Información de protección de datos a empleados

De conformidad con la normativa vigente de protección de datos (Reglamento UE 2016/679 y L.O. 3/2018) le facilitamos la siguiente información sobre el tratamiento de datos:

Responsable del tratamiento: Entidad empleadora (sociedad que figura en su contrato laboral) de HM HOSPITALES que corresponda.

Legitimación y finalidades del tratamiento:

Art. 6.1.b). Ejecución de un contrato en el que el interesado es parte.

- **Gestión de la relación laboral y de recursos humanos:** alta y baja con Seguridad Social, proceso "on boarding" del contratado, alta y baja con la Seguridad Social, contratación, gestión de permisos y/o vacaciones, etc.
- **Portal de empleado (Chris):** mediante la identificación de usuario y clave individual personalizada se le permitirá acceso a un área privada individual dónde podrá actualizar sus datos de carácter personal (dirección postal, teléfono, cuentas bancarias, etc.) y realizar gestiones como descargar nóminas, obtener certificados de retenciones… y realizar gestiones vinculadas a su relación laboral. Asimismo, pondremos a su disposición información corporativa sobre nuevas incorporaciones, ascensos, cambios de puestos...
- **Evaluación del desempeño del empleado:** medición de desempeño y talento del empleado.
- **Política de retribución flexible** a través de los diferentes programas que el Responsable ofrece a sus empleados.
- **Plan de carrera y movilidad** de acuerdo a sus metas profesionales.
- **Formación obligatoria a realizar en función del puesto desempeñado.**
- **Directorio:** gestión de herramienta de agenda de personal o tarjetas identificativas con la finalidad de proceder a su correcta identificación. En el caso de que esté insertar voluntariamente su fotografía en su perfil, se considerará una clara acción unívoca (Artículo 6.1. a) consentimiento) para el tratamiento de su imagen a estos únicos efectos de Directorio.
- **Voz del empleado:** recepción de feedback y aportaciones de empleados.

Art. 6.1.c). Cumplimiento de una obligación legal aplicable al responsable del tratamiento.

- **Registro jornada laboral** de acuerdo al artículo 34.9 del Estatuto de los trabajadores.
- **Prevención de Riesgos Laborales**: evaluación de riesgos de puesto de trabajo, adopción de medidas para mitigarlos, adopción de medidas de prevención colectiva, etc.
- **Supervisión del uso de medios digitales facilitados** (teléfonos, portátiles, tablets, etc. para control de las obligaciones laborales y garantizar la integridad de los dispositivos).
- **Gestión de las infracciones que se le notifiquen en materia de tráfico**, en los casos que pueda resultar de aplicación.
- **Gestión de embargos**, en los casos en que pueda verse afectado.
- **Canal de denuncias**: gestión de las denuncias que se pueden presentar ante posibles conductas irregulares o ilícitas. Este sistema se limita a las denuncias relacionadas con hechos o actuaciones que tengan una efectiva implicación en la relación laboral, así como de las leyes o las buenas prácticas empresariales.
- **Planes de igualdad retributiva** conforme el articulo 4 y ss. del RD902/2020, de 13 de octubre, de igualdad retributiva entre mujeres y hombres.
- **Cualquier otra finalidad que encuentre su habilitación en el cumplimiento de las obligaciones legales de la entidad empleadora** con motivo de la entrada en vigor de alguna norma con rango de ley.

Art. 6.1.e). Cumplimiento de una misión realizada en interés público.

- Por motivos de **seguridad de instalaciones, bienes y personas**, se han instalado cámaras de videovigilancia en el interior y exterior de las instalaciones por lo que su imagen podrá ser captada con esa finalidad.

La información solicitada al empleado para cumplimiento de los fines mencionados tiene carácter obligatorio, de tal forma que su ausencia impedirá la relación laboral.

Criterios de conservación:

- Los datos generales de gestión de Recursos Humanos se conservarán mientras se mantenga la relación laboral y, en todo caso, mientras no prescriban las posibles acciones legales derivadas de la finalidad y del tratamiento.
- Los datos de registro diario de jornada se conservarán durante cuatro años.
- Sus datos personales se conservarán en el sistema de denuncias durante el tiempo imprescindible para decidir sobre la pertinencia de iniciar una investigación sobre los hechos

denunciados (hasta 3 meses). Únicamente podrán conservarse por tiempo superior, y de forma anonimizada, si existe finalidad -ponderada y motivada- de dejar en evidencia el correcto funcionamiento del canal. En caso de iniciar investigación, los datos serán conservados una vez concluida la investigación de los hechos denunciados y vencidos los plazos de prescripción de las responsabilidades derivadas de la interposición de las denuncias o de la comisión de posibles infracciones, y como máximo, hasta la tramitación de los procedimientos judiciales que pudieran derivarse de la investigación realizada. Superado el plazo, sus datos serán suprimidos con medidas de seguridad adecuadas para garantizar la anonimización o la destrucción de los mismos. En ningún caso podrán conservarse los datos por un período superior a diez años.

- La información recabada mediante sistemas de videovigilancia será suprimida en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes se pondrán a disposición de la autoridad competente.

Comunicación de los datos:

- Entidades de HM HOSPITALES (www.hmhospitales.com, apartado cesiones de la Política de privacidad) a efectos de gestión administrativa centralizada de RRHH.
- Terceros con los que la Entidad empleadora tenga relación con la finalidad de contacto. Únicamente se cederán sus datos de contacto profesionales.
- Destinatarios por obligación legal o requerimiento judicial.
- Clientes y potenciales clientes en las ofertas presentadas con el fin de identificar el equipo técnico que participará en el desarrollo de los proyectos, la acreditación del cumplimiento de las obligaciones en el ámbito de la normativa laboral o de Seguridad Social de la Empresa y la coordinación de actividades empresariales.
- Administraciones Públicas en el caso de participar en concursos públicos que requieran la comunicación de sus datos en los documentos contractuales que regulen la relación.
- Empresas de formación para la impartición de cursos y empresas gestoras de la misma.
- Compañías aseguradoras, en el caso de suscripción de un seguro de vida y accidentes, con la finalidad de gestionar la contratación del seguro y, en su caso la tramitación de los siniestros.
- Empresas de renting/leasing, en el caso de que le sea asignado un vehículo de Empresa, con la finalidad de identificar al conductor o la gestión de los procedimientos en materia de infracciones de tráfico.

Derechos que asisten al interesado:

Derecho de acceso, rectificación, portabilidad, supresión de sus datos, limitación, oposición al tratamiento y a presentar una reclamación ante la Autoridad de Control (www.aepd.es), si considera que el tratamiento no se ajusta a la normativa vigente.

Datos de contacto:

Solicitud escrita dirigida al Responsable del tratamiento, acompañando documento acreditativo de su identidad, con dirección en la Plaza del Conde del Valle de Suchil 2, 28015 de Madrid o mediante el correo del DPD dpo@hmhospitales.com

Le informamos de que con el fin de mantener exactos y puestos al día los datos relativos a empleados, se obliga a comunicar de forma inmediata al Responsable cualquier modificación que se produzca en sus datos y que podrá realizarlo Ud. mismo a través del Portal del empleado Chris.

Acuerdo de confidencialidad y secreto profesional

El EMPLEADO, en su condición de USUARIO de la información y en el marco de la relación laboral o profesional que le une con LA ENTIDAD EMPLEADORA (sociedad que figura en su contrato laboral), en adelante, el RESPONSABLE o ENTIDAD EMPLEADORA, para el desarrollo de sus funciones en el centro de trabajo donde presta sus servicios, se da por informado y se obliga al cumplimiento del siguiente acuerdo de confidencialidad en relación con el Reglamento (UE), 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos o RGPD por sus siglas) así como de la Ley 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales (LOPD-GDD por sus siglas), y demás normativa aplicable.

1.- Definiciones

Se entenderá por "información confidencial", toda aquella información, oral o escrita, accesible al USUARIO que se transmita al USUARIO con anterioridad o posterioridad a la firma del presente Acuerdo. Incluirá, entre otras, informaciones de carácter científico, técnico, financiero, legal, fiscal y comercial, modelos y estrategias de negocio, "know how", nombres de posibles clientes y socios, proyectos y operaciones de cualquier carácter propuestas o en fase de estudio, informes, planos, proyecciones de mercado y datos, junto con los análisis y documentos, recopilaciones, comparaciones, estudios y en general, toda la información que no sea objeto de conocimiento público.

Asimismo, se entenderá por "datos personales" toda información relativa a una persona física identificada o identificable por la cual pueda determinarse, directa o indirectamente su identidad, sea mediante identificador, nombre, número, localización o elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

La información confidencial antes referida incluye los secretos comerciales establecidos en la Ley 1/2019, de 20 de febrero, de Secretos Empresariales, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados contra su obtención, utilización y revelación ilícitas, abarcando los siguientes tipos de información (conste por escrito o no), sin que la presente enumeración excluya otras clases de informaciones también confidenciales: técnicas, programas de formación, test, investigación y desarrollo, ideas, invenciones, conceptos, anotaciones, esquemas, diseños, dibujos, organigramas, memorandos, procesos, procedimientos, know-how, fórmulas, datos, programas y aplicaciones informáticas, mejoras, descubrimientos, conocimientos de cualquier clase puestos a disposición del USUARIO, materiales de referencia, materiales y técnicas de marketing, planes de investigación y desarrollo, marketing, nuevos productos, nombres de clientes, canales de comercialización, secretos comerciales y cualquier otra información relacionada con clientes y proveedores, listas

de precios, políticas de precios, política de ventas, información financiera, presupuestos, plantillas y métodos de gestión y contabilidad, así como los derechos, títulos e intereses que pudiera alegar sobre las invenciones, patentables o no, realizadas u obtenidas por la persona durante la vigencia de su contrato laboral.

2.- Compromiso de confidencialidad y secreto profesional

El USUARIO se compromete a cumplir con las instrucciones determinadas por la Entidad empleadora que afectan al desarrollo de sus funciones para garantizar la confidencialidad y el secreto profesional de toda la información confidencial, por lo que se obliga explícitamente a no divulgarla, publicarla, cederla, venderla, ni de otra forma, directa o indirecta, ponerla a disposición de terceros, ni total ni parcialmente, y a cumplir esta obligación incluso con sus propios familiares u otros miembros de la Entidad empleadora que no estén autorizados a acceder a dicha información, cualquiera que sea el soporte en el que la contenga.

El USUARIO accederá a la información confidencial solo si es necesario para la prestación de los servicios para los que ha sido contratado y exclusivamente para los fines autorizados por la Entidad Empleadora.

Asimismo, debe tener en cuenta que en el caso de que acceda a los datos de la historia clínica porque fuera necesario en el ejercicio de sus funciones queda sujeto al deber de secreto en virtud del artículo 16.6 de 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, así como cualquier otra normativa que sea de aplicación al personal sanitario y/o correspondiente al puesto a desempeñar.

Los medios proporcionados por la Entidad Empleadora (ordenadores, internet, correo electrónico, etc.) serán utilizados única y exclusivamente para el desarrollo eficiente del propio trabajo, pudiéndose realizar tareas de verificación, vigilancia y control sobre los mismos sin informar expresamente al USUARIO.

3.- Propiedad de la “Información confidencial”

El USUARIO reconoce la propiedad de la Entidad Empleadora respecto de toda la “Información Confidencial” descrita en el apartado 1 de este acuerdo y se compromete a devolver todas las copias de dicha información y cualquier soporte físico que estén bajo su control a la Entidad Empleadora si este lo solicita.

4.- Tratamiento de información y datos personales

El USUARIO declara conocer el **Anexo I.- Funciones y Obligaciones y Anexo II.- Política de seguridad**, y se compromete a seguir las instrucciones en ellas reflejadas.

En caso de percibir que están siendo violadas, a notificarlo sin demora injustificada al RESPONSABLE para su conocimiento y aplicación de medidas correctivas para remediar y mitigar los efectos ocasionados.

5.- Responsabilidad del USUARIO

El USUARIO será responsable frente la Entidad empleadora y terceros de cualquier perjuicio que pudiera derivarse para unos y otros del incumplimiento del presente Contrato, pudiendo suponer el inicio de acciones legales, así como la reclamación de las indemnizaciones, sanciones y daños o perjuicios que la Entidad Empleadora se vea obligado a atender a consecuencia de dicho incumplimiento.

6.- Fin de la relación laboral

El cumplimiento de las obligaciones contenidas en este acuerdo es de carácter indefinido y se mantendrá en vigor con posterioridad a la finalización de la relación entre el USUARIO y la Entidad empleadora.

Por ello, el USUARIO garantiza que, tras terminar la relación, guardará el mismo secreto profesional respecto de la «información confidencial» a que haya tenido acceso durante el desempeño de sus funciones.

ANEXO I: Funciones y obligaciones de los usuarios de HM Hospitales

USUARIOS son todas aquellas personas que ejercen sus funciones bajo la autoridad del RESPONSABLE que intervienen en el tratamiento de cualquier información generada por la Entidad empleadora relativa tanto a datos personales como a los que no lo son. Éstos deberán actuar de acuerdo con las instrucciones contempladas en el Acuerdo de confidencialidad y secreto profesional, obligándose además a cumplir las funciones y obligaciones relacionadas en este documento como Anexo I.

I. Confidencialidad de la información

El Usuario deberá:

1.- Conservar los datos en el mobiliario y departamento destinados a tal fin.

Para tratamientos automatizados se guardarán los archivos en los soportes, carpetas o directorio de red indicados por LA ENTIDAD EMPLEADORA de seguridad.

2.- Almacenar toda la información tratada en el directorio de red correspondiente indicado por LA ENTIDAD EMPLEADORA de seguridad, lo que permitirá que a esta información se le apliquen las medidas de seguridad existentes y que se someta a los procedimientos de copias de seguridad aplicados por la Entidad empleadora.

3.- Disponer los soportes documentales e informáticos de manera que no sean accesibles a personas no autorizadas.

4.- Ocultar los documentos y bloquear el ordenador si se ausenta de su puesto de trabajo temporalmente. De esta forma, se impedirá la visualización de la información con la que estaba trabajando.

5.- Recoger de manera inmediata, o imprimir de forma bloqueada, asegurándose de no dejar documentos impresos en la bandeja de salida.

6.- Destruir documentos físicos o soportes digitales que quieran ser eliminados y que incluyan datos personales mediante destructora o empresa homologada de destrucción de documentos.

7.- Aplicar las medidas establecidas por la Entidad empleadora relativas a la seguridad del tratamiento como pueden ser la seudonimización o cifrado de datos o advertencias de intrusión como antivirus, antispam, etc.

Están **expresamente prohibidas** las siguientes actividades:

1. Enviar al exterior o revelar a terceros, información que no haya sido declarada como no confidencial por el RESPONSABLE, mediante cualquier procedimiento o soporte, sea electrónico, digital, manual o documental, o a través de cualquier medio de comunicación, incluyendo la simple visualización o acceso a la misma.
2. El uso de cámaras fotográficas, de vídeo, de sonido o cualquier instrumento que pueda almacenar información audiovisual, entendida esta no solo de personas, si no de cualquier lugar, soporte o recurso del RESPONSABLE.
3. Divulgar directamente ni a través de terceras personas o empresas los datos, documentos, metodologías, claves, análisis, programas y demás información a la que tengan acceso durante su relación laboral con la Entidad empleadora, tanto en soporte material como electrónico. Esta prohibición continuará vigente tras la extinción del contrato laboral por tiempo indefinido.
4. Poseer, para usos fuera de su responsabilidad, ningún material o información propiedad del RESPONSABLE o del cliente del mismo donde se presten los servicios, tanto ahora como en el futuro.

En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el USUARIO entre en posesión de información que no haya sido declarada como no confidencial por parte del RESPONSABLE, bajo cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le irrogue derecho alguno de posesión, o titularidad o copia sobre la referida información.

Asimismo, el USUARIO deberá devolver dichos materiales al RESPONSABLE inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos, y, en cualquier caso, a la finalización de la relación laboral. La utilización continuada de la información en cualquier formato o soporte de forma distinta a la pactada y sin conocimiento del RESPONSABLE, no supondrá, en ningún caso, una modificación de esta cláusula.

El incumplimiento de estas obligaciones puede constituir un delito de revelación de secretos, previsto en los artículos 197 y 278 del Código Penal y dará derecho al RESPONSABLE a proceder como estime oportuno en defensa de sus intereses y a exigir al USUARIO una indemnización económica.

El incumplimiento de estas obligaciones puede constituir un delito de revelación de secretos, previsto en los artículos 197 y 278 del Código Penal y dará derecho al RESPONSABLE a proceder como estime oportuno en defensa de sus intereses y a exigir al USUARIO una indemnización económica.

5.- Conservar datos en el escritorio físico o digital. Solo se permite su tratamiento temporal en dicho escritorio para realizar las operaciones que lo precisen debiendo conservarse en el lugar apropiado al término de la jornada.

6.- Llevar a cabo el transporte de soportes que contengan datos personales únicamente si ha sido designado como personal autorizado.

II. Utilización de los sistemas informáticos (SI)

El Sistema Informático, y los terminales utilizados por cada USUARIO son, con carácter general, propiedad del RESPONSABLE o de un cliente del mismo.

Están **expresamente prohibidas** las siguientes actividades:

1. El uso de programas informáticos sin la correspondiente licencia, así como el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual o industrial. Su incumplimiento podrá ser causa de responsabilidad disciplinaria, administrativa, civil y penal.
2. Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos del RESPONSABLE o de terceros. Estos actos pueden constituir un delito de daños, previsto en el artículo 264.2 del Código Penal.
3. Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en los Sistemas Informáticos del RESPONSABLE o de terceros. Al respecto, recordar que el propio sistema ejecuta automáticamente los programas antivirus y sus actualizaciones para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos informáticos.
4. Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por el RESPONSABLE. Esta prohibición incluye cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización para ello.
5. Instalar copias ilegales de cualquier programa, incluidos los que están estandarizados.
6. Borrar cualquiera de los programas instalados legalmente.
7. Introducir contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos del RESPONSABLE.
8. Cifrar información sin estar expresamente autorizado para ello.

III. Salvaguarda y protección de las contraseñas personales

Están **expresamente prohibidas** las siguientes actividades:

1. Compartir o facilitar el identificador de usuario y la clave de acceso (contraseña) facilitado por el RESPONSABLE a otra persona física o jurídica. Si el USUARIO sospecha que otra persona conoce sus datos de identificación y acceso deberá notificar al Responsable de seguridad de esta incidencia para activar los mecanismos de cambio de contraseña. En caso de incumplimiento de esta prohibición, el USUARIO será el único responsable de los actos realizados por la persona física o jurídica que utilice de forma no autorizada su identificación.
2. Intentar distorsionar o falsear los registros log del sistema.
3. Intentar aumentar o disminuir el nivel de privilegios de un USUARIO en el sistema.

IV. Acceso a redes

Están **expresamente prohibidas** las siguientes actividades:

1. Utilizar los datos, la red corporativa y/o la intranet del RESPONSABLE y/o de terceros para incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de la Entidad empleadora y/o de terceros o que puedan atentar contra la moral o las normas de etiqueta de las redes telemáticas.
2. Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos del RESPONSABLE.
3. Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos del RESPONSABLE y/o de terceros.
4. Almacenar datos de carácter personal en el disco duro del ordenador, debiendo ser utilizadas para tal fin las carpetas de la red corporativa asignadas por el RESPONSABLE.
5. Obstaculizar voluntariamente el acceso de otros USUARIOS a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la Entidad empleadora, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas.

V. Recursos telemáticos y acceso a Internet

El RESPONSABLE se reserva el derecho de monitorizar y comprobar, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada por un USUARIO.

Cualquier fichero introducido en los SI desde Internet, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual y a control de virus.

Están **expresamente prohibidas** las siguientes actividades:

1. Utilizar los recursos telemáticos del RESPONSABLE y/o acceder a redes públicas como

Internet, páginas web (www), grupos de noticias (Newsgroups) y otras fuentes de información como FTP, etc. para temas no relacionados directamente con la actividad del RESPONSABLE o los cometidos del puesto de trabajo del USUARIO.

2. El acceso a debates en tiempo real (Chat/IRC), ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema.

VI. Utilización del correo electrónico y mensajería

Se considerará correo electrónico tanto el interno como el externo, dirigido o proveniente de otras redes privadas o públicas, especialmente Internet.

Ningún mensaje de correo electrónico será considerado como privado.

El RESPONSABLE se reserva el derecho de revisar, sin previo aviso, los mensajes de correo electrónico de los USUARIOS de la red corporativa y los archivos log del SI, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar a la Entidad empleadora como responsable civil subsidiario.

Cualquier fichero introducido en los SI a través de mensajes de correo electrónico, provenientes de redes externas, deberá cumplir los requisitos establecidos en estas normas o además de las del cliente, en especial, las referidas a propiedad intelectual e industrial y a control de virus.

Las direcciones de correo electrónico dirigidas a personas son consideradas datos personales, por lo que cuando se envíen correos a más de un destinatario, si no es estrictamente necesario que los otros vean las direcciones de correo de todos los demás, se deberán enviar como copia oculta "Cco".

Están **expresamente prohibidas** las siguientes actividades:

1. Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros USUARIOS. Esta actividad puede constituir un delito de interceptación de las telecomunicaciones (revelación de secretos), previsto en el artículo 197 del Código Penal.
2. Enviar mensajes de correo electrónico de forma masiva o con fines comerciales o publicitarios sin el consentimiento del destinatario.
3. Enviar o reenviar mensajes en cadena o de tipo piramidal.

VII. Tratamiento de la información

Están **expresamente prohibidas** las siguientes actividades:

1. Acceder a recursos que no sean necesarios para el desarrollo y cumplimiento de su labor, así como consultar, copiar, reproducir, transmitir, editar, modificar o eliminar información sin estar autorizado para estas funciones.

2. Utilizar impresoras o fotocopiadoras sin recoger de manera inmediata los documentos impresos en la bandeja de salida con el fin que otras personas no autorizadas puedan acceder a la información.
3. Destruir cualquier documento físico o soporte digital que incluya datos personales sin utilizar la destructora de papel o sin guardarlos debidamente custodiados hasta que sean retirados por una empresa homologada de destrucción de documentos.
4. Dejar la pantalla del ordenador sin bloquear cuando se abandona el puesto de trabajo temporalmente, de modo que se impida la visualización de la información a personas no autorizadas.

VIII. Gestión de incidencias

Es obligación del USUARIO, comunicar al RESPONSABLE en el menor plazo posible, todas aquellas incidencias que se produzcan en la Entidad empleadora, entendidas éstas como, cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos personales o al incumplimiento de las obligaciones detalladas en este documento.

Dicha comunicación deberá contener la identificación clara de la incidencia y una descripción detallada de la misma; que contendrá, como mínimo: el momento –día y hora- que se ha producido, la persona que ha tenido conocimiento de ella, las personas a la que se ha comunicado, los efectos producidos y las medidas correctoras adoptadas.

El conocimiento y no notificación de una incidencia por parte del personal se considerará una falta contra la seguridad de los datos y podrá suponer el inicio de acciones legales, así como la reclamación de las indemnizaciones, sanciones y daños o perjuicios que LA ENTIDAD EMPLEADORA se vea obligado a atender a consecuencia de dicho incumplimiento.

ANEXO II: Política de seguridad del personal para el tratamiento de datos personales

1. Ámbito de aplicación

El Responsable del tratamiento está comprometido en implantar una cultura de privacidad en la Entidad empleadora por lo que necesita que las personas autorizadas a tratar datos personales estén informadas del tratamiento de datos y se responsabilicen del mismo.

A toda persona autorizada para tratar datos personales se le exige que lea, comprenda, cumpla y haga cumplir esta Política de seguridad para proteger los datos que forman parte del tratamiento que le ha sido encomendado.

Esta Política de seguridad establece las obligaciones y procedimientos a seguir por el personal de la Entidad empleadora, tanto propio como externo, que trata datos personales en el desarrollo de su actividad y se basa en lo dispuesto en las normativas vigentes en protección de datos personales, el Reglamento (UE) 2016/679 de 27 de abril de 2016 (GDPR) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDPGDD).

En este sentido, para velar y hacer cumplir esta Política, la Entidad empleadora ha designado un Responsable de seguridad que estará a disposición de todo el personal y se encargará de coordinar, controlar, desarrollar y verificar el cumplimiento de las citadas normativas.

2. Conceptos básicos

Para proporcionar una mejor comprensión de la protección de datos, definimos los principales conceptos básicos:

Estructura del tratamiento:

- **Datos personales**: Información relativa a una persona física por la cual pueda determinarse su identidad.
- **Tratamiento**: Cualquier operación realizada sobre datos personales: obtención, acceso, intervención, transmisión, conservación y supresión.
- **Interesado**: Persona física sometida al tratamiento de sus datos personales.
- **Fichero**: Conjunto estructurado de datos personales susceptibles de tratamiento para un fin determinado.

- **Responsable del tratamiento**: Entidad empleadora que determina los fines y los medios del tratamiento.
- **Personal autorizado**: Persona autorizada por el Responsable para realizar un tratamiento de datos mediante un compromiso de confidencialidad.

Categorías de datos (nivel de seguridad):

- **Identificativos (nivel Básico)**: Datos que no correspondan a categorías Penales o Especiales, por ejemplo: nombre, dirección, email, teléfono, edad, sexo, firma, imagen, aficiones, patrimonio, datos bancarios, información académica, profesional, social, comercial, financiera, etc.
- **Penales (nivel Medio)**: Datos relativos a la comisión de infracciones administrativas o penales, o los que puedan ofrecer una definición de características de personalidad, etc.
- **Especiales (nivel Alto)**: Datos relativos al origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, afiliación sindical, datos genéticos o biométricos que permitan la identificación unívoca de una persona, datos relativos a la salud o a la vida y orientación sexuales.

3. Principios de la protección de datos

Los principios fundamentales para realizar un tratamiento de datos son:

- **Licitud**: lealtad y transparencia con el interesado.
- **Limitación de los fines**: tratados para fines determinados.
- **Minimización de los datos**: solo se deben obtener los datos necesarios para alcanzar los fines.
- **Exactitud**: actualizados.
- **Limitación del plazo de conservación**: guardados durante no más tiempo del necesario para conseguir los fines.
- **Integridad y confidencialidad**: aplicación de medidas de seguridad para la protección de los datos en todas las fases del tratamiento.
- **Responsabilidad proactiva**: se debe poder demostrar el cumplimiento.

Consentimiento para realizar un tratamiento de datos

- Para tratar datos deberemos obtener el consentimiento explícito del interesado y guardar el documento probatorio que lo acredite.
- Cuando obtengamos los datos de terceros, deberemos asegurarnos que la comunicación es lícita y guardar el documento probatorio que lo acredite.
- No es necesario obtener el consentimiento del interesado cuando el tratamiento se base en una obligación legal (por ejemplo, emitir una factura).

Información del tratamiento al interesado

Deberemos facilitar la siguiente información al interesado:

- La identidad y los datos de contacto del Responsable del tratamiento
- Los fines del tratamiento.
- La base jurídica del tratamiento.
- El plazo de conservación o los criterios que lo determinen.
- Los derechos que asisten al interesado.
- Y si existen:
    - Los destinatarios o categorías de destinatarios de los datos.
    - La transmisión de datos a países u organizaciones establecidas fuera de la UE.

Responsabilidad del tratamiento

El tratamiento de datos se podrá realizar por organizaciones externas siempre y cuando exista una autorización expresa del Responsable y se haya suscrito un contrato para realizar dicho tratamiento conforme a la legislación vigente. Para ñ qué empresas o terceros están autorizados a la cesión de datos, deben dirigirse al Responsable de seguridad.

Las organizaciones externas pueden ser:

- **Encargados del tratamiento**: Entidad empleadora que trata datos personales por cuenta del Responsable.
- **Destinatarios de datos**: Entidad empleadora distinta del Encargado, que recibe una comunicación de datos del Responsable.

Medidas de seguridad

La Entidad empleadora ha implementado medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado a los riesgos que pueda tener el tratamiento como consecuencia de la destrucción accidental o ilícita de datos, la pérdida, alteración o comunicación no autorizada y el acceso a los datos cuando son transmitidos, conservados u objeto de algún otro tipo de tratamiento.

El personal deberá velar por la seguridad de los datos tratados por la Entidad empleadora y comunicará al Responsable cualquier operación de tratamiento que pueda suponer un riesgo que afecte la protección de datos o los intereses y libertades de los interesados.

Cualquier diseño de una nueva operación de tratamiento o actualización de una operación existente deberá garantizar antes de su implantación, la protección de datos personales y el ejercicio de los derechos de los interesados en todas las fases del tratamiento: obtención, acceso, intervención, transmisión, conservación y supresión.

4. Funciones y obligaciones del personal

El personal deberá actuar en todo momento conforme las instrucciones detalladas en el acuerdo de confidencialidad suscrito con la Entidad empleadora y las establecidas en esta Política de seguridad. Para ello se establecen las siguientes medidas de protección de datos que el personal se obliga a cumplir expresamente:

Entidad empleadora de la información

Se deberán clasificar los datos de manera que se puedan ejercer los derechos de los interesados: acceso, rectificación y supresión de los datos y limitación u oposición al tratamiento.

Conservación de los datos

Se deberán conservar los datos en el mobiliario y departamento destinados a tal fin. Para tratamientos automatizados se guardarán los archivos en los soportes, carpetas o directorio de red indicados por el Responsable de seguridad.

No está permitido conservar datos en el escritorio físico o digital. Solo se permite su tratamiento temporal en dicho escritorio para realizar las operaciones que lo precisen debiendo ser conservados en el lugar apropiado al término de la jornada laboral.

Acceso a la información

Se deberán aplicar los mecanismos de acceso restringido a la información que haya implementado la Entidad empleadora, salvaguardando las claves de acceso de toda divulgación o comunicación a otras personas.

Cada persona sólo está autorizada a acceder a los recursos que sean necesarios para el desarrollo y cumplimiento de sus funciones.

Se restringirá el acceso a los equipos informáticos mediante procedimientos de puedan identificar y autenticar la persona que accede a los mismos. Los nombres de usuario y contraseña tendrán la consideración de datos personales intransferibles.

Procesamiento de datos

Los soportes documentales e informáticos deberán estar dispuestos de tal forma que no sean accesibles a personas no autorizadas.

Si una persona abandona su puesto de trabajo temporalmente, deberá ocultar los documentos y bloquear el ordenador, de modo que se impida la visualización de la información con la que estaba trabajando.

Cuando se utilicen impresoras o fotocopiadoras, después de la impresión de trabajos con información de carácter personal, se debe recoger de manera inmediata, o imprimir de forma bloqueada, asegurándose de no dejar documentos impresos en la bandeja de salida.

Transporte de soportes

El transporte de soportes que contengan datos personales deberá realizarse únicamente por personal autorizado o empresas externas contratadas para tal fin por el Responsable del tratamiento.

Eliminación de documentos

Cualquier documento físico o soporte digital que quiera ser eliminado y que incluya datos personales, debe ser destruido con la destructora o retirados por una empresa homologada de destrucción de documentos.

Copia de seguridad y recuperación de datos

El personal deberá almacenar toda la información tratada en el directorio de red correspondiente indicado por el Responsable de seguridad, lo que permitirá que a esta información se le apliquen las medidas de seguridad existentes y que se sometan los

procedimientos de copias de seguridad aplicados por la Entidad empleadora.

Protección de datos

Se deberán aplicar las medidas de protección de datos establecidos por la Entidad empleadora relativos a la seguridad del tratamiento como pueden ser la seudonimización o cifrado de datos o advertencias de intrusión como antivirus, antispam, etc.

Gestión de incidencias

Se considera una incidencia a cualquier violación de la seguridad que ocasione la destrucción accidental o ilícita, pérdida, alteración, o el acceso o comunicación no autorizados de datos personales.

El personal tiene la obligación de notificar sin demora injustificada, cualquier incidencia que tenga conocimiento al Responsable de seguridad para su conocimiento y aplicación de medidas correctivas para remediar y mitigar los efectos que hubiera podido ocasionar. Las incidencias deberán documentarse por la persona que la notifica con una descripción detallada de la misma y la fecha y hora en que se ha producido o se ha tenido conocimiento de ella.

El conocimiento y no notificación de una incidencia por parte del personal se considerará una falta contra la seguridad de los datos y podrá suponer el inicio de acciones legales, así como la reclamación de las indemnizaciones, sanciones y daños o perjuicios que el Responsable se vea obligada a atender como consecuencia de dicho incumplimiento.

ANEXO III: Política de Seguridad de la Información de HM HOSPITALES y Normas de Uso de los Sistemas de Información

El propósito de la **Política de la Seguridad de la Información** es proteger los activos de información de HM HOSPITALES, asegurando para ello la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información y de las instalaciones, sistemas y recursos que la procesan, gestionan, transmiten y almacenan, siempre de acuerdo con los requerimientos del negocio y la legislación vigente.

Esta Política de Seguridad de la Información es de aplicación y de obligado cumplimiento a todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información conocida, gestionada o propiedad de HM HOSPITALES para los procesos descritos.

En las **Normas de Uso de los Sistemas de Información** se detallan las normas de utilización de los activos de los sistemas de información que los usuarios deben cumplir y respetar con el objeto de:

Preservar la seguridad de la información y el adecuado funcionamiento de los sistemas de HM HOSPITALES.

Garantizar el cumplimiento de la legislación y la normativa aplicable, incluyendo la de protección de datos de carácter personal.

Evitar la vulneración de los derechos de propiedad intelectual o industrial.

Las normas incluidas en dicho documento son de obligado cumplimiento para todos los usuarios, internos o externos, de HM HOSPITALES.

Ambos documentos están disponibles en Dharma y en la intranet de HM Hospitales.

Mediante la presente firma, declaro haber leído y comprendido completamente todos los protocolos y políticas incluidos en este documento, y me comprometo a cumplirlos en su totalidad.

Fecha:

Firma empleado/a: **Razón social empleadora:**

<Firmante> **<Sello>**