INFORME DE AUDITORÍA INTERNA DE SEGUIMIENTO ANUAL 2013.	
SERV. /UNIDAD	Unidad Técnica
FECHA DE REALIZACIÓN DE LA AUDITORÍA:	14/11/2013 – 12:00 y 28/11/2013 – 14.45
AUDITORES :	▪ Auditor coordinador. Francisco David Susí García. ▪ Auditor. Luis Espinosa de los Monteros Moreno ▪ Auditor. Antonio Martínez Olea
RESPONSABLE DE UNIDAD:	▪ Nemesio Martínez Mellado ▪ Juan Navas Alba
PERSONAS DE LA UNIDAD ENTREVISTADAS	▪ José Miguel Estepa Álvarez ▪ Juan Miguel Cruz Lendínez ▪ Rafael Velasco García

INFORME EJECUTIVO

Nivel de implantación del plan de seguridad: ADECUADO

Recomendaciones básicas:

1. Actualizar las fichas del Plan de Seguridad de acuerdo a las anotaciones realizadas en las actividades y conclusiones de auditoría.
2. Instalación o actualización a la última versión del Software Antivirus propuesto por el Servicio de Informática.
3. Valorar la oportunidad para la realización de copias de seguridad de las comunicaciones de alertas recibidas por el BMS, al menos, a través del email.

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 la existencia de documentación en formato papel que no está incluida en las fichas del Plan. Se trata de documentación sobre la gestión del mantenimiento, partes que son firmados y posteriormente se registran en la base de datos. Se encuentran ubicados en la dependencia B1-103A. 2. Se observa que el correo nequipa@ujaen.es se gestiona a través de GMAIL no siendo descargado en ningún sitio y estando siempre en los servidores externos, no estando esta situación reflejadas en las fichas del plan. 3. Se observa que la versión del software antivirus no es homogénea en todos los equipos de la unidad. 4. Durante la auditoría del servicio de informática, realizada el 28/11/2013 a las 13 horas, se detecta que existe un sistema de gestión de edificios (BMS) que se encuentra ubicado en el CPD y que al producirse una variación por encima de los parámetros límite establecidos, envía un aviso a varios dispositivos móviles (de personal de la Unidad Técnica y del servicio de vigilancia de las instalaciones) así como correos electrónicos con información detallada de los sucesos. Estas comunicaciones no se salvaguardan en la UT. 5. Se observa durante la visita al CPD que ante la inexistencia de avisos durante un periodo de tiempo inusual, los miembros de la unidad técnica pusieron en marcha un registro manual de mediciones de temperaturas del CPD que se ha mantenido durante un tiempo hasta comprobar que no existen problemas. Este registro se

	encuentra en el propio CPD protegido con una funda de plástico multitaladro pegada al mobiliario. 6. Se observa durante la visita que existe un equipo en la Unidad Técnica que sólo se conecta cuando es necesario para dar de alta o baja llaves Dallas así como descargar el registro de accesos. Este equipo funciona con Windows 98 por la peculiaridad de las necesidades software para la programación de llaves.

Recomendaciones generales

- Se recomienda la actualización del motor del software antivirus a la última versión propuesta por el Servicio de Informática en su página web.
- Se recomienda la actualización de los elementos en fichas del Plan de Seguridad Documental.
- Se recomienda la realización de copias de seguridad de las comunicaciones de alertas del BMS.