Presentación

La rápida evolución de las Tecnologías de la Información presenta innumerables ventajas desde el punto de vista asistencial, pero tiene un impacto importante en la seguridad de los sistemas lo que hace necesario replantear las medidas, procedimientos y roles definidos tradicionalmente para la gestión de la seguridad de los Sistemas de Información.

Por otro lado, la automatización de los procesos de tratamiento de datos nos proporcionan sustanciales ventajas, aumentando nuestra productividad de forma considerable y poniéndonos a nuestro alcance ventajas y beneficios impensables hace algunos años.

Sin embargo, por un lado como ciudadanos, somos conscientes de la necesidad de una protección adecuada de nuestra privacidad y por otro lado como usuarios del sistema, debemos facilitar la consecución de éstos derechos. La Ley de Protección de Datos de Carácter Personal (LOPD), establece las reglas y obligaciones para la utilización de éste tipo de datos y protege los derechos del ciudadano, que es el propietario de los datos.

El objetivo de éste tríptico es simplemente relacionar una serie de medidas básicas, no por ello menos importantes, necesarias para poder establecer un nivel de seguridad adecuado en nuestro entorno de trabajo.

Solo deberás leerlas y cerciorarte de que cumples con ellas en tu trabajo diario, para así poder mejorar la seguridad entre todos día a día.

Recuerda:
Si exiges seguridad para tu vida, cumple con la seguridad en el trabajo.

Oficina de Seguridad de la Información

Junta de Castilla y León

Sacyl

Información sobre la Seguridad de la Información en el Centro de Trabajo

Junta de Castilla y León

Sacyl

Identificador y control de acceso

- El identificador (código de usuario) y la contraseña (palabra de paso) son estrictamente personales, por lo que no debes dejarlo al alcance en ningún tipo de soporte o papel, ni cediéndolo bajo ningún concepto para su uso por otro usuario.
- No debes de entrar en ningún caso a los sistemas de información utilizando un identificador ajeno, ni siquiera con el consentimiento del titular.
- Debes modificar la contraseña la primera vez que accedas al sistema y modificarla con periodicidad, evitando el uso de contraseñas antiguas.
- En el caso de que sospeches que alguien puede saber tu contraseña de acceso, debes notificarlo a tu responsable y modificarla de inmediato.

Almacenamiento

- No debes imprimir ni realizar fotocopias de datos confidenciales o de carácter reservado, a menos que sea absolutamente necesario. Si lo haces, debes recoger esos datos rápidamente de la bandeja de la impresora o fotocopiadora.

Software y Aplicaciones

- Solo deberás utilizar únicamente las versiones de software facilitadas por Sacyl, y en ningún caso se permite ni la instalación, ni el uso de copias ilegales o sin licencia de programas.
- El software antivirus debe estar habilitado de manera constante, notificando a tu responsable su posible mal funcionamiento en el caso de que se desactive.

Comunicaciones

- Es necesaria la autorización del responsable de comunicaciones para hacer uso de cualquier dispositivo, por ejemplo módem, que posibilite la conexión de los recursos informáticos de Sacyl a una red de comunicaciones externa diferente.

Puesto de Trabajo

- No debes dejar desatendido tu ordenador; si debes ausentarte de tu puesto, apágalo o bloquéalo por medio del salvapantallas con contraseña.
- Debes hacer buen uso de los medios de información disponibles (Internet, correo electrónico...) que Sacyl te proporciona.
- No debes utilizar ningún soporte informático de almacenamiento que provenga de fuera de tu ámbito de trabajo (disquetes, cd´s, usb´s...)

Seguridad de los Datos

- Debes mantener la más absoluta confidencialidad sobre todos los datos de los que tengas conocimiento directa o indirectamente en el ejercicio de tu trabajo.
- Debes comunicar a tus superiores cualquier anomalía o incidencia que observes.
- No debes sacar información de ningún tipo al exterior, bien sea por medios físicos o a través de medios telemáticos (envío de correos a terceras personas,...).

Confidencialidad de la información

- Deberás guardar, por tiempo indefinido, la máxima reserva sobre los datos gestionados. Además, no debes divulgar, ni utilizar directamente, ni a través de terceras personas o empresas, la información reservada a la que tengas acceso durante tu relación laboral con Sacyl, cualquiera que sea el soporte en el que se encuentre dicha información.

Datos de Carácter Personal

- Bajo ningún concepto, se pueden almacenar datos de carácter personal de forma particular. La creación de dichos ficheros, con contenido personal está absolutamente prohibido. Si dispones de datos de carácter personal debes contactar con el departamento de Informática de tu Centro.
- Cualquier persona que intervenga en el tratamiento de datos de carácter personal está obligado al secreto profesional respecto de los mismos "continuando ésta obligación aún después de finalizar sus relaciones profesionales con los responsables de los datos de carácter personal".