ANEXO DE MEDIDAS DE SEGURIDAD DEL REGISTRO DE ACTIVIDADES DE TRATAMIENTO DE DATOS PERSONALES

ANEXO

INFORMACIÓN DE INTERÉS GENERAL

Este documento ha sido diseñado para tratamientos de datos personales de bajo riesgo de donde se deduce que el mismo no podrá ser utilizado para tratamientos de datos personales que incluyan datos personales relativos al origen étnico o racial, ideología política religiosa o filosófica, filiación sindical, datos genéticos y biométricos, datos de salud, y datos de orientación sexual de las personas así como cualquier otro tratamiento de datos que entrañe alto riesgo para los derechos y libertades de las personas.

El artículo 5.1.f del Reglamento General de Protección de Datos (en adelante, RGPD) determina la necesidad de establecer garantías de seguridad adecuadas contra el tratamiento no autorizado o ilícito, contra la pérdida de los datos personales, la destrucción o el daño accidental. Esto implica el establecimiento de medidas técnicas y organizativas encaminadas a asegurar la integridad y confidencialidad de los datos personales y la posibilidad de demostrar, tal y como establece el artículo 5.2, que estas medidas se han llevado a la práctica (*responsabilidad proactiva*).

Además, deberá establecer mecanismos visibles, accesibles y sencillos para el ejercicio de derechos y tener definidos procedimientos internos para garantizar la atención efectiva de las solicitudes recibidas.

ATENCIÓN DEL EJERCICIO DE DERECHOS

El responsable del tratamiento informará a todos los trabajadores acerca del procedimiento para atender los derechos de los interesados, definiendo de forma clara los mecanismos por los que pueden ejercerse los derechos (medios electrónicos, referencia al Delegado de Protección de Datos si lo hubiera, dirección postal, etc.) y teniendo en cuenta lo siguiente:

- Previa presentación de su documento nacional de identidad o pasaporte, los titulares de los datos personales (interesados) podrán ejercer sus derechos de acceso, rectificación, supresión, oposición, portabilidad y limitación del tratamiento. El ejercicio de los derechos es gratuito.
- El responsable del tratamiento deberá dar respuesta a los interesados sin dilación indebida y de forma concisa, transparente, inteligible, con un lenguaje claro y sencillo y conservar la prueba del cumplimiento del deber de responder a las solicitudes de ejercicio de derechos formuladas.
- Si la solicitud se presenta por medios electrónicos, la información se facilitará por estos medios cuando sea posible, salvo que el interesado solicite que sea de otro modo.
- Las solicitudes deben responderse en el plazo de 1 mes desde su recepción, pudiendo prorrogarse en otros dos meses teniendo en cuenta la complejidad o el número de solicitudes, pero en ese caso debe informarse al interesado de la prórroga en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación.

ANEXO DE MEDIDAS DE SEGURIDAD DEL REGISTRO DE ACTIVIDADES DE TRATAMIENTO DE DATOS PERSONALES

DERECHO DE ACCESO: En el derecho de acceso se facilitará a los interesados copia de los datos personales de los que se disponga junto con la finalidad para la que han sido recogidos, la identidad de los destinatarios de los datos, los plazos de conservación previstos o el criterio utilizado para determinarlo, la existencia del derecho a solicitar la rectificación o supresión de datos personales así como la limitación o la oposición a su tratamiento, el derecho a presentar una reclamación ante la Agencia Española de Protección de Datos y si los datos no han sido obtenidos del interesado, cualquier información disponibles sobre su origen. El derecho a obtener copia de los datos **no puede afectar negativamente** a los derechos y libertades de otros interesados.

- Formulario para el ejercicio del derecho de acceso.

DERECHO DE RECTIFICACIÓN: En el derecho de rectificación se procederá a modificar los datos de los interesados que fueran inexactos o incompletos atendiendo a los fines del tratamiento. El interesado deberá indicar en la solicitud a qué datos se refiere y la corrección que haya de realizarse, aportando, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento. Si los datos han sido comunicados por el responsable a otros responsables, deberá notificarles la rectificación de estos salvo que sea imposible o exija un esfuerzo desproporcionado, facilitando al interesado información acerca de dichos destinatarios, si así lo solicita.

- Formulario para el ejercicio del derecho de rectificación

DERECHO DE SUPRESIÓN: En el derecho de supresión se eliminarán los datos de los interesados cuando estos manifiesten su negativa al tratamiento y no exista una base legal que lo impida, no sean necesarios en relación con los fines para los que fueron recogidos, retiren el consentimiento prestado y no haya otra base legal que legitime el tratamiento o éste sea ilícito. Si la supresión deriva del ejercicio del derecho de oposición del interesado al tratamiento de sus datos con fines de mercadotecnia, pueden conservarse los datos identificativos del interesado con el fin de impedir futuros tratamientos. Si los datos han sido comunicados por el responsable a otros responsables, deberá notificarles la supresión de estos salvo que sea imposible o exija un esfuerzo desproporcionado, facilitando al interesado información acerca de dichos destinatarios, si así lo solicita.

- Formulario para el ejercicio del derecho de supresión.

ANEXO DE MEDIDAS DE SEGURIDAD DEL REGISTRO DE ACTIVIDADES DE TRATAMIENTO DE DATOS PERSONALES

DERECHO DE OPOSICIÓN: En el derecho de oposición, cuando los interesados manifiesten su negativa al tratamiento de sus datos personales ante el responsable, este dejará de procesarlos siempre que no exista una obligación legal que lo impida. Cuando el tratamiento esté basado en una misión de interés público o en el interés legítimo del responsable, ante una solicitud de ejercicio del derecho de oposición, el responsable dejará de tratar los datos salvo que se acrediten motivos imperiosos que prevalezcan sobre los intereses, derechos y libertades del interesado o sean necesarios para la formulación, ejercicio o defensa de reclamaciones. Si el interesado se opone al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para estos fines.

- Formulario para el ejercicio del derecho de oposición.

DERECHO DE PORTABILIDAD: En el derecho de portabilidad, si el tratamiento se efectúa por medios automatizados y se basa en el consentimiento o se realiza en el marco de un contrato, los interesados pueden solicitar recibir copia de sus datos personales en un formato estructurado, de uso común y lectura mecánica. Asimismo, tienen derecho a solicitar que sean transmitidos directamente a un nuevo responsable, cuya identidad deberá ser comunicada, cuando sea técnicamente posible.

- Formulario para el ejercicio de la portabilidad de los datos.

DERECHO DE LIMITACIÓN AL TRATAMIENTO: En el derecho de limitación del tratamiento, los interesados pueden solicitar la suspensión del tratamiento de sus datos para impugnar su exactitud mientras el responsable realiza las verificaciones necesarias o en el caso de que el tratamiento se realice en base al interés legítimo del responsable o en cumplimiento de una misión de interés público, mientras se verifica si estos motivos prevalecen sobre los intereses, derechos y libertades del interesado. El interesado también puede solicitar la conservación de los datos si considera que el tratamiento es ilícito y, en lugar de la supresión, solicita la limitación del tratamiento, o si aun no necesitándolos ya el responsable para los fines para los que fueron recabados, el interesado los necesita para la formulación, ejercicio o defensa de reclamaciones. La circunstancia de que el tratamiento de los datos del interesado esté limitado **deberá constar claramente en los sistemas** del responsable. Si los datos han sido comunicados por el responsable a otros responsables, deberá notificarles la limitación del tratamiento de estos salvo que sea imposible o exija un esfuerzo desproporcionado, facilitando al interesado información acerca de dichos destinatarios, si así lo solicita.

- Formulario para el ejercicio de la limitación del tratamiento.

Si no se da curso a la solicitud del interesado, el responsable del tratamiento le informará, sin dilación y a más tardar transcurrido un mes desde la recepción de esta, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante la Agencia Española de Protección de Datos y de ejercitar acciones judiciales.

MEDIDAS DE SEGURIDAD

A tenor del tipo de tratamiento que ha puesto de manifiesto cuando ha cumplimentado este formulario, las medidas de seguridad mínimas que debería tener en cuenta son las siguientes:

MEDIDAS ORGANIZATIVAS

INFORMACIÓN QUE DEBERÁ SER CONOCIDA POR TODO EL PERSONAL CON ACCESO A DATOS PERSONALES

Todo el personal con acceso a los datos personales deberá tener conocimiento de sus obligaciones con relación a los tratamientos de datos personales y serán informados acerca de dichas obligaciones. La información mínima que será conocida por todo el personal será la siguiente:

- DEBER DE CONFIDENCIALIDAD Y SECRETO
    - Se deberá evitar el acceso de personas no autorizadas a los datos personales. A tal fin se evitará dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.). Esta consideración incluye las pantallas que se utilicen para la visualización de imágenes del sistema de videovigilancia. Cuando se ausente del puesto de trabajo, se procederá al bloqueo de la pantalla o al cierre de la sesión.
    - Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día.
    - No se desecharán documentos o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción efectiva
    - No se comunicarán datos personales o cualquier otra información de carácter personal a terceros, prestando especial atención a no divulgar datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.
    - El deber de secreto y confidencialidad persiste incluso cuando finalice la relación laboral del trabajador con la empresa.

- VIOLACIONES DE SEGURIDAD DE DATOS DE CARÁCTER PERSONAL
    - Cuando se produzcan violaciones de seguridad de datos de carácter personal como, por ejemplo, el robo o acceso indebido a los datos personales se notificará a la Agencia Española de Protección de Datos en término de 72 horas acerca de dichas violaciones de seguridad, incluyendo toda la información necesaria para el

esclarecimiento de los hechos que hubieran dado lugar al acceso indebido a los datos personales. La notificación se realizará por medios electrónicos a través de la sede electrónica de la Agencia Española de Protección de Datos en la dirección https://sedeagpd.gob.es/sede-electronica-web/.

MEDIDAS TÉCNICAS

IDENTIFICACIÓN

- Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.
- Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.
- Se garantizará la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras.
- Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).
- Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. Para la gestión de las contraseñas puede consultar la guía de privacidad y seguridad en internet de la Agencia Española de Protección de Datos y el Instituto Nacional de Ciberseguridad. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.

DEBER DE SALVAGUARDA

A continuación, se exponen las medidas técnicas mínimas para garantizar la salvaguarda de los datos personales:

- **ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS**: Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posible.
- **MALWARE**: En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y

datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.

- **CORTAFUEGOS O FIREWALL**: Para evitar accesos remotos indebidos a los datos personales se velará por garantizar la existencia de un firewall activado y correctamente configurado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.
- **CIFRADO DE DATOS**: Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.
- **COPIA DE SEGURIDAD**: Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.

Las medidas de seguridad serán revisadas de forma periódica, la revisión podrá realizarse por mecanismos automáticos (software o programas informáticos) o de forma manual. Considere que cualquier incidente de seguridad informática que le haya ocurrido a cualquier conocido le puede ocurrir a usted, y prevéngase contra el mismo.
Si desea más información u orientaciones técnicas para garantizar la seguridad de los datos personales y la información que trata su empresa, el Instituto Nacional de Ciberseguridad (INCIBE) en su página web www.incibe.es, pone a su disposición herramientas con enfoque empresarial en su sección «Protege tu empresa» donde, entre otros servicios, dispone de:

- un apartado de formación con un videojuego, retos para respuesta a incidentes y videos interactivos de formación sectorial,
- un Kit de concienciación para empleados,
- diversas herramientas para ayudar a la empresa a mejorar su ciberseguridad, entre ellas políticas para el empresario, el personal técnico y el empleado, un catálogo de empresas y soluciones de seguridad y una herramienta de análisis de riesgos.
- dosieres temáticos complementados con videos e infografías y otros recursos,
- guías para el empresario,

Además INCIBE, a través de la Oficina de Seguridad del Internauta, pone también a su disposición herramientas informáticas gratuitas e información adicional pueden ser de utilidad para su empresa o su actividad profesional.

ANEXO DE MEDIDAS DE SEGURIDAD DEL REGISTRO DE ACTIVIDADES DE TRATAMIENTO DE DATOS PERSONALES

CAPTACIÓN DE IMÁGENES CON CÁMARAS Y FINALIDAD DE SEGURIDAD (VIDEOVIGILANCIA)

La imagen de una persona, en la medida que la identifique o la pueda identificar, constituye un dato de carácter personal que puede ser objeto de tratamiento para diversas finalidades. Si bien la más común consiste en utilizar las cámaras para garantizar la seguridad de personas, bienes e instalaciones, también pueden usarse con otros fines como el control de la prestación laboral de los trabajadores. A continuación, se incluyen las directrices básicas a respetar para que el tratamiento de las imágenes obtenidas a partir de cámaras de videovigilancia sea conforme a la normativa de protección de datos. No obstante, se recomienda la consulta de la Guía sobre el uso de videocámaras para seguridad y otras finalidades para un conocimiento más exhaustivo de las obligaciones que conlleva este tipo de tratamiento.

- **UBICACIÓN DE LAS CÁMARAS**: Se evitará la captación de imágenes en zonas destinadas al descanso de los trabajadores, así como la captación de la vía pública si se utilizan cámaras exteriores, estando únicamente permitido la captación de la extensión mínima imprescindible para preservar la seguridad de las personas, bienes e instalaciones.

- **UBICACIÓN DE MONITORES**: Los monitores donde se visualicen las imágenes de las cámaras se ubicarán en un espacio de acceso restringido de forma que no sean accesibles a terceros. A las imágenes grabadas sólo accederá el personal autorizado.

- **CONSERVACIÓN DE IMÁGENES**: Las imágenes se almacenarán durante el plazo máximo de un mes, con excepción de las imágenes que acrediten la comisión de actos que atenten contra la integridad de personas, bienes e instalaciones. En ese caso las imágenes deben ser puestas a disposición de la autoridad competente en un plazo de 72 horas desde que se tuviera conocimiento de la existencia de la grabación.

- **DEBER DE INFORMACIÓN**: Se informará acerca de la existencia de las cámaras y grabación de imágenes mediante un distintivo informativo colocado en un lugar suficientemente visible donde se identifique, al menos, la identidad del responsable y la posibilidad de los interesados de ejercer sus derechos en materia de protección de datos. En el propio pictograma se podrá incluir también un código de conexión o dirección de internet en la que se muestre esta información. Dispone de modelos, tanto del pictograma como del texto, en la página web de la Agencia.
    - Modelo de cartel de aviso de zona videovigilada.

- **CONTROL LABORAL**: Cuando las cámaras vayan a ser utilizadas con la finalidad de control laboral según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informará al trabajador y a sus representantes sindicales por cualquier medio que garantice la recepción de la información acerca de las medidas de control establecidas por el empresario con indicación expresa de la finalidad de control laboral de las imágenes captadas por las cámaras.

- **DERECHO DE ACCESO A LAS IMÁGENES**: Para dar cumplimiento al derecho de acceso de los interesados a las grabaciones del sistema de videovigilancia se solicitará una fotografía reciente y el Documento Nacional de Identidad del interesado para comprobar su identidad, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso. No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. En caso de no ser posible la visualización de las imágenes por el interesado sin mostrar imágenes de terceros, se le facilitará un documento en el que se confirme o niegue la existencia de imágenes del interesado.

Para más información puede consultar las guía y las fichas de videovigilancia y los informes jurídicos publicados por la Agencia Española de Protección de Datos en la sección de Videovigilancia.