RESULTADOS DE AUDITORÍA INTERNA DE SEGUIMIENTO DEL PLAN DE SEGURIDAD DOCUMENTAL DEL SIGC-SUA. CICLO DE GESTIÓN 2013.	
SERV. /UNIDAD	SERVICIO DE INFORMÁTICA
FECHA DE REALIZACIÓN DE LA AUDITORÍA:	28/11/2013 – 13:30
AUDITORES :	▪ Auditor coordinador. Francisco David Susí García. ▪ Auditor. Antonio Martínez Olea
RESPONSABLE DE UNIDAD:	▪ Adelaida Cabrero.
PERSONAS DE LA UNIDAD ENTREVISTADAS	▪ Julián García Cabrera ▪ Fran Soler Soler ▪ Francisco Alcántara Checa ▪ Antonio Rabadán López

INFORME EJECUTIVO

Nivel de implantación del plan de seguridad: ADECUADO

Recomendaciones básicas:

1. Actualizar y completar las fichas del Plan de Seguridad de acuerdo a las anotaciones realizadas en las actividades y conclusiones de auditoría.
2. Actualización a la última versión del Software Antivirus propuesto por el propio Servicio de Informática en su micrositio.

INFORME GENERAL

OBJETIVOS DE AUDITORÍA: PLAN DE SEGURIDAD DOCUMENTAL DEL SISTEMA	
Verificación de los elementos reflejados en las fichas de la unidad contenidas en el Plan de Seguridad Documental del SIGC-SUA	
Tipo de Elemento	***Elementos de seguridad de documentación y elementos ELECTRÓNICOS***
Actividades y conclusiones de auditoría	1. Se observa que el sistema de gestión de solicitudes GESOL se encuentra ubicado en un servidor con el mismo nombre. Dado que el sistema están en desuso por la implantación del nuevo gestor integral EASYVISTA, no procede la revisión de las copias de seguridad de las mismas. 2. El nuevo sistema de gestión de peticiones e incidencias de servicios TIC es gestionado por Easyvista desde el 20 de Junio de 2013. Este sistema se encuentra gestionado por la propia empresa Easyvista y cuenta con acceso TIC identificado para técnicos y las propias medidas de seguridad del proveedor. Existe un contrato de mantenimiento donde se especifican todas estas condiciones. Se acuerda con la responsable de la unidad el envío del contrato para seleccionar la información a publicar en el Plan de Seguridad Documental. 3. Durante la auditoría del Repositorio de Documentación del Servicio de Informática, al estar alojado en el servidor CARABE, común para multitud de elementos documentales de muchos de los servicios y unidades administrativas de la Universidad, se observa el robusto sistema de copias de seguridad diario con 30 días de caducidad, contándose con logs descriptivos de los procesos de backup a través del Sistema de Backup Centralizado (TIVOLI). 4. Durante la Auditoría, se observa que la versión del motor antivirus de algún equipo no está actualizada. En este sentido, se comenta la posibilidad de realizar un envío de correo electrónico a la comunidad universitaria informando de la

	idoneidad de instalar la última versión del motor del software antivirus. 5. Se observa que el gestor de contenidos institucional cuenta con un contrato de mantenimiento con la empresa que participó en su diseño. Además, los técnicos del Servicio de Informática realizan copias de seguridad diarias a través de TIVOLI, tanto de la estructura y contenidos del gestor de contenidos, como de la capa de BBDD del mismo.
Tipo de Elemento	***Medidas de seguridad en los sistemas TIC gestionados por el Servicio de Informática de la Universidad de Jaén***
Actividades y conclusiones de auditoría	1. Se observa que el CPD cuenta con las medidas de seguridad reflejadas en el Anexo correspondiente al Plan de Seguridad Documental y además, la responsable del servicio indica que existe una segunda puerta de acceso que sólo se abre desde el interior del CPD por seguridad. 2. Se observa que el sistema BMS (Building Management System) que controla las variables de seguridad del CPD tanto de alimentación eléctrica, como de temperatura e incendios, está gestionado por la Unidad Técnica, según se indica en las propias instrucciones técnicas de esta unidad (IT 025 e IT 010). El BMS emite alertas que son recibidas por distintos responsables de la Unidad Técnica además de la empresa de seguridad privada. Se observa que en el propio CPD existe un registro manuscrito de mediciones diarias de valores termométricos realizadas por miembros de la Unidad Técnica. 3. Existe un Sistema de Almacenamiento en Red (SAN, Storage Area Network) en el propio CPD y sese observa como se mantienen en funcionamiento algunos sistemas de Backup en cintas magnéticas.

Recomendaciones generales
• Se recomienda la actualización de la información en las fichas del Plan de Seguridad Documental de acuerdo a las observaciones realizadas en las actividades y conclusiones de auditoría sobre los sistemas de copias de seguridad centralizados. • Se recomienda, recabar información sobre los contratos externos vigentes para, una vez seleccionada la información no sensible que no comprometa la propia seguridad del sistema, se publique como anexo dentro del Plan de Seguridad Documental (Easyvista y Gestor de Contenidos Institucional)