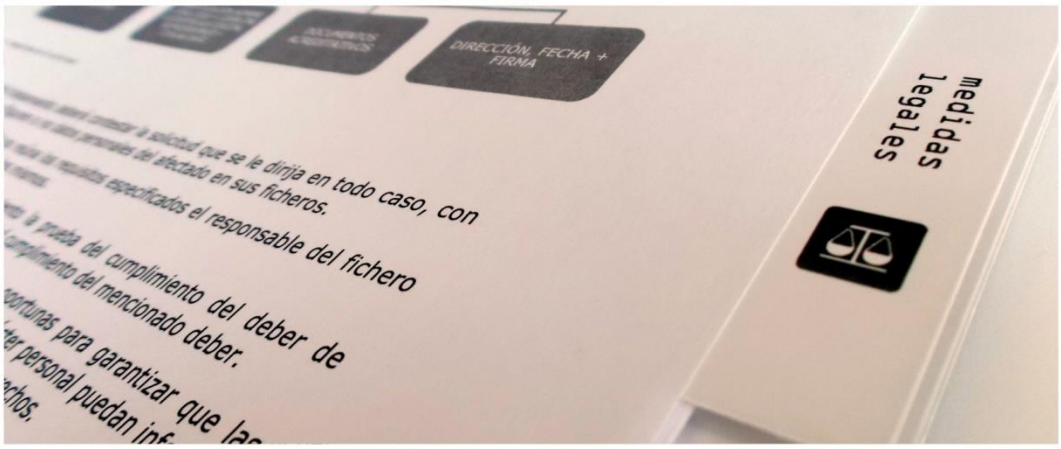
DIAGNOSIS INFÓRMATICA



administracion@aixacorpore.es www.aixacorpore.es Tel: 922 625 942 Fax: 922 623 878 C/ El Cristo 30-A Las Torre de Taco 38108 - La Laguna S/C de Tenerife

ÍNDICE

1. INTRODUCCIÓN

1.1. OBJETO

El objeto del presente informe consiste en realizar un estudio de la implementación de las medidas de seguridad para la documentación que contenga datos de carácter personal gestionada por parte de **COLEGIO OFICIAL DE QUIMICOS DE CANARIAS**, (en adelante, LA EMPRESA).

1.2. ÁMBITO DE APLICACIÓN

El informe comprende una revisión del sistema de información de la EMPRESA:

- Sistema informático
- Organización y segregación de funciones del personal
- Documento de seguridad
- Medidas de seguridad informáticas

1.3. DESCRIPCIÓN GENERAL DEL SISTEMA DE INFORMACIÓN

El sistema informático de LA EMPRESA consta de un total de 2 ordenadores dentro de un mismo sistema de información.

- 1 Linux Ubuntu
- 1 Windows 7 Home

2. ANALISIS GENERAL INFORMATICO

Según el estudio realizado a COLEGIO OFICIAL DE QUIMICOS DE CANARIAS, se ha obtenido la siguiente información:

2.1. ANALISIS SATISFACTORIO

ORDENADORES:

- El equipo tiene instalado como sistema operativo Windows 7 Home Premium SP1, por lo que es más seguros, estable y avanzado tecnológicamente.
- El Sistema Operativo se encuentra actualizado en los Equipos, por lo que éstos se encuentran protegidos contra las últimas amenazas conocidas.
- Los equipos requieren de usuario y contraseña para el acceso al sistema.
- Cada miembro del personal tiene un usuario que lo identifica inequívocamente en los sistemas y su contraseña es confidencial.
- El protector de pantalla se activa de forma automática tras un periodo de inactividad no superior a 10 min y es necesario introducir la contraseña de sesión para su desbloqueo.
- Los sistemas de LA ENTIDAD se encuentran protegidos ya que los equipos tienen instalados como solución antivirus (Avast), el antiespías y el firewall se encuentra activado.
- LA ENTIDAD tiene insertado en las firmas de correo electrónico la advertencia de protección de datos. De esta forma en cada correo generado se informa de la normativa al receptor.

SERVIDOR:

- El sistema operativo instalado (Linux Ubuntu 16.04) es específico para cumplir las tareas típicas de un servidor. Estas funciones son alojamiento de ficheros y controlador de dominio. Con estas dos funciones se garantiza que en la copia de seguridad se incluya una mayor cantidad de datos y se minimice el impacto por pérdida de éstos y una mejor gestión de las contraseñas.
- El Sistema Operativo se encuentra actualizado y protegido contra las últimas amenazas conocidas.
- Para el acceso al Servidor se requiere de Usuario y Contraseña.
- Las contraseñas se encuentran compuestas por mayúsculas, minúsculas y caracteres alfanuméricas.

- El Servidor se encuentra localizado en una zona restringida, accesible sólo por el personal autorizado.

APLICACIONES:

- **Microsoft Office**
    - Herramienta estándar utilizada para el manejo de los documentos de texto, hojas de cálculo, etc.

TRATAMIENTOS:

- Se encuentra firmado el contrato de protección de datos entre LA ENTIDAD y el encargado del tratamiento de los tratamientos externalizados.
- Están en Vigencia los contratos con los encargados del tratamiento de los tratamientos externalizados de la Entidad.

ACCESO A TRAVÉS DE REDES DE COMUNICACIÓNES:

- La entidad utiliza Cloud Station para acceder de forma remota a los datos que gestiona.
- El acceso a datos de carácter personal a través de redes de comunicaciones de forma remota es seguro, ya que la aplicación utilizada garantiza el mismo nivel de seguridad que en un acceso local.
- La transmisión de datos de carácter personal por medio de las redes de telecomunicaciones se llevan a cabo de forma cifrada, por lo que es seguro.
- El prestador de servicios de mantenimiento informático tiene acceso remoto en el caso que se produzca una incidencia.
- LA ENTIDAD dispone de redes inalámbricas.
- El acceso remoto realizado por parte del personal de mantenimiento informático se encuentra autorizado por escrito.
- La wifi de LA ENTIDAD se encuentra bloqueada por medio de una clave según el estándar WPA con cifrado AES y tiene una clave con al menos 15 caracteres y cobina numeros, letras y caracteres especiales.

FICHEROS TEMPORALES:

- Se generan temporalmente ficheros de trabajo necesarios para un tratamiento

ocasional o como paso intermedio durante la realización de un tratamiento; pero éstos mantienen en todo momento un nivel de seguridad adecuado para el acceso a los datos.

- Los ficheros temporales son eliminados una vez han dejado de prestar la utilidad para los que fueron creados.

EXISTENCIA DE LAS POLÍTICAS DE SEGURIDAD:

- En LA ENTIDAD existe un Documento de Seguridad en el que se recogen todos los extremos recomendados. Tambien se establecen en éste, el ámbito de aplicación y los recursos protegidos.
- En el Documento, se especifica con claridad al responsable de Seguridad.
- El documento de seguridad se encuentra actualizado ya que su revisión se realiza con regularidad y se plasma en él, las distintas modificaciones que se producen en LA ENTIDAD.

FUNCIONES Y OBLIGACIONES DEL PERSONAL:

- Están documentadas las funciones y obligaciones de cada una de las personas con acceso a datos de carácter personal y a los sistemas de información por medio de perfiles declarados en las políticas de seguridad.
- En las políticas de seguridad se encuentra declarada la delegación de funciones e identificado los miembros del personal habilitados para otorgar autorizaciones.
- El responsable de seguridad ha proporcionado al personal la circular de protección de datos y se encuentra firmada por todos los empleados y colaboradores de LA ENTIDAD.
- Durante la tramitación de los datos, los miembros del personal siguen una política de mesas limpias para impedir que personas no autorizadas accedan a los datos en tramitación y que no se encuentran almacenados.

REGISTRO DE INCIDENCIAS:

- No se han producido incidencias desde la última revisón tecnica realizada; aunque se prevé llevar a cabo su registro cuando éstas afecten a los datos de carácter personal que maneja LA ENTIDAD, utilizando el protocolo de actuación estandarizado en las políticas de Seguridad en el Anexo "Gestión de incidencias" donde se incluye un modelo de notificación y resolución de incidencias para facilitar al Responsable de Seguridad su documentación y archivo.
- Las incidencias producidas se registran cuando éstas afectan a los datos de

carácter personal que maneja LA ENTIDAD, utilizando el protocolo de actuación estandarizado en las políticas de Seguridad en el Anexo "Gestión de incidencias" donde se incluye un modelo de notificación y resolución de incidencias para facilitar al Responsable de Seguridad su documentación y archivo.

IDENTIFICACIÓN Y AUTENTICACIÓN

- Todos los usuarios del sistema tienen una cuenta de usuario y contraseña que los identifica inequívocamente, además de existir una relación actualizada de ellos en el sistema.
- Las contraseñas son asignadas asignada por el usuario de modo que se guarda en todo momento la confidencialidad de éstas, siendo conocida única y exclusivamente por el usuario.
- Las contraseñas se almacenan de manera cifrada en el sistema.
- Las contraseñas se cambian con una periodicidad de cuando hay cambio de personal días.
- Los equipos están protegidos por medio de contraseña.

CONTROL DE ACCESO*:*

- Los usuarios tienen acceso autorizado a la información y se utiliza el sistema de grupos y permisos para el nivel de acceso.
- Se utilizan mecanismos para impedir el acceso a recursos a usuarios sin autorización.
- El personal externo que trabaja en LA ENTIDAD tiene las medidas de seguridad adecuadas para el tipo de datos a los que accede.

GESTIÓN DE SOPORTES:

- El inventario de los equipos y perifericos de la entidad se encuentra correctamente actualizado reflejando los sistemas que gestionan regularmente los datos de LA ENTIDAD

COPIAS DE SEGURIDAD:

- Se realiza las copias de seguridad en Servidor con una frecuencia diaria por medio de Copia directa.
- Se comprueba que la copia de respaldo se realiza satisfactoriamente al menos

semestralmente.

- Para las pruebas que se realizan con datos reales el sistema garantiza una seguridad adecuada para el nivel de datos utilizados, además de la realización de una copia de seguridad anterior al comienzo de las pruebas.

- La copia de seguridad se realiza con una frecuencia diaria; que es adecuada.

CRITERIOS DE ARCHIVOS DE DOCUMENTOS:

- Los datos gestionados en soporte papel, son organizados por medio de un proceso definido, por lo que es posible la localización y consulta de la información, además de posibilitar los derechos de oposición al tratamiento, acceso, rectificación, cancelación, portabilidad y limitación de uso.

DISPOSITIVOS DE ALMACENAMIENTO DE DOCUMENTOS:

- La documentación física de LA ENTIDAD se almacena de forma que se obstaculiza su apertura y acceso a personal no autorizado.

2.2. CORRECCIONES

EXISTENCIA DE LAS POLÍTICAS DE SEGURIDAD:

- No se llevan a cabo los controles periódicos indicados en el documento de seguridad.

COPIAS DE SEGURIDAD:

- No se ha redactado un procedimiento que garantice la reconstrucción de los datos en caso de pérdida de información en el sistema.

2.3. MEDIDAS RECOMENDADAS A ADOPTAR

El sistema de información de LA EMPRESA se compone de 1 estación de trabajo y un servidor. El equipo informático que compone el sistema de información tiene como Sistema Operativo Linux Ubuntu 16.04 y Windows 7 Home Premium SP1, por lo que la totalidad de los sistemas no se encuentran protegidos contra las últimas amenazas ya que el Windows XP ha dejado de tener soporte por parte de Microsoft. Por lo que recomendamos que dicho sistema operativo sea actualizado a alguno de los que aún cuentan con dicho soporte.

Con respecto al servidor, el sistema operativo utilizado es correcto ya que es específico para el alojamiento de ficheros.

En lo que se refiere a su ubicación, éste se encuentra localizado en despacho con acceso restringido, siendo sólo accedido por personal autorizado.

Respecto a la identificación en los equipos no hay objeción ya que se encuentran dados de alta todos los usuarios en los sistemas de manera personalizada y única.

Los ordenadores cuentan con antivirus (Avast), firewall activado y antiespias, por lo que en este aspecto no hay objeciones.

La firma de correo electrónico se encuentra correctamente configurada, ya que en cada mensaje enviado se muestra la advertencia de protección de datos.

Respecto a los ficheros temporales, como pueden ser correos electrónicos o plantillas, utilizados en la entidad para el desarrollo de las tareas diarias, son eliminados una vez han dejado de prestar la utilidad para los que fueron creados.

Las copias de seguridad se realizan con una periodicidad diaria mediante Servidor utilizando la aplicación Copia directa y se comprueba que se ha realizado correctamente.

Los empleados y colaboradores han firmado la circular de protección de datos por lo que dan a entender que se les ha informado acerca de las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias en caso de su incumplimiento.

Por último, sólo recordar que es necesario realizar las actualizaciones pertinentes en el Documento de Seguridad de LA EMPRESA, cambios que incluyen modificaciones de software, alta y baja de usuarios, inventario de soportes o el registro de incidencias.

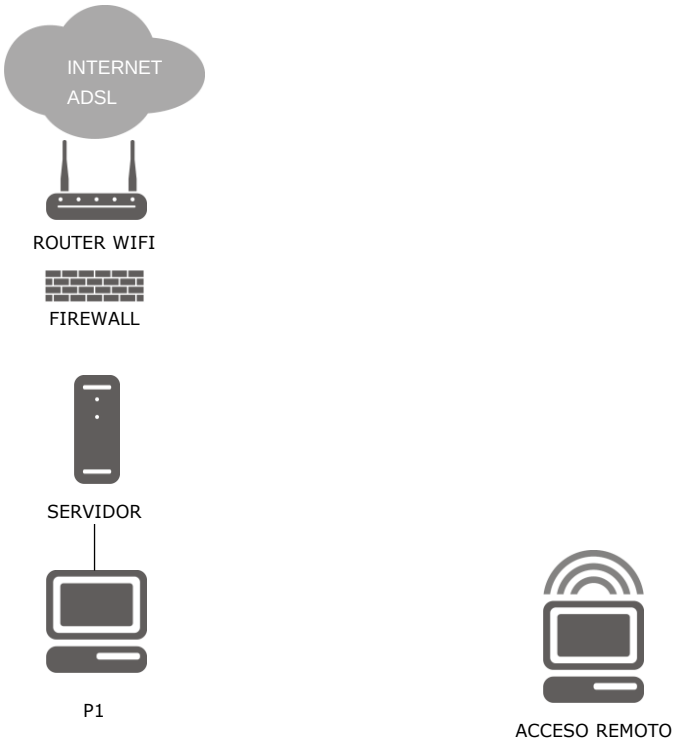
3. CONCLUSIONES-RECOMENDACIONES

Para solventar las deficiencias encontradas recomendamos:

Nº	EXISTENCIA DEL DOCUMENTO DE SEGURIDAD
1	Realizar los controles periódicos que se encuentran en el anexo "Registro de controles periódicos" de su documento de seguridad.

Nº	MEDIDAS RECOMENDADAS A ADOPTAR CON LAS COPIAS DE SEGURIDAD
1	Redactar un procedimiento que permita recuperar el funcionamiento del sistema en caso de fallo, describiendo la forma de restaurar las copias de seguridad.

4. ARQUITECTURA DEL SISTEMA



CLIENTE: COLEGIO OFICIAL DE QUIMICOS DE CANARIAS

Nº DE CONTRATO: PD00111

FECHA: 24/11/2012

AIXA CORPORE, S.L me ha informado de las medidas que debe implementar COLEGIO OFICIAL DE QUIMICOS DE CANARIAS para adecuarse correctamente al RGPD, a través del informe de verificación técnica del día 28/05/2021.

El informe se ha realizado de conformidad con la entrevista mantenida con D. MIGUEL JAUBERT.

COLEGIO OFICIAL DE QUIMICOS DE CANARIAS

D. Iñigo Jaudenes Ruíz de Atauri

AIXA CORPORE S.L

D. Alejandro Benítez