



DECLARACIÓN FUNCIONES Y OBLIGACIONES del personal CON ACCESO A DATOS PERSONALES

ALCANCE

Afecta a todo el personal de **HHSCJ HOSPITAL SAN RAFAEL** con acceso a datos de carácter personal. Este acceso puede ser directo, motivado por razones de trabajo, o indirecto, por circunstancias eventuales o para compartir espacios de trabajo.

Sus obligaciones son cumplir las medidas de seguridad determinadas para los tratamientos de datos que realicen y reportar cualquier incidencia o carencia que detecten al responsable del área, sistemas o, en su caso Delegado de Protección de Datos, según el procedimiento de gestión Violaciones de Seguridad que se pondrá en conocimiento de los usuarios.

FUNCIONES Y OBLIGACIONES

D./Dña. [REDACTED], miembro del perfil [REDACTED], mayor de edad, declara haber sido formado e informado de las obligaciones que asume como usuario con acceso a datos personales de HHSCJ HOSPITAL SAN RAFAEL, especialmente de las siguientes:

OBJETIVO DEL DOCUMENTO

La seguridad siempre ha sido un concepto presente en todos los sistemas de gestión de la información. Su implementación no es sencilla, porque abarca todos los eslabones de la cadena de gestión de la información y requiere de un gran conjunto de medidas organizativas y tecnológicas.

El éxito de su implantación depende además de que exista en todos los niveles de la organización una cultura de la seguridad, es decir, una concienciación sobre la necesidad de que la información se mantenga en secreto, íntegra y disponible.

Uno de los eslabones normalmente más débiles de la cadena de gestión de la información es precisamente el Usuario final del sistema (informático y papel).

El Usuario final necesita, por tanto, ser concienciado en materia de seguridad de la información y al mismo tiempo debe disponer de unas normas de obligado cumplimiento respecto al uso de los sistemas informáticos a su alcance, así como soportes o documentos en papel.

El presente documento establece así, las normas de uso del ordenador asignado al puesto de trabajo, la red corporativa, equipos portátiles, aplicaciones informáticas, así como sobre el acceso y tratamiento de datos de carácter personal, a nivel informático y en papel.

Es fundamental que todos los empleados de HHSCJ HOSPITAL SAN RAFAEL que utilizan equipamiento informático y accedan o traten información de carácter personal para la realización de sus funciones y tareas sean conocedores de estas normas.

1. PROPIEDAD Y USO DE LOS ORDENADORES PERSONALES.

HHSCJ HOSPITAL SAN RAFAEL facilita a los usuarios el equipamiento informático necesario para la realización de las tareas relacionadas con su puesto de trabajo.

Este equipamiento es propiedad de HHSCJ HOSPITAL SAN RAFAEL y no está destinado a un uso personal. En consecuencia, y ejercitando el derecho establecido en el artículo 20.3 del Estatuto de Trabajadores,

"El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso."

HHSCJ HOSPITAL SAN RAFAEL se reserva el derecho, de realizar temporalmente, previo aviso al trabajador, controles de los soportes informáticos y/o en papel, puestos a disposición del empleado, para el desarrollo de las tareas relacionadas con su puesto de trabajo.

La dirección de sistemas junto con el responsable de seguridad serán los responsables de definir la configuración básica hardware y software de los puestos de trabajo y administrar los accesos a la red corporativa. Cualquier necesidad de modificación del puesto será solicitada por la persona responsable de la dirección o unidad que lo solicita.

Los usuarios deben cumplir las siguientes medidas de seguridad establecidas por HHSCJ HOSPITAL SAN RAFAEL para el uso de los ordenadores personales:

- No está permitido alterar la configuración física de los equipos ni conectar otros dispositivos a iniciativa del usuario, así como variar su ubicación.
- No está permitido alterar la configuración software de los equipos, desinstalar o instalar programas o cualquier otro tipo de software distinto a la configuración lógica predefinida.
- No está permitida la conexión de ordenadores no autorizados (fijos o portátiles) a la red corporativa.
- La copia de seguridad periódica de los datos alojados en los servidores corporativos es responsabilidad de las unidades de informática.
- Está prohibido utilizar, copiar o transmitir información contenida en los sistemas informáticos para uso privado o cualquier otra distinta del servicio al que está destinada.
- Los ordenadores portátiles tienen la misma consideración de puestos de trabajo y se rigen por estas mismas normas. El uso al que están destinados y la posibilidad de que estos equipos se utilicen fuera del entorno de seguridad de la red corporativa de HHSCJ HOSPITAL SAN RAFAEL hace necesarios procedimientos de seguridad específicos en relación con la actualización de los sistemas antivirus y del software instalado.
 - Los equipos portátiles, así como los dispositivos o soportes informáticos, única y exclusivamente están puestos a disposición con la finalidad de permitir el desempeño de las funciones y tareas laborales encomendadas, estando prohibido el uso para otras finalidades de carácter personal.
 - El usuario está obligado a utilizar los sistemas de información de HHSCJ HOSPITAL SAN RAFAEL y sus datos sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de HHSCJ HOSPITAL SAN RAFAEL o de terceros.
 - Las contraseñas de acceso al equipo, sistema y/o a la red, concedidos por HHSCJ HOSPITAL SAN RAFAEL, son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida. De este modo, está prohibido, entre otros: i) emplear identificadores y contraseñas de otros usuarios para acceder al sistema y a la red de la organización ii) Intentar modificar o acceder al registro de accesos. iii) Burlar las medidas de seguridad establecidas en el sistema informático, intentando acceder a ficheros y iv) En general, el empleo de la red corporativa, sistemas, equipos informáticos y cualquier medio puesto al alcance del usuario, vulnerando



el derecho de terceros, los propios de la organización, o bien para la realización de actos que pudieran ser considerados ilícitos.

- Queda prohibido terminantemente la apropiación de archivos o ficheros titularidad de HHSCJ HOSPITAL SAN RAFAEL, para uso particular y/o de terceros. Es por esto que, en este sentido, se abstendrá de copiar la información contenida en los ficheros en los que se almacenen datos de carácter personal u otro tipo de información de la organización en ordenador propio, pen drives o a cualquier otro soporte informático. En caso de que así fuera menester, deben ser eliminados una vez hayan dejado de ser útiles y pertinentes para la satisfacción de los fines que motivaron su creación. Asimismo, durante el periodo de tiempo que los ficheros o archivos permanezcan en el equipo o soporte informático de su propiedad, deberá restringir el acceso y uso de la información que obra en los mismos.
- En relación con lo anterior, deberá restringir a terceros (familiares, amistades o cualesquiera otros) el acceso a los archivos o ficheros titularidad de la organización y dispuesto a razón única de las funciones o tareas desempeñadas en HHSCJ HOSPITAL SAN RAFAEL
- Toda actividad realizada sobre los sistemas de información de HHSCJ HOSPITAL SAN RAFAEL es susceptible de ser auditada
- En el caso de que los ordenadores tengan un uso compartido, tal responsabilidad alcanzará al empleado durante el tiempo en el que tenga a su disposición el citado equipo
- Se establecerán medidas de protección adicionales que aseguren la confidencialidad de la información almacenada en el equipo cuando el usuario del mismo así lo solicite o cuando se trate de datos de carácter personal que requieran de las medidas de seguridad establecidas por la legislación vigente.

2. USO DE LA RED CORPORATIVA.

La red corporativa es un recurso compartido y limitado. Este recurso sirve no sólo para el acceso de los usuarios internos de HHSCJ HOSPITAL SAN RAFAEL la intranet o Internet, sino también para el acceso a las distintas aplicaciones informáticas corporativas y la comunicación de datos entre sistemas de tiempo real y explotación.

Los usuarios deben cumplir las siguientes medidas de seguridad establecidas por HHSCJ HOSPITAL SAN RAFAEL para el uso de la red corporativa:

- La utilización de Internet por parte de los usuarios autorizados debe limitarse a la obtención de información relacionada con el trabajo que se desempeña como HHSCJ HOSPITAL SAN RAFAEL, debiendo por lo tanto evitarse la utilización que no tenga relación con las funciones del puesto de trabajo de usuario, o que pudiera conducir a una mejora en la calidad del trabajo desarrollado.
- Está prohibido el uso de programas de compartición de contenidos, habitualmente utilizados para la descarga de archivos de música, vídeo, etc.
- Se considera el correo electrónico como un instrumento básico de trabajo.
- Los envíos masivos de información, así como los correos que se destinen a gran número de usuarios serán solo los estrictamente necesarios, que no puedan provocar un colapso del sistema de correo. Todos estos envíos se realizarán aplicando la funcionalidad de 'Copia Oculta' (Bcc o CCo) del gestor de correo electrónico.

- No deberán abrirse anexos de mensajes ni ficheros sospechosos o de los que no se conozca su procedencia.

3. ACCESO A APLICACIONES Y SERVICIOS.

Los usuarios deben cumplir las siguientes medidas de seguridad establecidas por HHSCJ HOSPITAL SAN RAFAEL el uso de aplicaciones y servicios corporativos:

- Tanto el acceso al ordenador como a las distintas aplicaciones corporativas será identificado (mediante usuario y contraseña, u otro mecanismo) y previamente autorizado por el responsable correspondiente.
- La custodia de la contraseña es responsabilidad del usuario. Nunca debe utilizarse la cuenta de usuario asignada a otra persona.
- Las contraseñas no deben anotarse, deben recordarse.
- Las contraseñas deben cambiarse periódicamente. Los usuarios disponen de mecanismos para modificar la contraseña de acceso siempre que lo consideren conveniente. Esto garantiza el uso privado de las mismas.
- Cuando se considere que la identificación de acceso se ha visto comprometida se deberá comunicar al responsable correspondiente.
- Al abandonar el puesto de trabajo deben cerrarse las sesiones con las aplicaciones establecidas, y apagar los equipos al finalizar la jornada laboral. Excepto en los casos en que el equipo deba permanecer encendido.

4. ACCESO Y TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL, A NIVEL INFORMÁTICO Y EN PAPEL.

Las anteriores instrucciones serán de aplicación en la observancia del cumplimiento de una normativa de especial importancia, la protección de datos de carácter personal [Ley Orgánica de Protección de Datos de Carácter Personal]. Dado que esta Ley trata de salvaguardar un derecho fundamental, mediante la adopción de diferentes medidas de seguridad, técnicas y organizativas, el usuario, que accede y trata información de carácter personal en el desempeño de las funciones y tareas, deberá atender a las siguientes obligaciones

- Guardar el necesario **secreto** respecto a cualquier tipo de información de carácter personal, conocida en función del trabajo desarrollado, incluso una vez concluida la relación laboral con el HHSCJ HOSPITAL SAN RAFAEL
- **Datos de carácter personal** = información alfabética, numérica, gráfica, fotográfica, acústica o de cualquier otro tipo, relativa a un aspecto/s físico, psíquico, fisiológica, cultural, social o económico de la persona, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.

FICHEROS INFORMÁTICOS

En particular, respecto a la información de carácter personal contenida en ficheros informáticos, deberá cumplir, en consonancia con lo expuesto en anteriores apartados, las siguientes diligencias:

- **Claves de acceso al sistema informático.**- Las contraseñas de acceso al sistema informático son personales e intransferibles, siendo el Usuario el único responsable de las consecuencias que pudieran derivarse de su mal uso, divulgación o pérdida. Queda prohibido, asimismo, emplear identificadores y contraseñas de otros Usuarios para acceder al sistema informático. En caso de que fuera necesario acceder al sistema, en ausencia de un compañero, se solicitará al Departamento de Informática para que se



habilite el acceso eventual. Una vez finalizada la/s tarea/s que motivaron el acceso, deberá ser comunicado, de nuevo, al Departamento de Informática.

- **Bloqueo o apagado del equipo informático.-** Bloquear la sesión del usuario en el supuesto de ausentarse temporalmente de su puesto de trabajo, a fin de evitar accesos de otras personas al equipo informático. Esto, sobre todo, deberá tenerse en cuenta, por parte del personal que esté en atención al público.
- **Almacenamiento de archivos o ficheros en la red informática.-** Guardar todos los ficheros de carácter personal empleados por el Usuario, en el espacio de la red informática habilitado por HHSCJ HOSPITAL SAN RAFAEL a fin de facilitar la realización de las copias de seguridad o respaldo y proteger el acceso frente a personas no autorizadas.
- **Manipulación de los archivos o ficheros informáticos.-** Únicamente las personas autorizadas, podrán introducir, modificar o anular los datos personales contenidos en los ficheros. Los permisos de acceso de los usuarios a los diferentes ficheros son concedidos por el HHSCJ HOSPITAL SAN RAFAEL en concreto por el Departamento de Informática. En el caso de que cualquier usuario requiera, para el desarrollo de su trabajo, acceder a ficheros a cuyo acceso no está autorizado, deberá ponerlo en conocimiento del citado departamento.
- **Generación de ficheros de carácter temporal.-** Ficheros de carácter temporal son aquellos en los que se almacenan datos de carácter personal, generados a partir de un fichero general para el desarrollo o cumplimiento de una tarea/s determinada/s. Estos ficheros deben ser borrados una vez hayan dejado de ser necesarios para los fines que motivaron su creación, y mientras estén vigentes, deberán ser almacenados en la carpeta habilitada en la red informática. Si transcurrido un mes el usuario detecta la necesidad de continuar utilizando la información almacenada en el fichero, deberá comunicárselo al Departamento de Sistemas, para adoptar las medidas oportunas sobre el mismo.
- **No uso del correo electrónico para envíos de información de carácter personal sensible.-** No utilizar el correo electrónico (corporativo o no) para el envío de información de carácter personal especialmente sensible (esto es, salud, opiniones políticas, ideología, convicciones religiosas o filosóficas, origen racial o étnico, afiliación sindical, vida sexual u orientación sexual, datos genéticos o biométricos). Este envío únicamente podrá realizarse si se adoptan los mecanismos necesarios para evitar que la información no sea inteligible ni manipulada por terceros. De modo que, se pondrá en conocimiento del Departamento de Informática para que implemente el cifrado, encriptado u otro mecanismo que salvaguarde la integridad y privacidad de la información.
- **Comunicación de incidencias que afecten a la seguridad de datos de carácter personal.-** Comunicar al Departamento de sistemas las incidencias de seguridad de las que tenga conocimiento, que puedan afectar a la seguridad de los datos personales. Para ello se dispone de la siguiente dirección de correo electrónico: dpd.hsrafael@hospitalarias.es

Entre otros, tienen la consideración de **incidencia** de seguridad que afecta a los ficheros informáticos, los sucesos siguientes:

- Pérdida de contraseñas de acceso a los Sistemas de Información.
- Uso indebido de contraseñas.
- Acceso no autorizado de usuarios a ficheros excediendo sus perfiles.
- Pérdida de soportes informáticos con datos de carácter personal.

- Pérdida de datos por mal uso de las aplicaciones.
- Ataques a la red.
- Infección de los sistemas de información por virus u otros elementos dañinos.
- Fallo o caída de los Sistemas de Información, etc.

FICHEROS EN PAPEL

En relación con los ficheros en soporte o documento papel, el Usuario deberá cumplir con las siguientes diligencias:

- **Custodia de llaves de acceso a archivadores o dependencias.-** Mantener debidamente custodiadas las llaves de acceso a los locales o dependencias, despachos, así como a los armarios, archivadores u otros elementos que contenga soportes o documentos en papel con datos de carácter personal.
- **Cierre de despachos o dependencias.-** En caso de disponer de un despacho, cerrar con llave la puerta, al término de la jornada laboral o cuando deba ausentarse temporalmente de esta ubicación, a fin de evitar accesos no autorizados.
- **Almacenamiento de soportes o documentos en papel.-** Guardar todos los soportes o documentos que contengan información de carácter personal en un lugar seguro, cuando estos no sean usados, particularmente, fuera de la jornada laboral. Cuando estos soportes o documentos no se encuentren almacenados, por estar siendo revisados o tramitados, será la persona que se encuentre a su cargo la que deba custodiar e impedir, en todo momento, que un tercero no autorizado pueda tener acceso.
- **No dejar en fotocopiadoras, faxes o impresoras papeles con datos de carácter personal.-** Asegurarse de que no quedan documentos impresos que contengan datos personales, en la bandeja de salida de la fotocopiadora, impresora o faxes.
- **Documentos no visibles en los escritorios, mostradores u otro mobiliario.-** Se deberá mantener la confidencialidad de los datos personales que consten en los documentos depositados o almacenados en los escritorios, mostradores u otro mobiliario.
- **Desechado y destrucción de soportes o documentos en papel con datos personales.-** No tirar soportes o documentos en papel, donde se contengan datos personales, a papeleras o contenedores, de modo que pueda ser legible o fácilmente recuperable la información.

A estos efectos, deberá ser siempre desechada o destruida mediante destructora de papel u otro medio que disponga HHSCJ HOSPITAL SAN RAFAEL.

Se prohíbe terminantemente echar en papeleras, contenedores de cartón o papel, soportes o documentos, donde se contengan datos personales.

- **Archivo de soportes o documentos.-** Los soportes o documentos en papel deberán ser almacenados siguiendo el criterio de archivo de HHSCJ HOSPITAL SAN RAFAEL. Dichos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información.

Los soportes o documentos se archivarán en el lugar correspondiente, de modo que permitan una buena conservación, clasificación, acceso y uso de los mismos.

No podrá acceder o utilizar los archivos pertenecientes a otros Departamentos, que compartan la sala o dependencia habilitada a archivo.

- **Traslado de soportes o documentos en papel con datos de carácter personal.-** En los procesos de traslado de soportes o documentos deberán adoptarse medidas dirigidas para impedir el acceso o manipulación por terceros y, de manera que, no pueda verse el contenido, sobre todo, si hubieren datos de carácter personal.



- **Traslado de dependencias.**- En caso de cambiar de dependencia, en el proceso de traslado de los soportes o documentos en papel, se deberá realizar con el debido orden. Asimismo, se procurara mantener fuera del alcance de la vista de cualquier personal de la entidad, aquellos documentos o soportes en papel donde consten datos de carácter personal.
- **Envío de datos personales sensibles en sobre cerrado.**- Si se envían a terceros ajenos al HHSCJ HOSPITAL SAN RAFAEL datos especialmente sensibles (esto es, salud, ideología, religión, creencias, origen racial o étnico) contenidos en soporte o documento papel, se debe realizar, en sobre cerrado y, en cualquier caso, tener presente que haya de efectuarse por medio de correo certificado o a través de una forma de correo ordinario que permita su completa confidencialidad.
- **Comunicación de incidencias que afecten a la seguridad de datos de carácter personal.**- Comunicar las incidencias de las que tenga conocimiento y que puedan afectar a la seguridad de los datos personales.
Entre otros, tienen la consideración de **incidencia** de seguridad, que afecta a los ficheros en papel, los sucesos siguientes:
 - Pérdida de las llaves de acceso a los archivos, armarios y/o dependencias, donde se almacena la información de carácter personal.
 - Uso indebido de las llaves de acceso.
 - Acceso no autorizado de usuarios a los archivos, armarios y/o dependencias, donde se encuentran ficheros con datos de carácter personal.
 - Pérdida de soportes o documentos en papel, con datos de carácter personal.
 - Deterioro de los soportes o documentos, armarios o archivos, donde se encuentran datos de carácter personal.

De todo lo cual, declaro haber recibido la información/formación

En Barcelona, a de Enero de 2020

NOMBRE:

DNI:

Firma: