

Este documento se ha obtenido directamente del original que contenía las firmas auténticas y se han ocultado los datos personales protegidos y los códigos que permitían acceder al original

Hospital El Escorial

Normativa buenas prácticas para terceros

Hospital El Escorial.

Uso Interno

Comité de Seguridad

Control de versiones:

Ver	Fecha	Descripción	Autor(es) Fecha	Aprobado Fecha
V1.0	Noviembre 2014	Documento H. El Escorial. Normativa buenas prácticas para terceros	Jefe Servicio Informática Comité de Seguridad	Nov 2014
V1.1	Marzo 2016	Documento H. El Escorial. Normativa buenas prácticas para terceros	Jefe Servicio Informática Comité de Seguridad	Abril 2016
V1.2	Marzo 2017	Documento H. El Escorial. Normativa buenas prácticas para terceros	Jefe Servicio Informática Comité de Seguridad	Abril 2017
V1.3	Marzo 2024	Documento H. El Escorial. Normativa buenas prácticas para terceros	Jefe Servicio Informática Comité de Seguridad	

Consideraciones de seguridad

La presente documentación es propiedad del Hospital El Escorial y tiene carácter de USO INTERNO. No podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquiera otro. Asimismo, tampoco podrá ser objeto de préstamo, o cualquier forma de cesión de uso sin el permiso previo y por escrito del Hospital El Escorial, titular de los derechos de propiedad intelectual. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga acceso a la documentación será perseguido conforme dicte la ley.

Índice

1.	Introducción.....	4
1.1	Objetivo	4
1.2	Ámbito de Aplicación	4
1.3	Vigencia.....	5
1.4	Referencias y Marco Normativo.....	6
1.5	Normas Previas	7
1.6	Responsabilidades	7
1.7	Definiciones	8
2.	Desarrollo.....	10
2.1	Medidas de Seguridad con respecto a TERCEROS	11
2.2	Retirada de material por TERCEROS.....	14
2.3	Intercambio de Información	15
2.4	Accesos Remotos.....	15
2.5	Uso de Acceso a Internet.....	16
2.6	Supervisión y Revisión de Acuerdos.....	17
2.7	Uso del Correo Electrónico	17
2.8	Funciones y obligaciones en materia de LOPD.....	17
2.9	Comunicación de incidencias, deficiencias y mejoras	19
2.10	Accesos a carpetas/recursos de red	20
2.11	Instalación y uso del Software	21
2.12	Gestión de Usuarios (altas, bajas y modificaciones)	21
2.13	Cumplimiento del presente Código	21
3.	ANEXOS	21

1.1 Introducción

1.2 Objetivo

Esta norma tiene como objetivo presentar un Modelo de Contenido de Buenas Prácticas para Terceros, cuando estos últimos presten servicios en el Hospital El Escorial, permitiendo que se tenga acceso a una recopilación de los principales aspectos y normas con el fin de garantizar un nivel de seguridad adecuado en la utilización de los sistemas de información pertenecientes al Hospital El Escorial, sin perjuicio del cumplimiento del resto de las obligaciones que les pudiera ser de aplicación.

La información debe ser protegida, independientemente del soporte en el que se encuentre. Por ello, se deben establecer normas que deberán ser comunicadas a todo el personal y a terceras partes, para proteger la información y cualquier activo de información.

Por todo ello, los empleados externos del Hospital El Escorial con acceso a información, tendrán acceso a este documento, en el que se definen las funciones y obligaciones del personal externo.

1.3 Ámbito de Aplicación

Esta normativa es de aplicación a todo el ámbito de actuación del Hospital El Escorial, y sus contenidos se ubican bajo las directrices de carácter más general definidas en la Política de Seguridad de la Información del Hospital El Escorial.

Este documento se considera de uso interno del Hospital El Escorial y por tanto no podrá ser divulgado salvo autorización del Comité de Seguridad.

En este sentido, su alcance comprende toda la información utilizada para el desarrollo de las funciones y competencias atribuidas al Hospital El Escorial, así como los sistemas de información que la gestionan, y será de obligado cumplimiento para todo el personal de terceras instituciones que preste sus servicios en el Hospital El Escorial. Por tanto, su alcance incluye a todos los usuarios de entidades externas al Hospital El Escorial que requieran, en el marco de un acuerdo

de colaboración o relación contractual, de acceso a los activos de información del Hospital El Escorial.

Este documento deberá ser comunicado a todos los empleados externos, manteniéndose actualizado e informando a los empleados externos cada vez que se produzcan cambios.

1.3 Vigencia

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte del Hospital El Escorial.

Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de esta Normativa.

La gestión de esta Norma corresponde al Comité de Seguridad, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.
- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
- Verificar su efectividad.

Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el Comité de Seguridad revisará la presente Norma, que se someterá, de haber modificaciones, a la aprobación del Comité de Seguridad del Hospital El Escorial.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

Será el Comité de Seguridad el encargado de la custodia y divulgación de la versión aprobada de este documento.

1.4. **Referencias y Marco Normativo**

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en adelante LOPD.
- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.
- Real Decreto 17/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en adelante Reglamento de desarrollo o RDLOPD.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) en el ámbito de la Administración Electrónica.
- Ley 34/2002, de 11 de Julio, de Servicios de Sociedad de la Información y de Comercio Electrónico (LSSICE).
- Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.
- Ley 31/1995, de 8 de Noviembre, de Prevención de Riesgos Laborales.
- Acuerdo de confidencialidad y seguridad para el personal externo que presta servicios para la Consejería de Sanidad de la Comunidad de Madrid.
- ORDEN 491/2013, de 27 de junio, por la que se aprueba la política de seguridad de la información en el ámbito de la Administración Electrónica y de los Sistemas de Información de la Consejería de Sanidad de la Comunidad de Madrid.

1.5. **Normas Previas**

El presente "Modelo de Buenas Prácticas para Terceros" complementa, en sus aspectos específicos, a la "NORMATIVA GENERAL DE BUENAS PRÁCTICAS", así como a la "NORMATIVA GENERAL DE UTILIZACIÓN DE LOS RECURSOS Y SISTEMAS DE INFORMACIÓN DEL Hospital El Escorial, así como por lo que tales normativas generales serán de aplicación en los aspectos no señalados en ésta.

1.6. Responsabilidades

Las responsabilidades del presente procedimiento son las siguientes.

Actores	Responsabilidades
Usuarios	Cumplir con las directrices establecidas en la Normativa de Buenas Prácticas para Terceros , haciendo un uso responsable de los canales de intercambio de información del Hospital El Escorial, así como de la información intercambiada.
Comité de Seguridad	<p>Comprobar que los usuarios de las entidades prestando servicios para el Hospital El Escorial tienen conocimiento de la Normativa de Buenas Prácticas para Terceros del Hospital El Escorial.</p> <ul style="list-style-type: none"> Definir y actualizar las líneas maestras en las que se debe basar el intercambio de información con entidades externas. Coordinar las actuaciones de auditoría para garantizar el cumplimiento por parte de las entidades prestando servicios para el Hospital El Escorial de las medidas de seguridad definidas en la presente normativa.

1.7. Definiciones

A los efectos previstos en esta normativa, se atenderá a las definiciones recogidas en el documento de "GLOSARIO DE TÉRMINOS". En particular para esta Norma se entenderá por:

- Tercero:** la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento. Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados
- Usuario:** cualquier persona que preste sus servicios en cualesquiera de los Hospitales pertenecientes a la Consejería de Sanidad de la Comunidad de Madrid, u organismos dependientes de la misma, así como al personal de entidades externas, que desarrollen tareas, permanentemente u ocasionalmente, en cualquier órgano perteneciente o adscrito a

la Consejería. Tendrán la consideración de usuarios los sujetos autorizados a acceder a los sistemas de información.

- **Confidencialidad:** propiedad o característica de los activos consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- **Sistema de tratamiento:** modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados (o manuales) o parcialmente automatizados (o mixtos).
- **Soporte:** objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.
- **Tratamiento de datos:** cualquier operación y/o procedimiento técnico de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
- **Accesos autorizados:** autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.
- **Datos especialmente protegidos:** Son datos correspondientes al ámbito de la intimidad personal y familiar, y no de la profesional. El artículo 7 LOPD establece que son los datos de carácter personal que revelen ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual, así como la comisión de infracciones penales o administrativas.

Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética

- **Responsable del fichero o tratamiento:** persona física o jurídica, de naturaleza pública o privada u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

- **Afectado o interesado:** persona física titular de los datos que sean objeto del tratamiento de conformidad con la LOPD.
- **Encargado del tratamiento:** la persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.
- **Documento:** todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.
- **Ficheros temporales:** ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.
- **Identificación:** procedimiento de reconocimiento de la identidad de un usuario.
- **Incidencia:** cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.
- **Perfil de usuario:** accesos autorizados a un grupo de usuarios.
- **Recurso:** cualquier parte componente de un sistema de información.
- **Sistema de información:** conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.
- **Sistema de tratamiento:** modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

1.4 Desarrollo

El presente documento establece una serie de medidas de seguridad que serán aplicables y exigibles a terceros que presten sus servicios al Hospital El Escorial, debido al riesgo que conlleva el acceso de terceros a su información.

El Hospital El Escorial se reserva el derecho a realizar auditorías periódicas cuyo objetivo es la verificación del cumplimiento de toda aquella medida de seguridad adicional que no ha sido recogida en la presente normativa e incluida en las cláusulas particulares de los contratos suscritos con terceros.

Adicionalmente, los análisis de riesgos periódicos realizados por el Hospital El Escorial, recogerán las amenazas detectadas en servicios prestados por terceros.

2.1. Medidas de Seguridad con respecto a TERCEROS

- La empresa adjudicataria deberá cumplir las especificaciones y los requerimientos técnicos establecidos por la metodología de trabajo del Servicio de Informática del Hospital Universitario El Escorial (en adelante HESC).
- En cumplimiento con lo dispuesto en el artículo 99.4 de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, y el artículo 18 del Real Decreto 311/2022 de 3 de Mayo por el que se regula el Esquema Nacional de Seguridad, el licitador incluirá referencia precisa, documentada y acreditativa de que los productos de seguridad, equipos, sistemas, aplicaciones o sus componentes, han sido previamente certificados por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información. En el caso de que no exista la certificación indicada en el párrafo anterior, o esté en proceso, se incluirá, igualmente, referencia precisa, documentada y acreditativa de que son los más idóneos, debiendo estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad

Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad (ENS) en el que se establece la política de seguridad en la utilización de medios electrónicos y se aplica a todo el sector público y a sus proveedores tecnológicos del sector privado. Dicha adecuación al cumplimiento del ENS, "es obligatoria para los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas"

Cuando los operadores del sector privado presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad,

cuando se trate de sistemas de categorías MEDIA o ALTA, utilizando los mismos procedimientos que los exigidos en esta Instrucción Técnica de Seguridad para las entidades públicas". Por lo tanto, las empresas privadas que prestan servicios a entidades públicas también deben cumplir los requerimientos del Esquema Nacional de Seguridad según el tipo de servicio e información que manejen.

- Necesidad de que todos los contratos firmados con las entidades que prestarán servicios para el Hospital El Escorial deberán recoger en su clausulado la obligación de confidencialidad en el marco de la relación contractual.
- Los usuarios de terceras empresas prestando servicios para el Hospital El Escorial deberán tener conocimiento de la Normativa de Buenas Prácticas para Terceros del Hospital El Escorial, así como firmar el correspondiente Acuerdo de Confidencialidad contenido en la normativa interna sobre el Acuerdo de Confidencialidad con Terceros.
- Las empresas prestando servicios para el Hospital El Escorial que requieran de acceso a sus sistemas de información deberán seguir las directrices establecidas en el Procedimiento de Gestión y Configuración de Redes del Hospital El Escorial.
- El personal de terceros prestando servicios para el Hospital El Escorial en sus dependencias deberá seguir las directrices establecidas en la Normativa General de Utilización de los Recursos y Sistemas de Información correspondiente del Hospital El Escorial, entre las que se encuentran las siguientes normas generales:
 - Es responsabilidad de los usuarios leer, entender y actuar según las normas de seguridad desde el momento de la entrega de los recursos por el Hospital El Escorial.
 - Los usuarios deben proteger y utilizar los recursos y las herramientas asignadas de manera responsable, y siempre teniendo presente los objetivos profesionales fijados.
 - En cuanto a las credenciales de acceso a los sistemas, cada empleado accederá mediante una tarjeta electrónica, identificación biométrica o bien acreditándose a través de usuario y contraseña. Sea cual sea el mecanismo de acceso, éste tiene carácter personal e intransferible, no pudiéndose ceder a ningún otro usuario.
 - El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel ni dejarla en sitios donde pueda ser fácilmente accesible.

- Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarse inmediatamente.
- Está prohibido el uso de contraseñas acordadas para uso de un grupo de personas como medio para facilitar el acceso a archivos, aplicaciones, bases de datos, ordenadores, redes, y otros recursos del sistema, salvo que se justifique y sea autorizado expresamente.
- La manipulación de la información confidencial, mediante cualquier medio, debe ser efectuada con gran precaución con el fin de evitar que sea divulgada. En el caso de documentación con datos de carácter personal, mientras ésta no se encuentre archivada en un dispositivo de almacenamiento, la persona que esté manipulándola deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.
- Siempre que se disponga de autorización para destruir información en soporte papel, CD o DVD, u otro soporte, se deberán emplear las destructoras de documentos existentes para tal fin o desechar la documentación en los contenedores de documentos confidenciales.
- Toda información necesaria para el correcto funcionamiento de las actividades del Hospital El Escorial deberá estar almacenada en las ubicaciones autorizadas por este, y sujeta a la política de copias de seguridad y restauración correspondiente. En ningún caso podrá ser almacenada localmente en los equipos informáticos puestos a disposición del personal, o en caso de su almacenamiento local deberá encontrarse cifrada.
- No se permite almacenar ni tratar información corporativa en ordenadores particulares, ni dispositivos de almacenamiento particulares.
- El uso de los sistemas de información, puestos a disposición de los usuarios y de terceras partes, es exclusivamente para fines profesionales.
- Cualquier acción de la que pudiera tener conocimiento un usuario y que pudiera constituir un riesgo potencial para los sistemas de información y seguridad del Hospital El Escorial o la CSCM (infección de virus, pérdida o corrupción de la información, robo de equipo, uso indebido de una cuenta de usuario, acceso no autorizado a información, correos electrónicos o información con contenido ofensivo, etc.), se comunicará inmediatamente al Responsable de Seguridad de la Información para que se adopten las medidas oportunas.

- El personal tomará las medidas necesarias para evitar que información confidencial del Hospital El Escorial pueda ser interceptada por terceros. Existen diferentes situaciones en las que esto podría ocurrir, como son:
 - ✓ Interceptación de la información por las personas que se encuentran a nuestro alrededor, especialmente cuando utilizamos la telefonía móvil u otros mecanismos de comunicación actuales.
 - ✓ Intervención de teléfonos y/o utilización de otras formas de escucha no autorizadas a través del acceso físico al teléfono o a la línea telefónica, o el uso de dispositivos receptores.
 - ✓ Grabación de mensajes en contestadores automáticos.
 - ✓ Y, en general, el mantenimiento de conversaciones confidenciales en lugares públicos u oficinas o salas de reuniones abiertas o sin las suficientes medidas que garanticen la imposibilidad de escucha por personas no autorizadas.
- Los sistemas de información no podrán ser usados para la comisión de acciones contrarias a los objetivos de los servicios prestados o la legislación vigente.
- Está prohibida favorecer la descarga e instalación de programas maliciosos (virus, troyanos, gusanos, generadores de spam, etc.), que puedan causar incidentes de seguridad o interrumpir la continuidad de los servicios, así como la descarga e instalación de programas que no hayan sido autorizados por el responsable de la Unidad.
- No está permitido eludir la autenticación del usuario o la seguridad de cualquier sistema, revelar la identificación personal de acceso, permitir el uso de la cuenta a otros usuarios, aunque sean de la misma empresa y/o Unidad o suplantar la personalidad de otro usuario accediendo o haciendo uso de los recursos informáticos.
- No se podrán hacer cambios sin autorización en la configuración estándar de los sistemas, tanto de hardware como de software. Cualquier cambio en la configuración estándar que se considere necesario para el desempeño de la función deberá ser autorizado.
- No está permitido ejecutar cualquier forma de análisis o monitorización de la red o equipos, que intercepten datos, a menos que sean parte de las actividades corporativas autorizadas.

- El Hospital El Escorial podrá exigir, en aplicación del clausulado de los contratos de prestación de servicios firmados con terceros, cualesquiera evidencias de cumplimiento de la legislación y/o normativa vigente.
- El personal de terceros prestando servicios para el Hospital El Escorial será informado y concienciado en buenas prácticas, uso responsable de los sistemas de intercambio de información y en los mecanismos existentes en el Hospital El Escorial para la apertura de incidencias de seguridad relacionadas con dichos sistemas.
- Las medidas de seguridad anteriormente descritas, son las medidas que conforman la base normativa que regirá la relación con terceros que presten servicios para el Hospital El Escorial, pudiéndose completar con medidas más restrictivas para el caso en que los servicios así lo requieran.

2.2 Retirada de material por TERCEROS

Será necesaria notificación al departamento de informática y la autorización previa por parte del Comité de Seguridad, para todo desplazamiento de activos hardware, software o información fuera de las instalaciones del Hospital El Escorial.

Esta autorización será solicitada a través del gestor de incidencias del Hospital El Escorial, y toda salida deberá ser consignada en un registro de salida de material, del que se presenta un modelo en el apartado ANEXO I de la presente Normativa.

El registro de salida de material se almacenará en el gestor documental del Hospital El Escorial y se comprobará periódicamente para garantizar el retorno de los activos, especialmente a la finalización de la relación contractual con terceros prestando servicios para el Hospital El Escorial.

2.3 Intercambio de Información

El Hospital El Escorial intercambiará información en el ámbito de la prestación de servicios por parte de terceros, a través de los canales debidamente configurados, protegidos y controlados, que el Hospital El Escorial determine para cada proyecto.

Excepcionalmente, podrá considerarse conveniente por motivos de confidencialidad y especial trascendencia, aplicar medidas de seguridad adicionales sobre la información recogida en el registro de intercambio de información que se encuentra disponible a través del gestor documental del Hospital El Escorial.

2.4 Accesos Remotos

En el caso de que el Hospital El Escorial disponga de un servicio de acceso remoto a la información (VPN) que permita desarrollar su actividad profesional y conectarse a distintos servicios en un entorno seguro desde cualquier ordenador conectado a Internet, el usuario deberá custodiar diligentemente su dispositivo electrónico y/o usuario y contraseña con el fin de garantizar la seguridad de la información accesible.

2.5 Uso de Acceso a Internet

- Cada empresa de servicios deberá facilitar el acceso a Internet para los empleados que desempeñen su labor en el Hospital El Escorial.

En el caso de que sea el Hospital El Escorial quien provea de este servicio a la empresa externa y a sus empleados se aplicarán las mismas normas que para personal interno de la CSCM.

- El Hospital El Escorial podrá registrar las actividades y los accesos a Internet de los empleados y personal externo a quienes se facilite este servicio, incluyendo las páginas o recursos visitados, para garantizar el cumplimiento de la política y normativa de seguridad, así como de la legislación vigente.
- El acceso a Internet será concedido según las necesidades y usos de los empleados, y en cualquier momento podrá ser retirado si el responsable de un empleado lo considerase oportuno.
- Los empleados no depositarán material del Hospital El Escorial (software, comunicados internos, notas de prensa, bases de datos, etc.) en ningún sistema informático de acceso público como Internet, a menos que tal acción haya sido previamente aprobada por un Responsable de Unidad.
- Los usuarios son los únicos responsables de las sesiones iniciadas en la red Internet desde

sus terminales de trabajo. El acceso a Internet no debe ser utilizado con fines distintos a los relativos a su desempeño laboral.

- En ningún caso se pueden modificar las configuraciones de los navegadores (opciones de Internet) del equipo ni la activación de servidores o puertos sin previa autorización del Responsable de Seguridad de la Información.
- Se prohíbe expresamente el acceso, la descarga y/o el almacenamiento en cualquier soporte desde Internet, de páginas o contenidos ilegales, inadecuados o que atenten contra la moral y las buenas costumbres.
- Los ordenadores portátiles y móviles, y medios móviles utilizados por el personal fuera de las instalaciones, no deben prestarse a nadie que no pertenezca al Hospital El Escorial, permaneciendo siempre bajo custodia del empleado responsable, una vez haya sido autorizada su salida y anotada en el registro correspondiente.
- El equipamiento informático usado para trabajar a distancia debe ser autorizado por un Responsable de Unidad, y éste deberá ser compatible con los sistemas de información y los controles de seguridad establecidos.

2.6 Supervisión y Revisión de Acuerdos

El Hospital El Escorial podrá requerir la firma de Acuerdos de Nivel de Servicio (SLA), para aquellos servicios que presenten especiales condicionantes en cuanto a confidencialidad, disponibilidad, integridad, autenticidad o trazabilidad de la información manejada o los servicios prestados. Dichos acuerdos serán supervisados y auditados de manera periódica para garantizar el adecuado cumplimiento de las condiciones contractuales pactadas.

El Hospital El Escorial se reserva el derecho de realizar un seguimiento de los servicios contratados mediante las correspondientes auditorías, con objeto de verificar el cumplimiento de los acuerdos firmados. Este derecho se plasmará tanto en los pliegos de las licitaciones como en los contratos firmados con terceros.

2.7 Uso del Correo Electrónico

El personal externo deberá utilizar una cuenta de correo electrónico facilitada por el Hospital El

Escorial, bajo las mismas condiciones establecidas en la "Normativa General sobre la utilización los Recursos y Sistemas de Información", así como en lo dispuesto en la "Normativa General de Buenas Prácticas".

2.8 Funciones y obligaciones en materia de LOPD

Cada una de las personas con acceso a información de carácter personal tiene las siguientes funciones y obligaciones:

- Asumir la responsabilidad del puesto de trabajo asignado, garantizando la confidencialidad e integridad de la información a la que tienen acceso.
- Cumplir con todas las obligaciones que se deriven del presente documento y con los procedimientos que se detallan en el mismo.
- Garantizar la confidencialidad de las contraseñas que le fueran asignadas.
- Utilizar y gestionar los soportes y la información con la diligencia debida y atendiendo en todo caso al tratamiento de la información autorizado.
- Comunicar al Responsable de Seguridad correspondiente cualquier incidencia de la que tenga conocimiento.
- Colaborar con el Hospital El Escorial en todo lo necesario para facilitar el cumplimiento de lo establecido en la legislación vigente en materia de protección de datos.

El personal externo que preste sus servicios para el Hospital El Escorial está obligado a cumplir todas las medidas de seguridad establecida, así como los requisitos y condiciones que se deban aplicar de acuerdo a las normas y procedimientos existentes y con los controles de seguridad que se encuentren establecidos, haciendo uso de la información a la que tengan acceso sólo para los fines relacionados con el desarrollo de sus competencias y para la realización exclusiva de su trabajo y funciones. Los usuarios podrán ser responsables del incumplimiento de sus obligaciones de conformidad con el régimen jurídico aplicable.

2.9. Comunicación de incidencias, deficiencias y mejoras

El personal es la parte clave para la gestión eficaz de los incidentes, ya que en numerosas ocasiones son los que detectan las anomalías de los sistemas en el trato diario con los mismos.

La comunicación temprana es vital para disminuir los impactos posibles de un incidente, por ello

es vital concienciar, formar y entrenar a los usuarios de que son parte activa en la aplicación de las medidas de seguridad. Todo usuario debe comunicar cualquier incidente detectado a través de los medios puestos a su disposición, siguiendo el procedimiento para comunicar los incidentes.

Una vez que los usuarios, tanto internos como externos se percatan de algún incidente que pueda afectar a la seguridad de la información, procederá a comunicarlo, en el menor tiempo posible, a través del Servicio de Soporte que corresponda. Deben comunicarse todos los detalles observados que hayan llevado al usuario a sospecha, prestando asimismo la colaboración que pueda ser precisa al Servicio de Soporte para la resolución de la incidencia.

Así mismo, los usuarios deberán comunicar al Servicio de Informática que corresponda, cualquier incidencia de funcionamiento o deficiencia de las aplicaciones informáticas que hubieran podido observar, así como cualquier mejora que se estime adecuada.

2.10. Accesos a carpetas/recursos de red

El Hospital El Escorial facilitará al personal externo accesos a sus recursos de red, únicamente si es necesario para el desempeño de su labor, y siempre y cuando éste acceso sea solicitado por el Responsable de Unidad del Hospital El Escorial.

Para todas las carpetas de los proyectos de las Unidades que forman parte del Hospital El Escorial, será el Responsable de Unidad el que decida y solicite sobre dichos accesos.

2.11. Instalación y uso del Software

El Hospital El Escorial cederá a las Empresas de Servicios el uso temporal de las licencias de software que el Hospital El Escorial considere necesario para el desempeño de las actividades del personal externo en el ámbito del contrato firmado.

El Responsable de Unidad será el encargado de facilitar los accesos a las aplicaciones de su responsabilidad y deberá llevar un registro de las licencias instaladas o "prestadas" a las Empresas de Servicios.

Los usuarios no podrán modificar el software instalado a nivel corporativo, que en ningún caso deberá ser desactivado.

La instalación de "software" o programas en los ordenadores, cuando el trabajador externo lo

considere necesario, deberá solicitarse al responsable correspondiente para que lo gestione, no estando permitido que el usuario proceda a la instalación de ningún "software" sin tener previamente la debida autorización. De igual manera, se encuentra prohibida la realización de copias del "software" instalado en los ordenadores.

2.12. Gestión de Usuarios (altas, bajas y modificaciones)

El alta, baja y modificación de usuarios en los sistemas del Hospital El Escorial deberá ser solicitado a través de los Responsables de Unidad del Hospital El Escorial.

Los sistemas de información provistos por el Hospital El Escorial son accesibles para el personal externo que preste sus servicios en éste exclusivamente mientras se mantenga vigente su relación o vinculación con la misma.

Por otro lado, cuando un empleado de una Empresa de Servicios deje de trabajar en el Hospital El Escorial, el empleado dejará de tener acceso a los sistemas de información del Hospital El Escorial, y a los datos en ellos contenidos, debiendo devolver al Hospital El Escorial cualesquiera soportes que obren en su poder y que contengan datos a los que hayan tenido acceso en el marco de su vinculación o relación con el Hospital El Escorial.

Será el responsable de su empresa en el Hospital El Escorial quien deberá comunicarlo inmediatamente para proceder a dar de baja los usuarios de dicho empleado en los sistemas del Hospital El Escorial.

2.12. NORMAS GENERALES APLICABLES A LA EMPRESA DE SERVICIOS

Cuando una empresa es contratada para que preste un servicio en el Hospital El Escorial, y que vaya a incorporar personal y equipamiento de usuario, deberá asegurar en el contrato que cumple las siguientes medidas de seguridad:

- Todos los equipos disponen de agente antivirus, y éste es actualizado diariamente, según la distribución de firmas de cada fabricante.
- Todos los equipos disponen de una solución de cifrado de disco duro.
- Todos los equipos disponen de una solución anti malware y anti rootkit.
- Todos los equipos disponen de una solución de destrucción de datos.
- Los equipos llevarán instalado exclusivamente el software necesario para la prestación del servicio contratado.

- Los equipos han sido actualizados con los últimos parches de seguridad, y están configurados para que sean actualizados periódicamente, bien de manera automática o manual.
- En cualquier caso, la responsabilidad de mantener los equipos actualizados será de la Empresa de Servicios.
- La Empresa de Servicios garantiza el cumplimiento de la legislación de propiedad intelectual, y certifica que todo el software empleado en los equipos es legal, y dispone de su correspondiente licencia.
- La Empresa de Servicios autoriza a que el Hospital El Escorial, pueda realizar las auditorías de seguridad que considere necesarias, entre ellas:
 - ✓ Análisis de Vulnerabilidades en los equipos.
 - ✓ Auditoría de los términos indicados en la presente Política de Seguridad y en el contrato de prestación de servicios.
- La Empresa de Servicios garantiza que el método de autenticación al sistema, cuando sea responsabilidad de la propia Empresa de Servicios, cumplirá la Política de Seguridad respecto al Control de Accesos a los Sistemas de Información establecida por el Hospital El Escorial.
- La Empresa de Servicios garantiza que la ubicación física de los equipos de tratamiento de la información, cuando sea responsabilidad de ésta, estará dotada de un mecanismo de identificación y control de acceso, donde existe un listado del personal autorizado, y un registro de entrada cuando se produzca un acceso fuera del horario acordado para el servicio.
- Cuando sea responsabilidad de ésta y se considere necesario, la Empresa de Servicios pondrá a disposición de todo su personal, destructoras de CDs, DVDs y papel, de tal forma que toda la información del Hospital El Escorial, que no vaya ser utilizada sea destruida, y en ningún caso utilizado como papel reciclado.
- Todo documento con información relevante para el Hospital El Escorial, debe ser destruida cuando esta no vaya a ser utilizada, pudiendo llevar dicha documentación a contenedores de información confidencial si no hubiese destructora de papel.

2.13. Cumplimiento del presente Código

Todo el personal externo que preste sus servicios para el Hospital El Escorial deberá cumplir la presente norma de Buenas Prácticas. El incumplimiento de cualquiera de las pautas de comportamiento contenidas en el presente Código podrá dar lugar a la correspondiente responsabilidad disciplinaria, si a ello hubiere lugar en aplicación de las normas reguladoras del régimen jurídico propio del usuario.

3. ANEXOS

❖ ANEXO I

Modelo de registro de salida de material.

Fecha	Empresa	Nombre empleado	Firma	Tipo	Descripción	Comentarios
dd/mm/aaaa						

❖ ANEXO II

Modelo de registro de intercambio de información

Información	Área funcional	Entidad de Intercambio	Medida Adicional