quién es el poseedor de cada identificador y qué derechos ostenta. Cuando un usuario cesará en su actividad, el identificador será inhabilitado, manteniendo los registros de actividad, para asegurar los requisitos de trazabilidad.

La normativa exige una protección de los recursos del sistema que impida su uso por personal no autorizado o con derechos insuficientes. Dichos derechos se establecen por el responsable del recurso y se realiza acorde a la política y normativa de seguridad.

Debe existir segregación de diferentes funciones y tareas que, por su naturaleza, deben ser incompatibles entre sí, por ejemplo, labores de desarrollo, prueba y operación.

Los derechos de los usuarios se deben establecer lo más estrictamente posible, dentro de las necesidades del cargo que desempeña. Estos derechos sólo pueden ser concedidos por el personal correspondiente bajo petición, por escrito, del responsable.

Cada Sistema de Información debe tener identificado un mecanismo de autenticación que, en caso de ser contraseñas, ha de cumplir con los parámetros básicos de configuración y renovación.

El autentificador deberá encontrarse, desde el primer momento de su activación, bajo el control efectivo y exclusivo del usuario correspondiente. Es obligado que el usuario sea informado de su responsabilidad de protección y custodia.

Finalmente, los identificadores deben ser retirados inmediatamente al finalizar la relación con la Organización o cambiar sus responsabilidad en ésta.

Trabajo realizado

AOC dispone de unos procedimientos operativos cuyo alcance incluye el servicio Hestia que permiten asegurar una correcta gestión del control de acceso lógico a los sistemas de información del servicio, estableciendo así unas directrices generales en materia de control de acceso, unos roles y responsabilidades, así como el uso de una herramienta de registro de solicitud en la que quedan registrado el solicitante, perfil y aprobaciones requeridas. Concretamente

- Existe una normativa de control de acceso por parte de AOC, que posee un apartado de identificación, evidencia “EV_002_AOC_NOR_04_Control acces_V2.0”, en él queda especificado:
  - Cada usuario debe tener un identificador singular.
  - Diferentes roles frente al sistema según acceda como ciudadano, como trabajador o administrador de sistemas.
  - Define cuando un usuario será inhabilitado.
- Además, en este documento se especifica en un apartado como el método por el cual se asignan privilegios a un nuevo usuario.
- Existe un procedimiento de dada de altas y bajas, donde los responsables solicitan estas operaciones mediante una herramienta de tiketing, evidencias ‘AltaUsuariOT’ y ‘BaixaUsuariOT’.
- Existe un control que permite identificar al usuario que accede al sistema y opera en él, por el registro de los parámetros de conexión tales como: sistema operativo, dominio, IP.
- El servicio Hestia está dividido en 81 áreas.
- La Normativa de control de acceso “AOC_NOR_04_Control acces_V2.0” apartado 6.2. define la segregación de funciones el proceso de gestión de derechos de acceso y los mecanismos de autentificación. Se especifica que el rol de administrador es incompatible con cualquier otro rol.
- La Normativa describe que los requisitos de acceso de cada usuario están basados en los principios de mínimo privilegio y la necesidad de conocer.

- En cuanto al proceso de alta/baja/modificación de usuarios finales de clientes del Servicio, Los administradores del servicio Hestia dan de alta a un usuario local del cliente con derecho para administrar usuarios locales. Recae en este usuario del cliente administrar correctamente los usuarios y perfiles locales. El servicio Hestia tiene establecido y documentado unos roles y perfiles por defecto que no puede ser modificados por los clientes. Las peticiones de altas y bajas de usuarios admin se realiza por correo electrónico. AOC suele dar un único usuario "coordinador" por cliente.
- Existe documentación detallada en lo referente a identificación y autenticación de los empleados de AOC en el documento "AOC_NOR_04_Control acces_V2.0". En la evidencia se especifica los controles de acceso:
    - Identificación: Queda definido que debe existir un identificador único por entidad (usuario o proceso) que accede al sistema, así como la segregación de roles.
    - Mecanismos de autentificación: Se destacan que existe los siguientes mecanismos:
        - Contraseña
        - Claves concertadas
        - Tarjetas / Certificados de software
        - Biometría
    - Se definen los accesos locales y los remotos.
- En lo relativo a la identificación y autentificación empleada por el sistema Hestia, se posee una evidencia del acceso con usuario y contraseña y la posibilidad de emplear un certificado. Este hecho queda reflejado en la evidencia 'Acces amb certificat'.
- El usuario es informado en la barra superior de la aplicación Hèstia de la última conexión realizada, dando como datos dia/mes/año hora:minutos:segundos.
- El mecanismo de entrega de credenciales para los usuarios del servicio Hèstia se realiza por medio del Administrador de Área encargado de generar dicho usuario. Queda delegada en el cliente concretamente en el usuario Administrador de Área la responsabilidad de marcar la casilla para el cambio de credenciales tras el primer inicio.
- La política de contraseña de acceso al servicio Hestia incluye:
    - Caducidad de contraseñas: 90 días
    - Histórico de contraseñas: 1
    - Complejidad de contraseñas: Mayúscula, minúscula, dígitos
    - Bloqueo de contraseñas: 5 y desbloqueo por administrador
    - Número mínimo de caracteres: 8
- La Normativa de control de acceso incluye controles sobre accesos locales y remotos.
- Existe un registro de accesos fallidos y accesos exitosos a la aplicación Hèstia. Evidencia 'Registre d'accessos erronis'.

Sin embargo, en la revisión de los accesos se han detectado los siguientes aspectos relativos a gestión de accesos:

- No se posee evidencia de inhabilitación de usuarios ni de la retención de cuentas a nivel técnico.
- En la revisión de accesos de una muestra de áreas, se ha identificado una cuenta genérica "Admin" con el Rol de Administrador. Este usuario genérico con máximo privilegios utilizado por los administradores de AOC. Hemos sido informados que al menos 8 usuarios de AOC comparte este usuario. Se ha identificado que almenas ocho personas conocen la contraseña de este usuario y operan con él. Hemos sido informado que la contraseña asociada se ha cambiado recientemente. Se ha identificado para el área de CCT otro usuario con role administrador CCT.
- En el proceso de creación de las credenciales de un nuevo usuario, se crea la misma contraseña por defecto. Como el cambio de contraseña tras la primera conexión, no está configurado por defecto, sino que es el administrador local quién habilita la opción o no, nos podemos encontrar en la situación que algún usuario del área sigue utilizando la misma contraseña por defecto conocida por todos.
- No se dispone de controles para restringir el acceso de usuarios por horario o ubicaciones geográficas.
- Por la sensibilidad de los datos almacenados, el acceso al servicio Hestia exige el uso de al menos dos factores de autenticación. El acceso al servicio se puede hacer con certificado electrónico y unas credenciales o únicamente con usuario y contraseña. Pese a ofrecer doble factor de autenticación a sus clientes, estos suelen utilizar un único factor de autenticación.
- Los accesos remotos por parte de empleados del servicio Hestia se realiza con un cliente VPN y unas credenciales de acceso. No se requiere utilizar un dispositivo de AOC para conectarse remotamente a la red interna. Los usuarios acceden a un escritorio remoto por lo que tendrá el mismo acceso que en local. No hay restricciones de accesos específicos ni tampoco se requiere autorizaciones especiales. Cualquier usuario de AOC tiene acceso remoto a la red interna.
    - Se dispone de evidencia de alta y baja de usuarios en el dominio, VPN. Estas acciones se realizan a través de la herramienta de tiketing empleada por AOC. Las evidencias que se han facilitado muestran las solicitudes de Altas y Bajas para dar acceso a través de la VPN al dominio así como la creación o eliminación de un correo corporativo.

Marco	Marco operacional (explotación)
Medidas	Op.exp.1 Inventario de activos Op.exp.2 Configuración de seguridad Op.exp.3 Gestión de la configuración Op. exp.4 Mantenimiento Op.exp.5 Gestión de cambios Op.exp.6 Protección frente a código dañino Op.exp.7 Gestión de incidencias Op.exp.8 Registro de la actividad de los usuarios Op.exp.9 Registro de la gestión de incidencias Op.exp.10 Protección de los registros de actividad

Descripción

Se debe disponer de herramientas y otras fuentes de información que permitan disponer de un inventario completo de los elementos de red, parque informático y otros servidores que componen su red, asignados a sus respectivos responsables. Además, estos inventarios se mantendrán actualizados.

Se requiere de procedimientos escritos y guías de configuración segura y bastionado para cada uno de los entornos / sistemas desplegados. En caso de que el usuario propicie situaciones que conlleven un posible riesgo para la seguridad de la Organización, se le informará y pedirá consentimiento expreso.

La Organización debe mantenerse informada de las posibles actualizaciones y parches que publiquen los fabricantes. Además, debe disponer de procedimientos que aseguren el análisis y adecuación de la implantación de dichas actualizaciones.

La normativa obliga a que se disponga de un procedimiento que indique la configuración de seguridad inicial y el uso de mecanismos de prevención y reacción frente a código dañino.

Se debe dispone de un procedimiento operativo formal que permita asegurar una correcta gestión de las incidencias, debilidades o eventos que puedan afectar a la seguridad de la información de forma integral.

Se tiene la obligación de disponer de mecanismos que garanticen un correcto sellado de tiempo. Adicionalmente, para los datos categorizados de nivel alto, se requiere una monitorización de las actividades (de acuerdo con las conclusiones del análisis de riesgos) de las actividades de los usuarios, incluyendo los intentos fallidos.

Trabajo realizado y Observaciones

Se ha revisado la información proporcionada y se ha comprobado que:

- El departamento de sistemas dispone de fuentes de información que permiten disponer de un inventario completo de los elementos de red, parque informático y otros servidores que componen su red. Estos inventarios se actualizan automáticamente. Se dispone a su vez de un inventario especifico de las máquinas que dan soporte al servició Hèstia. Evidencia “AOC - AOC-NetworkingBackbone”. De las maquinas del servicio Hèstia se poseen los detalles de las funcionalidades que poseen y cuál es su rol dentro del servicio. Evidencia “Diagrama_Hestia_produccio”
- Las máquinas identificadas del entorno de producción y del entorno de preproducción son:
- PRE:
    - VM00917 - AOC - Eacat PRE FP2IIS - Frontal - Windows server 2008 r2 standard
    - VM00922 - AOC - Eacat PRE FP2SQL - DB - Windows server 2008 r2 standard
- PRO
    - AOC-W-HESTIA-PRO-FP1 - Frontal - Windows server 2008 r2 standard
    - AOC-W-HESTIA-PRO-FP2 - Frontal - Windows server 2008 r2 standard
    - HESTIA-PRO-SQL1 - DB - Windows server 20012 r2 standard
    - HESTIA-PRO-SQL2 - DB - Windows server 20012 r2 standard

- eacatTR64-SQL01 - Antic DB migrat al cluster - Windows server 2008 r2 enterprise

- Para cada una de las máquinas existen responsables bien identificados, de los cuales se posee el rol, el nombre la dirección de correo electrónico y un teléfono fijo. Evidencia "01 Projects - PRJ-HESTIASQL2014PRO".
- Se dispone de guías de configuración segura del CESICAT para plataformas UNIX y Windows. El departamento de sistemas dispone de maquetas pre configuradas de servidores y script de configuración según el servicio que dará el nuevo servidor.
- Todos los dispositivos críticos de AOC disponen de mantenimiento, realizándose a su vez tareas periódicas de mantenimiento sobre los mismos. Sobre los servidores se realizan un mantenimiento preventivo que está documentado y se aplican actualizaciones de sistema operativo controladas siguiendo las indicaciones del fabricante.
- Se dispone de un procedimiento documentado de gestión de parches de seguridad. Todos los parches críticos y de seguridad se instalan en los servidores. Los otros parches son valorados por el equipo de sistemas y seguridad en base a una valoración de riesgos. De la revisión de los parches instalados se destaca:
  - Servidor web IIS: A día de emisión del informe todos los parches disponibles han sido instalados y no existen más actualizaciones para el sistema. Siendo el ultimo parche instalado el día 21 de marzo de 2018.
  - Active Directory: El ultimo parche instalado es del 07 de julio de 2017, previo a este, no se parcheaba el sistema desde el día 04 de diciembre de 2017. Existen actualizaciones importantes de seguridad que deben instalarse.
  - Base de datos SQL: El sistema es parcheado con periodicidad siendo el ultimo parche instalado del día 04 de enero de 2018. Sin embargo a fecha de emisión del informe existen actualizaciones del sistema que no están instaladas
- Los cambios se realizan en ventanas de tiempo concertadas entre sistemas y el personal responsable del servicio Hestia.
- Todo cambio requiere aprobación del responsable, la documentación del cambio, pruebas del sistema tras el cambio, copias de seguridad, actualización del inventario de activos, etc
- Se dispone de una solución completa de protección frente a Antivirus. Se posee evidencia de la instalación de Antivirus en los puestos de trabajo. Además, existe una centralización de los clientes de antivirus en un servidor. En concreto la solución anti virus utilizada por el Consorcio AOC es Kaspersky. "EV_025-Configuracio Antivirus".
- AOC dispone de un procedimiento operativo formal que permite asegurar una correcta gestión de las incidencias, debilidades o eventos que puedan afectar a la seguridad de la información. El Consorcio AOC posee un procedimiento escrito de la gestión de incidentes documentado en la evidencia "EV_002_AOC_PROC_01_incidents seguretat". La gestión de incidencias es soportada por una herramienta de registro que incluye información del solicitante, descripción de la incidencia, tipificación, prioridad, asignación de recursos, actividades de emergencia y modificaciones del sistema derivadas del incidente.
- Se tiene habilitados registros de auditoria de las aplicaciones en el alcance de la revisión. Se ha revisado la información proporcionada en relación al registro de actividad de los usuarios y se ha comprobado que queda reflejado el registro de actividad de los usuarios, en concreto se obtiene registros de:
  - Aplicación
  - SQL Server
  - Sistema Operativa
- Se dispone de un centralizador de logs.
- Se dispone de un procedimiento escrito de gestión y solicitud de los certificados AOC "Gestió de certificats". El servicio Hestia utiliza los siguientes certificados:
  - Certificado de dispositivo de servidor seguro instalado en los 2 frontales del Hestia utilizado para la comunicación TLS entre el cliente Hestia y el servidor IIS. Se utiliza también para la comunicación entre la aplicación cliente de la Hestia y el frontal web para establecer el canal TLS entre los frontales y la AD.
  - Certificado RSA utilizado para encriptar el archivo de configuración de la aplicación (web.config) que contiene los datos de acceso (IPs, usuarios, contraseñas) a los diferentes servidores de la Hestia (AD, BD, SMTP, etc.) a clave es generada, instalada y custodiada automáticamente por .NET a través de scripts.

No obstante, se han observado las siguientes deficiencias:

- Se ha comprobado la habilitación en servidores de producción de servicios innecesarios como el servicio de cola de impresión, Windows Audio o con reconocidas vulnerabilidades como los servicios Remote Registery, UmRdpService, Routing and Remote Access, RPC and Netlogon.
- Se ha evidenciado la presencia de identificadores genéricos en la lista de usuarios locales de servidores como pueden ser administrator, HestiaUSER, CLIUSR o Nttrmadm (utilizado por el proveedor NTT
- En relación a la gestión de logs, se han identificado las siguientes incidencias:
    - No se han identificado controles de seguridad específicos para asegurar la integridad de los registros de auditoria. Hemos sido informados que, para otros servicios, AOC está implementando una solución desarrollada internamente para asegurar la integridad de los registros de auditoria.
- No se dispone de soluciones de protección antivirus en los 3 servidores que compone el servicio.
- Referente al control de gestión de incidentes Se echa en falta procedimientos específicos que definan casos concretos como:
    - Procedimiento de gestión de problemas y análisis de causa raíz
    - Procedimientos para informar a las partes interesadas, internas y externas frente a un incidente de seguridad.

Marco	Marco operacional (Servicios externos)
Medidas	Op.exp.1 Contratación y acuerdos de nivel de servicio Op.exp.2 Gestión diaria Op.exp.3 Medios alternativos

Descripción

Se debe contemplar los riesgos derivados de la contratación a un tercero de determinados servicios. Previamente a formalizar un acuerdo, se debe seguir un procedimiento documentado con los requisitos exigidos a la contratación de servicios externos. En dicho procedimiento se deben incluir aspectos como el impacto producido en la organización (utilizando para ello el análisis de riesgos), las características precisas del servicio prestado, lo que se considera calidad mínima y las consecuencias para el proveedor de incumplimiento por su parte, así como las responsabilidades.

Para la Entidad es obligatorio disponer de un sistema rutinario y documentado que mida el cumplimiento de las obligaciones de servicio, definiendo la frecuencia de las mediciones, el responsable de dicha medición y el protocolo de actuación en caso de incumplimiento o de que la desviación superase el margen de tolerancia acordado.

Trabajo realizado y Observaciones

Se ha revisado la información proporcionada y se ha comprobado que:

- Se ha evidenciado que todos los proveedores de servicios de TI en el alcance del servicio disponen de un contrato de prestación de servicios de TI firmado y vigente.
- Las características de los servicios prestados por proveedores externos al AOC están establecidos contractualmente, y se realizan reuniones periódicas para coordinar y hacer seguimiento en relación al cumplimiento de las obligaciones del servicio.
- Los Pliegos técnicos de condiciones incluyen cláusulas de confidencialidad, deber de secreto, continuidad, seguridad y cumplimiento de los requerimientos del ENS.
- Los contratos con prestadores de servicios incluyen cláusulas de contratación, características del servicio prestado y cómo se determinarán y medirán los acuerdos de nivel de servicio establecidos entre el AOC y el prestador.
- Se dispone de un sistema rutinario para medir el cumplimiento de las obligaciones de servicio. En general, se lleva una coordinación y relación fluida con todos los proveedores mediante reuniones periódicas.
- Se ha facilitado evidencia de un informe de NTT Communications, donde se detalla:
    - Gestión de Niveles de Servicio
    - Gestión de Incidentes y Peticiones
    - Gestión de Eventos
    - Gestión de Capacidades
    - Servicio de Mejora Continua
    - Gestión de Riesgos

No obstante, se han observado las siguientes deficiencias:

- No se dispone de un procedimiento documentado de contratación y seguimiento de servicios externos.
- Se debería incluir en los pliegos de condiciones de productos y servicios externalizados relacionados con el servicio Hestia la obligatoriedad de presentar a petición del AOC un certificado de cumplimiento de los requerimientos del ENS por una entidad independiente.

Marco	Marco operacional (Continuidad del servicio)
Medidas	Op.cont.1 Análisis de impacto Op.cont.2 Plan de continuidad Op.cont.3 Pruebas periódicas

Descripción

Se debe disponer de un procedimiento para el análisis del impacto de una contingencia en continuidad del servicio. En él se verán plasmados los requisitos de disponibilidad del servicio, identificando sus elementos críticos. Dicho procedimiento será revisado periódicamente y requerirá de la aprobación de la dirección.

La Entidad debe disponer de un plan de continuidad en el que se identifiquen las funciones, las responsabilidades y las actividades a realizar. En él se establecerá un comité de crisis que será el encargado de aplicar dicho plan, se definirá la reacción ante interrupciones del servicio y se tendrá documentado un método de actualizaciones periódicas y revisiones.

La Organización debe poseer un procedimiento documentado de mejora para el plan de continuidad realizando las pruebas pertinentes. Dicho procedimiento incluye, entre otros aspectos, al responsable de la ejecución de las pruebas, la forma de realizarlas, los integrantes involucrados.

Trabajo realizado y Observaciones

AOC tiene establecidas medidas para evitar tanto la pérdida de información como la interrupción de actividades del negocio frente a desastres o fallos de los sistemas de información a través de controles como:

- Se realizan copias de seguridad periódicas incrementales y totales de los datos de los servidores de Hestia.
- Todo el personal de Sistemas y desarrollo tiene un backup que puede soportar sus actividades por ausencia prolongada.
- Se realizan pruebas de recuperación periódicas de servidores y bases de datos. En concreto, en las últimas semanas con el proyecto de montar en el Cloud de Azure un entorno de contingencias de Hestia, se han realizado pruebas de recuperación del servicio en Azure.

No obstante, se han observado las siguientes deficiencias:

- No se incluyen los datos de los servidores que soportan el servicio Hestia en las copias de seguridad que externaliza AOC. Las copias del servicio Hestia se hacen en disco y en cintas pero que se ubican en el mismo DataCenter de MediaPro.
- No se dispone de un Plan de recuperación ante desastre de los activos de TI que soportan el servicio Hestia. El Departamento de Sistemas está trabajando en desarrollar planes de recuperación ante desastre de los servicios de AOC.
- No se dispone de los requerimientos de continuidad de negocio en relación al servicio Hestia. No se ha realizado un análisis de impacto cuyo objetivo es conocer las consecuencias de una interrupción en la realización de las actividades del servicio Hestia. Un análisis de impacto permite identificar las necesidades y requerimientos existentes, y consecuentemente, diseñar una adecuada estrategia de recuperación. Este análisis permite establecer un orden de criticidad de las funciones operativas, en función del impacto global que tendría para el servicio y para AOC.
- No se dispone de un Plan de Continuidad de Negocio. El propósito general de un Plan de Continuidad de Negocio es garantizar a la organización la continuidad de los procesos críticos de negocio, y el restablecimiento de las funciones y operaciones críticas en un periodo de tiempo aceptable, para que no se provoque una ruptura total para la organización. El Departamento de Seguridad está trabajando para otros servicios en desarrollar un Plan de Continuidad de Negocio. Se podría aplicar la metodología y actividades aplicadas para el servicio Hestía.
- Se dispone de una única sala de servidores dónde se ubican los servidores que componen el servicio Hestia. En caso de incidente mayor que afecte al CPD, el servicio Hestia quedaría afectado. Tomamos en consideración que se está valorando externalizar la infraestructura tecnológica del servicio a Azure cual servicio ofrece alta disponibilidad.
- Existe una falta de documentación y registro de las pruebas de contingencias tecnológicas que se están realizando.

Marco	Marco operacional (Monitorización del sistema)
Medidas	Op.mon.1 Detección de intrusión Op.mon.2 Sistema de métricas

Descripción

Para la Organización es de obligado cumplimiento aplicar a sus sistemas herramientas de detección o prevención de intrusos. Además, ha de existir documentación publicada que determine el responsable de atender las incidencias y el responsable y frecuencia con la que se analizarán los registros de dicha herramienta.

La Entidad debe tener diseñado y documentado formalmente un sistema de indicadores variable y ampliable en el tiempo capaz de medir la acción real de los sistemas de seguridad implantados por la Organización. Las mediciones deberán reflejar el grado de implantación de las medidas de seguridad en la Organización, la eficacia y eficiencia de estas y el impacto que supone cada incidente de seguridad

Trabajo realizado y Observaciones

Los Firewalls (Cisco ASA 5520 8.2 OS y Palo Alto PAN-3020 6.1 OS) protege la red de producción de AOC de los accesos externos incluye un módulo/sistema de detección de intrusión el cual es configurado y mantenido por el departamento de Sistemas de AOC.

Se dispone de un sistema de monitorización continúa basado en la aplicación Nagios para verificar la disponibilidad y correcto funcionamiento de sus sistemas de información. Se detalla a continuación los controles de monitorización que tiene establecidos AOC:

- Componentes HW del entorno como por ejemplo utilización de la RAM, CPU, capacidad de almacenamiento.
- Correcta ejecución de servicios en servidores que componen la plataforma
- Revisar la LAN de comunicaciones a través de ping.
- Para servidores Windows, se puede llegar a monitorizar accesos específicos de administradores y usuarios como borrado de ficheros o accesos a carpetas.
- Se tiene establecido un sistema de avisos por SMS y turnos de guardia para monitorizar los sistemas.

Se han identificado ciertos indicadores inventariados y medidos por el Departamento de Seguridad de AOC que ayudan a medir el desempeño real del sistema en materia de seguridad. Por ejemplo, se disponen de indicadores relacionados con:

- Numero de vulnerabilidades de los análisis de vulnerabilidades periódicos realizados
- Número de incidentes de Seguridad
- Estadísticas sobre virus

El Departamento de Seguridad dispone de un presupuesto propio revisado y controlado.

No obstante, se han observado las siguientes deficiencias:

- Pese a disponer y tener implementado un sistema de detección de intrusión, no se ha establecido un procedimiento de revisión y monitorización del sistema de detección. No se dispone de alertas preventivas, sino que es tarea del equipo asignado verificar y comprobar los registros y alertas del módulo. La actuación es más reactiva que preventiva.

- AOC no dispone de las métricas requeridas por el Centro Criptográfico Nacional en la herramienta INES para monitorizar cumplimiento del ENS de la Organización o de los servicios que ofrece a entidades públicas y en el alcance del Esquema Nacional de Seguridad. Los indicadores definidos y medidos por el departamento de Seguridad de AOC no cubren todos los dominios de seguridad del Esquema Nacional de Seguridad.

Marco	Medidas de protección (Protección de las instalaciones e infraestructuras)
Medidas	Mp.if.1 Áreas separadas y con control de acceso Mp.if.2 Identificación de las personas Mp.if.3 Acondicionamiento de los locales Mp.if.4 Energía eléctrica Mp.if.5 Protección frente a incendios Mp.if.6 Protección frente a inundaciones Mp.if.7 Registro de entrada y salida de equipamiento Mp.if.8 Instalaciones alternativas

Descripción

La distribución por áreas debe diseñarse según funcionalidad, encontrarse documentada e inventariada. Los permisos de acceso a las diversas áreas han de especificarse en una normativa en la que también se indiquen los controles y vigilancia.

La normativa obliga a la Organización a seguir una política de segregación de las funciones en la gestión del control de acceso, distinguiendo tres roles: autorización, ejecución y registro. Requiere la existencia de un procedimiento que obligue a identificarse de manera inequívoca, previamente al acceso las instalaciones, y a que quede registrada junto con la fecha y hora de entrada/salida.

En caso de nivel de seguridad medio, el procedimiento también debe reflejar el tiempo que permanecerán los registros en el sistema y la obligación del personal de llevar los identificadores siempre visibles.

Cuando el nivel de seguridad se considere alto, será necesario que cada rol anteriormente mencionado recaiga en una persona diferente, y las visitas deberán ser acompañadas en todo momento, salvo consentimiento expreso del responsable de la visita.

La legislación exige la existencia de una normativa que especifique que el suministro de potencia eléctrica será suficiente y que existirá un número adecuado de luces de emergencia, así como su procedimiento de revisión.

Se exige la existencia de documentación donde se indica la protección anti incendio disponible. Esta documentación debe ser acorde a la normativa industrial pertinente.

Trabajo realizado y Observaciones

El Centro de Procesamiento de Datos del servicio Hestia está externalizado al Centro de Procesamiento de Datos del Proveedor de Servicios de TI MEDIAPRO cuyo centro está localizado en las instalaciones del edificio de MEDIAPRO en Barcelona. Mediacloud basa sus servicios en la implementación de las mejores prácticas de ITIL y posee las certificaciones de ISO 27001, ISO 20000, TIER III, etc.

Se han observado los siguientes controles de acceso físico y medioambientales:

- Control de Acceso:
  - El acceso al edificio de MediaPro y al DatCenter se hace a través de una petición inicial realizada a través de la aplicación de ticketing del proveedor. Solo unos usuarios autorizados de AOC están autorizados a pedir acceso.
  - Los sistemas de información de AOC se ubican en una sala compartida con otros clientes. Los sistemas de información de AOC se ubican en rack restringidos por un acceso por llave. Solo Mediapro dispone de las llaves de los Racks
  - El acceso a la sala de servidores se hace a través de una tarjeta de acceso que solo dispone personal del Proveedor. Ningún usuario de AOC dispone de dichas tarjetas. Los accesos no están registrados ni controlados pero el acceso a la sala es monitorizado por una camera de videovigilancia.

- El acceso de visitantes se hace siempre en compañía de un usuario habilitado. Hay un registro de visitas establecido.
- Existe separación física con controles de acceso diferenciado entre la zona de servidores y los armarios de comunicaciones.

- Protección contra incendio:
  - La sala de servidor dispone de sensores de humo conectados a la monitorización general del edificio.
  - El mecanismo de extinción de incendio es automático y contiene gas (F-2000) el cual es permitido y adecuado para la extinción de incendios en los Centros de Procesamiento de Datos.
  - Los sistemas anti-incendios son probados periódicamente por el proveedor de la instalación.
- Medidas Medioambientales:
  - Todos los servidores están almacenados en Racks.
  - El sistema de climatización se compone de varias máquinas de aire acondicionado que funcionan en paralelo para dar cobertura a toda la sala de servidores. Existe un control automático de la temperatura en el Data center y se monitoriza desde el Proveedoor
  - Los sistemas de climatización son probados periódicamente por el proveedor de la instalación.
  - Falso suelo/Falso techo.
- Abastecimiento Eléctrico:
  - Los sistemas de información almacenados en el Data Center disponen de dos fuentes de alimentación independiente.
  - Se dispone de un SAI como suministro de potencia eléctrica en caso de fallo del suministro principal de corriente.
  - Los sistemas de abastecimiento eléctrico son probados periodicamente por el proveedor de la instalación.

Marco	Medidas de protección (Gestión del personal)
Medidas	Mp.per.1 Caracterización del puesto de trabajo Mp.per.2 Deberes y obligaciones Mp.per.3 Concienciación Mp.per.4 Formación Mp.per.5 Personal alternativo

Descripción

Se exige que exista y esté documentado en una política la caracterización de cada puesto de trabajo en materia de seguridad y que se definan sus responsabilidades. Además, dicha política debe incluir los requisitos exigidos para cada puesto de trabajo y obliga a que el proceso de selección del personal se verifique y sea acorde a estos requisitos.

Se obliga a mantener informado al trabajador sobre los deberes y responsabilidades de su puesto en materia de seguridad y a guardar registro de su aceptación. Dentro de la información facilitada al trabajador, deben exponerse las medidas disciplinarias en caso de incumplimiento, el periodo de vigencia de las mismas y el deber de confidencialidad.

La Organización debe diseñar un plan de concienciación para el personal acerca de su responsabilidad con la seguridad. Dicho plan debe contener los datos del responsable de su elaboración, su periodicidad y el contenido.

Se requiere la existencia de un plan de formación que identifique las necesidades de formación en materia de seguridad por cada puesto de trabajo, la planificación de la impartición de la formación y la frecuencia.

Trabajo realizado y Observaciones

AOC dispone de mecanismos para garantizar la seguridad de la información en el ámbito del personal, concretamente en las fases previas a la contratación, durante el período del contrato, y finalmente durante la fase de rescisión del contrato.

- Durante la fase previa a la contratación del personal:
  - Existe un Catálogo de Puestos de Trabajo de todo el personal del AOC. Cada puesto tiene una ficha en la que constan las funciones de dicho puesto.
  - Los empleados de AOC, firman cláusulas en materia de confidencialidad y sus consecuencias legales en caso de incumplimiento. La política de seguridad de AOC especifica que cualquier incumplimiento de la Política y marco normativo que la desarrolla conllevará las acciones disciplinarias pertinentes.
  - la Política incluye un apartado de Directrices de Seguridad de obligado cumplimiento para empleados.
- Durante la relación contractual con el personal:
  - La Política de Seguridad de AOC especifica que, según las necesidades identificadas, el Consorcio AOC realizara obligatoriamente las actividades de formación y concienciación, pudiendo ser específicas para cada área, grupo o persona destinataria. Para todo el personal que utilice, opere o administre los sistemas de información y comunicaciones del Consorcio AOC, es obligatorio la asistencia a las acciones formativas que se realicen en materia de seguridad de la información. Para la difusión y conocimiento de la Política de Seguridad y la normativa complementaria, se realizarán sesiones de formación para todo e | personal del Consorcio AOC, donde se informará de la obligatoriedad de cumplimiento con dichas normativas. La asistencia a las sesiones de formación es de carácter obligatorio.
  - Se ha difundido a todos los empleados de AOC sus funciones y obligaciones en aspectos de seguridad y protección de Datos" COMUNICACIÓ FUNCIONS I OBLIGACIONS DEL PERSONAL". El documento de seguridad de protección de datos incluye las funciones y obligaciones de los empleados respecto a la seguridad de la información.
  - No se ha detectado de forma generalizada, iniciativas de concienciación, educación y capacitación en materia de seguridad de la información, y en el uso correcto de los recursos

de información que tengan a su disposición, con objeto de minimizar los posibles riesgos de seguridad existentes en el desempeño de sus labores diarias.

- Se han identificado cursos de formación a empleados de AOC relacionados con Seguridad de la Información como por ejemplo curso de formación en la herramienta de análisis de riesgos PILAR, cursos sobre privacidad, protección de datos. Existe una falta de Formación específica en Seguridad de la Información para el personal de Sistemas.

- Durante la fase de rescisión contractual:
  - Todos los activos relacionados con la persona que causa baja son devueltos correctamente, al mismo tiempo que se eliminan completamente todos sus derechos de acceso.

Marco	Medidas de protección (Protección de los equipos)
Medidas	Mp.eq.1 Puesto de trabajo despejado Mp.eq.2 Bloqueo de puesto de trabajo Mp.eq.3 Protección de equipos portátiles Mp.eq.9 Medios alternativos

Descripción

La Organización debe disponer de una normativa que refleje la política de “mesas limpias”.

Debe existir una normativa de seguridad que asegure el bloqueo automático, tras un tiempo de inactividad, de cualquier terminal a través del cual se pueda acceder a datos clasificados como nivel de seguridad medio o alto.

La Organización ha de proveer una protección adecuada a los equipos portátiles, detallada en un procedimiento escrito y acorde con la normativa general de la Entidad. En dicho procedimiento se podrán encontrar los mecanismos a seguir en caso de pérdida del control del equipo y la gestión de incidencias.

La Organización debe disponer, además del plan de continuidad, de documentación formal que especifique el procedimiento en caso de indisponibilidad de uso de los equipos habituales

Trabajo realizado y Observaciones

En base a las entrevistas realizadas con las diferentes áreas y las visitas a algunos de los puestos de trabajo se ha observado que:

- No se han identificado incidencias significativas en la gestión del papel. Se aplican los controles de seguridad sobre ficheros no automatizados de la Ley de Protección de datos.
- Está establecida una política de salvapantallas protegido por contraseñas tras 10 minutos de inactividad del usuario.
- Los usuarios no son administradores locales de sus máquinas. Cabe destacar que el grupo de desarrolladores son administradores locales de sus maquinas
- El marco normativo de seguridad de AOC incluye directrices en el buen uso de los sistemas de información de AOC tanto desde las instalaciones de la entidad como en fuera de las instalaciones.
- Se usan portátiles pero la política de empresa es que no se almacena datos sensibles en las maquinas.

Marco	Medidas de protección
Medidas	Mp.com.1 Perímetro seguro Mp.com.2 Protección de la confidencialidad Mp.com.3 Protección de la autenticidad y de la integridad Mp.com.4 Segregación de redes Mp.com.9 Medios alternativos

Descripción

Se obliga a la Organización a disponer de un procedimiento documentado que determine el uso de un firewall configurado para que, únicamente, permita el tráfico de contenido previamente autorizado.

Se debe disponer de una normativa que determine el uso de VPN cifradas (empleando algoritmos certificados por el CCN).

Se debe disponer de una normativa documentada que proteja la autenticidad e integridad de los datos.

Se debe disponer de una normativa que exija, de acuerdo con la arquitectura del sistema, una red segmentada. El tráfico entre segmentos de red ha de encontrarse restringido por defecto, se debe disponer de mecanismos que permitan controlar la entrada de usuarios a cada segmento y se recopila la información que sale de cada uno de dichos segmentos.

Trabajo realizado y Observaciones

La Seguridad perimetral es adquirida a través de los siguientes controles:

- Se dispone de un procedimiento que detalla el estándar de configuración de los cortafuegos que debe ser utilizado por el Ajuntament para mantener una red más segura y prevenir interrupciones en el servicio producidos por amenazas de tipo accidental o intencional que pueda ingresar al perímetro de la red o los sistemas de información.
- El trafico externo del servicio Hestia pasa por los siguientes dispositivos. Se dispone de:
    - Dos firewalls PaloAlto PAN-3020 6.1 OS redundados en alta disponibilidad que ofrece seguridad de capa 7 (aplicación) para separar la red interna de AOC de la red externa.
    - Dos firewalls CISCO ASA Cisco Systems 5520 8.2 OS de nivel 3 en alta disponibilidad. De este modo se mitigan los riesgos de amenazas que afectan a un proveedor de Firewall.
- El acceso a la administración de Firewall es restringido a los empleados de sistemas. No obstante, el Usuario de administración del firewall es genérico. No podemos identificar el usuario que se conecta con el usuario de administración.
- El diagrama de red está actualizado.
- La red interna del AOC está segregada en redes virtuales VLANs. Concretamente los servidores de producción, de pre-producción y estaciones de trabajo se ubican en VLANs diferentes con reglas de acceso entre redes. Existe también una DMZ para los servidores publicados a Internet. Ninguno de los tres servidores que compone la infraestructura Hestia se ubica en la DMZ.
- El departamento de Sistemas realiza periódicamente análisis de vulnerabilidades sobre las IP públicas de servicios públicos. Estos análisis con el mismo alcance son realizados por el CESICAT. No se incluye en el alcance de los análisis de riesgos máquinas de la red interna de AOC entre cuales maquinas se ubican los tres servidores que soportan el servicio Hestia. Tampoco se realizan Test de intrusión o análisis de código sobre el servicio Hestia para identificar amenazas sobre el proceso.
- Las comunicaciones entre clientes y servicios Hestia se hacen vía protocolo TLS 1.2 asegurando la seguridad de las comunicaciones.

- Todos los usuarios de AOC tiene acceso remoto vía escritorio remoto a la red interna de AOC. El usuario que se conecta remotamente tendrá el mismo acceso que si estuviera físicamente conectado a la red interna.
- Se dispone de una lista actualizada de los proveedores de servicios de TI con acceso remoto habilitado. Cada usuario externo tiene un responsable interno en AOC.
- Para acceder remotamente, el usuario interno o externo requiere tener instalado en sus maquina un cliente VPN y disponer de unas credenciales de acceso de Active Directory. No ha doble factor de autenticación para acceder remotamente a la red de AOC. Los accesos remotos se hacen vía VPN. No se emplean soluciones hardware para edificios y clientes VPN para usuarios.
- No se han identificado controles de seguridad sobre sistemas BYOD que se conecta remotamente a la red interna de AOC. Estaciones de trabajo sin Antivirus o Firewall local pueden conectarse a la red interna de AOC siempre y cuando con credenciales autorizados de acceso.

Marco	Medidas de protección (Protección de los soportes de información)
Medidas	Mp.si.1 Etiquetado Mp.si.2 Criptografía Mp.si.3 Custodia Mp.si.4 Transporte Mp.si.9 Borrado y destrucción

Descripción

Se obliga a la Entidad a disponer de procedimientos documentados en los que se especifique la metodología utilizada para el etiquetado de soportes.

Para un nivel de seguridad medio, la Organización debe disponer de una normativa que determine la obligatoriedad de cifrar la información almacenada.

Se debe disponer de un procedimiento documentado que garantice el control sobre los soportes de información. Se requiere que exista un inventario de todos los soportes indicando, entre otros datos, su contenido actual, su responsable y su ubicación.

Se debe disponer de un procedimiento documentado que obligue a registrar toda salida de soportes de las instalaciones de la Entidad, incluyendo el nombre del transportista. También debe quedar constancia de toda entrada de soportes, incluyendo al trasportista.

Se obliga a la Organización a disponer de un sistema documentado que asegure el correcto borrado de los soportes de información que, completada su misión, se destinen a otros usos o se cedan a otra Organización. En caso de que por las características del soporte no sea posible asegurar un borrado adecuado, se tendrá que destruir de modo seguro.

Trabajo realizado y Observaciones

AOC dispone de soportes de información (cintas) que utilizan como soporte extraíble de copias de seguridad de datos críticos de AOC. Hemos sido informados que los datos del servicio Hestia no se incluye a fecha de auditoria en el alcance de las copias de seguridad en cintas.

Se han revisado las medidas de protección de los soportes de información con el objetivo de comprobar la correcta definición y descripción de un procedimiento de gestión de los soportes que contienen datos de ciudadanos. En este sentido, se ha comprobado la existencia de un adecuado procedimiento de gestión de soportes de información dentro del procedimiento de copias de seguridad y el documento de Seguridad.

Se confirma entre otros que:

- las copias de seguridad se externalizan fuera de la sala de servidores de AOC y se almacena de manera segura en otra ubicación.
- Las copias de seguridad cumplen con los requerimientos de protección de datos en cuanto a registro de entrada y salida de datos, inventario e etiquetado y confidencialidad de los datos guardados a través del cifrado del contenido.
- Los soportes y documentos se encuentran debidamente etiquetados e inventariados, y solo son accesibles por personal autorizado a las salas de servidores. La relación completa y actualizada de los soportes utilizados por el CONSORCIO AOC se encuentra referenciada al inventario de soportes custodiado por Seguridad.
- Los soportes que contienen datos de carácter personal son almacenados en un lugar con acceso restringido, accesibles únicamente al personal autorizado
- Existe un registro de entrada y salida de soportes, que permite controlar las entradas y salidas de soportes o documentos, su tipología, la fecha y hora de entrada/salida, el emisor/receptor y destinatario/origen, el número de soportes o documentos del envío cumpliendo con los requerimientos de Protección de datos.
- El traslado de las copias de Seguridad es realizado por personal autorizado.
    - Se dispone de un procedimiento de borrado o destrucción de soportes. El desecho de cualquier documento o soporte con datos de carácter personal, por norma general, se realiza tomando medidas para evitar el acceso a la información o su recuperación posterior.

Marco	Medidas de protección (Protección de las aplicaciones informáticas)
Medidas	Mp.sw.1 Desarrollo Mp.sw.2 Aceptación y puesta en servicio

Descripción

Se debe disponer de una normativa que indique que el desarrollo de aplicaciones se realiza sobre sistemas que no se encuentran en explotación, y que los equipos en producción no pueden encontrarse herramientas de desarrollo.

Se debe disponer de un plan de pruebas documentado previo al paso a explotación, incluyendo verificaciones en materia de seguridad. Dichas comprobaciones han de realizarse en un entorno aislado y se deberá verificar que el nuevo software no compromete la seguridad de los ya existentes.

Trabajo realizado y Observaciones

AOC dispone de una metodología de desarrollo que permite asegurar una correcta gestión del "Desarrollo y Mantenimiento de Sistemas de información" de la Organización, estableciendo unas directrices generales así como el modo en que dichas directrices se deben implantar y operar. Esta Metodología se aplica a los desarrollos del servicio Hestia.

De la revisión de la documentación de los proyectos y cambios realizados, se han identificados los siguientes controles:

- Se dispone de una metodología formal a aplicar en los desarrollos con una estandarización de la documentación en cada fase del proyecto/desarrollo.
- Se ha identificado una documentación extensa de proyectos.
    - Documento de toma de requerimientos (actas de reunión entre el equipo de desarrollo y el equipo del servicio que solicita el cambio).
    - Documento de análisis Funcional.
    - Documento de análisis Técnico.
    - Planes y resultados de pruebas los cuales incluyen controles de entrada/salida y coherencia en la integración de procesos.
- La metodología de desarrollo y los controles a aplicar se incluye en los contratos de prestación de servicios con proveedores de servicio de Desarrollo. Se ha podido evidenciar en algunos pliegos de desarrollo de nuevos servicios la inclusión de la metodología a seguir y los controles de seguridad a aplicar.

No obstante, se han identificado los siguientes incumplimientos respecto a los requerimientos del Esquema Nacional de Seguridad:

- En la definición de los requerimientos, no se ha tenido evidencia que se tienen en cuenta requerimientos de tipo no funcional, como son los requerimientos de seguridad, privacidad de los datos o aspectos de rendimiento del entorno. El Departamento de Seguridad no suele intervenir de manera activa en los proyectos.
- Se ha identificado una falta de segregación de funciones en los pases a producción. Los pases a producción de cambios del servicio Hestia son realizados por los propios desarrolladores, no existiendo una adecuada segregación de funciones. Este hecho ha sido corregido en el transcurso de la auditoria. Los cambios son realizados por el equipo de sistemas de AOC
- Durante la auditoria, por una incidencia aislada que afecte al entorno de producción del servicio Hestia, se dispone de un único entorno para producción y test con los evidentes riesgos de seguridad asociados. Las pruebas se realizan en el mismo entorno productivo.
- No se incluye previo a la entrada en servicio de nuevos cambios en el servicio Hestia los siguientes controles:

- Análisis de vulnerabilidades. Los análisis que se ejecutan no incluyen en su alcance los 3 servidores del Servicio Hestia.
- Pruebas de penetración
- Auditorias del código fuente.

Marco	Medidas de protección (Protección de la información)
Medidas	Mp.info.1 Datos de carácter personal Mp.info.2 Calificación de la información Mp.info.3 Cifrado Mp.info.4 Firma electrónica Mp.info.5 Sellos de tiempo Mp.info.6 Limpieza de documentos Mp.info.9 Copias de seguridad

Descripción

Se debe disponer de un procedimiento documentado que permita identificar si el sistema trata datos de carácter personal y, en caso de utilizar dicho tipo de datos, si cumple con las medidas indicadas por el R.D. 1720/2007.

Se debe reflejar en la política de seguridad quién es el responsable de cada información manejada por el sistema. Además, se especifica los criterios con los que la entidad, conforme a la ley, categoriza la información. Para cada responsable, existirá un procedimiento formal que detalla el método de asignar a la información un determinado nivel de seguridad.

La Organización debe disponer de una normativa documentada que exija el cifrado de la información de seguridad de nivel alto tanto en su almacenamiento como en su transmisión. Únicamente estará permitida la información en claro mientras se encuentre en uso.

La Organización debe disponer de una política de Firma Electrónica aprobada por el órgano superior competente.

La Entidad ha de disponer de un procedimiento documentado para identificar, establecer un tiempo de retención y fechar electrónicamente documentos acreditativos.

Se debe disponer de un procedimiento documentado en el cual el responsable de la información debe determinar la frecuencia con la que se realizan copias de seguridad de los datos bajo su responsabilidad y durante qué periodo se mantendrá.

Trabajo realizado y Observaciones

En lo relativo a la Ley Orgánica de Protección de Datos (LOPD 15/1999 y RD 1720/2007), el AOC ha realizado las siguientes acciones:

- Se han declarado sus ficheros a la Agencia Catalana de Protección de Datos.
- Se dispone del Documento de seguridad requerido por la Ley actualizado a fecha de octubre de 2017.
- Se está ejecutado la auditoria bienal de cumplimiento de los requerimientos del RD 1720/2007. Dicha auditoria ha sido realizada por una consultora externa.

No se han identificado normas y procedimientos de gestión de los activos de información en el Consorci (inventario, marcado y utilización, y clasificación de la información), los cuales, fundamentalmente deben permitir identificar y mantener un inventario de activos, y clasificar según la importancia de la información por parte de las diferentes áreas de negocio del Consorci en términos de seguridad (derivados principalmente de los atributos confidencialidad, integridad y disponibilidad), para asegurar un nivel adecuado de protección de los activos.

Pese a almacenar información clasificada como de nivel alto según los requerimientos de confidencialidad del Esquema Nacional de Seguridad, no se está aplicando requerimientos de cifrado en la información almacenada en la BBDD SQL de Hestia.

El Servicio Hestia no incluye a fecha de auditoria firma electrónica y sello de tiempo.

Existe un procedimiento formal y escrito de realización de copias de seguridad o de recuperación de datos que incluye los servidores del servicio Hestia.

El alcance de las copias de seguridad de los datos del Servicio Hestia es:

- Copia Incremental diaria a disco con tiempo de retención mensual. Es responsabilidad de sistemas asegurarse que las copias de seguridad se realizan de manera adecuada.

- Copia Full semanal a disco con tiempo de retención semanal. Es responsabilidad de sistemas asegurarse que las copias de seguridad se realizan de manera adecuada.
- Se realiza además por parte del equipo de desarrollo una copia de la Base de Datos de Producción total con periodicidad mensual en la misma máquina de Producción.
- Se realizan restauraciones de datos y de Bases de Datos de manera periódica con objeto de verificar el funcionamiento y aplicación de los procedimientos antes descritos.
- Existe un procedimiento de copias y restauraciones de backups del Consorcio AOC, en él se detalla:
    - Procediment de còpies de seguretat de la plataforma de negoci
    - Ubicació de suports
    - Revisió de les còpies de seguretat
    - Registre dels suports
    - Sol·licitud d'una alta, baixa o modificació d'un còpia de seguretat
    - Procediment de restauració de còpies de seguretat de la plataforma de negoci
    - Sol·licitud de restauració
    - Execució de la restauració
    - Procediment de còpies de seguretat de la plataforma d'oficines
    - Política de backups.
    - Ubicació de suports
    - Revisió de les còpies de seguretat
    - Registre dels suports
    - Sol·licitud d'una alta, baixa o modificació d'un còpia de seguretat
    - Procediment de restauració de còpies de seguretat de la plataforma d'oficines
    - Sol·licitud de restauració
    - Execució de la restauració

Cabe destacar que las copias de seguridad no se hacen en base a unos requerimientos de continuidad de Negocio.

Marco	Medidas de protección (Protección de los servicios)
Medidas	Mp.s.1 Protección del correo electrónico Mp.s.2 Protección de servicios y aplicaciones web Mp.s.8 Protección frente a la denegación de servicio Mp.s.9 Medios alternativos

Descripción

Se debe disponer de procedimientos documentados que detallen la protección del servicio de correo electrónico, incluyendo aspectos de disponibilidad. En dichos procedimientos debe quedar reflejada la protección a la que se somete la información distribuida vía correo electrónico, la protección durante el encaminamiento de mensajes, el filtrado de spam o la utilización de medidas de protección contra código dañino.

Se debe disponer de una normativa documentada que especifique las medidas de seguridad de los subsistemas de publicación de información, en concordancia con las amenazas detalladas en el análisis de riesgos. Especialmente debe garantizar un adecuado control de acceso a la información que requiera autenticación, evitando vías de acceso alternativas y sin control.

Se debe disponer de capacidad de procesamiento suficiente para atender con holgura la carga de trabajo prevista. Se debe dotar a los sistemas de tecnologías para la prevención de ataques de denegación de servicio.

Trabajo realizado y Observaciones

Se observan los siguientes aspectos:

- Se dispone de sistemas de Antivirus y Antispam como medidas de protección para el correo electrónico.
- El departamento de Sistemas realiza periódicamente análisis de vulnerabilidades sobre las IP públicas de servicios públicos. Estos análisis con el mismo alcance son realizados por el CESICAT. No se incluye en el alcance de los análisis de riesgos máquinas de la red interna de AOC entre cuales maquinas se ubican los tres servidores que soportan el servicio Hestia. Tampoco se realizan Test de intrusión o análisis de código sobre el servicio Hestia para identificar amenazas sobre el proceso.
- Frente a ataques de denegación de servicios, se dispone de los siguientes controles de seguridad:
    - Balanceadores de carga y dos frontales que controlan las peticiones de conexión

PARA MÁS INFORMACIÓN:

Valentín Fauna
+34 932 003 233
valentin.faura@bdo.es

bdo.es
bdo.global

Auditoría & Assurance | Advisory | Abogados | Outsourcing