MEDIDAS DE SEGURIDAD EN EL TRATAMIENTO DE LOS DATOS PERSONALES DE LA EMPRESA WORK&TRAVEL GUIDE

En este documento se describen las medidas de protección de datos para asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de cada uno de los soportes o sistemas de tratamiento, así como medidas para asegurar la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.

Igualmente se describen las medidas organizativas adoptadas para garantizar que las personas autorizadas a tratar datos personales sigan determinadas instrucciones y buenas prácticas

Medidas técnicas de seguridad en el tratamiento de los datos personales.

1. Medidas relativas a los soportes electrónicos.

Cuando los datos de carácter personal son tratados mediante dispositivos electrónicos, ya sean ordenadores o cualquier otro dispositivo, la empresa adopta las siguientes medidas de seguridad:

Medidas de acceso:

- es imposible que cualquier persona **no autorizada** tenga acceso a los equipos, se encuentran **ubicados en un despacho/armario cerrado bajo llave**.

- los equipos cuentan con un bloqueo automático de acceso que se activa cuando han transcurrido 30 segundos de inactividad y se requiere una **contraseña** para su desactivación y posterior acceso.

- los equipos tienen varios usuarios y cada uno accede con sus propias claves/ contraseñas.

Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal debe 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.

El sistema de contraseñas seguras deberá contener un mínimo de 8 caracteres alfanuméricos, serán contraseñas irrepetibles, únicas e intransferibles.

Deberá modificar las contraseñas al menos con una frecuencia mensual, conservando un registro de los cambios, así como de los usuarios que tienen acceso a los datos.

Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se debe disponer de un usuario y contraseña específicos (identificación inequívoca).

Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.

Las contraseñas serán facilitadas por la persona encargada de la creación y asignación de contraseñas.

Medidas de protección:

- Elementos de protección instalados en los equipos: Antivirus, Cortafuegos, Antispam.

Copias de seguridad de los datos de carácter personal.

- Para garantizar la disponibilidad y la restauración de los datos, se realizan copias de seguridad de todos los datos con la siguiente periodicidad: diaria

- Las copias de seguridad se realizan en soportes distintos de los soportes en los que se realizan los tratamientos de los datos: ubicación de red (programa interno: zoho)

- Se mantiene un registro de los soportes con actividades de tratamiento (ver registro de soportes).

Borrado de datos

Cuando sea necesario el borrado de datos de carácter personal de un dispositivo, el borrado se realizará en condiciones seguras, comprobando que los datos serán destruidos y que no es posible su recuperación (salvo en las copias de seguridad).

Cuando el borrado se lleve a cabo sobre datos que no son necesarios, se identificarán perfectamente los datos personales que deben ser eliminados de los sistemas de tratamiento, verificando que sobre los datos no se aplican acciones de conservación por imperativo legal y que los usuarios no se han pronunciado al respecto. Una vez realizadas las comprobaciones se eliminarán los datos de los sistemas de tratamiento, comprobando que también son borrados de las copias de seguridad.

Cuando el borrado de datos sea parcial, al objeto de limitar las actividades de tratamiento o a petición de los interesados, y siempre que no exista un imperativo legal que obligue a guardarlos durante un periodo determinado, se procederá a eliminar los datos no necesarios, tanto de los sistemas de tratamiento como de las copias de seguridad.

Cuando el borrado de datos sea consecuencia del cese de la actividad de tratamiento sobre los datos, pero requiera su conservación para futuras reclamaciones o por imperativo legal, se señalarán los datos guardados de forma que no sea posible su tratamiento, tanto en los sistemas de tratamiento como en las copias de seguridad.

Borrado de datos:

- Borrado periódico de la documentación contenida en la carpeta de descargas y papelera de reciclaje

2. Medidas relativas a los soportes en papel.

Para el mantenimiento de los soportes manuales o en papel que contienen datos de carácter personal se adoptan las siguientes medidas:

- La ubicación de los soportes impide el acceso a personas no autorizadas (bajo llave, etc...)
- La ubicación de los soportes garantiza la integridad de los datos, permitiendo su conservación en condiciones ambientales adecuadas.
- La ubicación de los soportes garantiza la disponibilidad de los datos en cualquier momento.

3. Medidas organizativas y de control.

Control de entrada/salida de soportes

Todos los soportes que contienen datos de carácter personal, tanto los soportes que dan servicio al sistema de tratamiento como los que recogen las copias de seguridad o de respaldo están obligados a un control exhaustivo por parte de la empresa. Cuando un soporte que contiene datos de carácter personal debe salir de las instalaciones de la empresa queda fuera del control y de las medidas impuestas por la empresa.

En este caso, en primer lugar, se asegura que el encargado del transporte del soporte es un encargado del tratamiento debidamente seleccionado y con el que se dispone el correspondiente acuerdo de confidencialidad firmado.

Si es necesario y en función a los datos de carácter personal que contiene el soporte deberán adoptarse medidas adicionales de seguridad, de cifrado de datos por ejemplo o alguna medida que impida a cualquier usuario el acceso y comprensión de los datos.

Se registrará tanto el soporte como el destinatario (que debe ser un encargado del tratamiento o un usuario con autorización de acceso a los datos), el motivo de salida del soporte, así como la fecha de salida y finalmente la fecha de entrada del mismo.
El responsable o la persona encargada de estas actividades de control verificarán a su recepción que todo está correcto.

Información a los trabajadores

A todos los trabajadores con acceso a datos de carácter personal y con permisos de tratamiento se les informa de determinados deberes y obligaciones:

Deber de confidencialidad y secreto

Se informa que deben evitar el acceso de personas no autorizadas a los datos personales, a tal fin 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, procederá al bloqueo de la pantalla o al cierre de la sesión.

Los documentos en papel y soportes electrónicos se almacenan en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día. En caso de utilizar cualquier documento con datos de carácter personal debe devolver el documento a su archivo seguro.

Nunca desechar documentos o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción.

No comunicar datos personales o cualquier información personal a terceros, prestando atención especial en no divulgar los datos protegidos durante las consultas telefónicas, correos electrónicos, etc.

Videovigilancia

Nunca se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestran imágenes de terceros. Para acceder a las imágenes, cada usuario deberá solicitarlo por escrito.
Si las imágenes están guardadas en un soporte interno el acceso a las imágenes es responsabilidad del responsable o del encargado de seguridad y salvaguarda.
Si las imágenes las conserva la empresa de videovigilancia, igualmente la empresa tiene que firmar el acuerdo de confidencialidad de los datos debiendo seguir el procedimiento que como encargado del tratamiento se haya definido contractualmente en cuanto a la atención al ejercicio de los derechos de los afectados.

Uso de internet

Los trabajadores son responsables de las sesiones iniciadas de Internet desde sus terminales de trabajo. Internet tiene carácter laboral, y no puede ni debe usarse con otros fines.
En ningún caso se pueden modificar las configuraciones de los navegadores del equipo, ni la activación de servidores o puertos sin autorización del coordinador de seguridad, o en su caso del responsable del tratamiento.

Debe evitarse la utilización de imágenes y sonidos distintos e incompatibles a la actividad laboral.
Se prohíbe expresamente el acceso y/o la descarga y/o el almacenamiento en cualquier soporte de páginas y contenidos ilegales, inadecuados o que atenten contra la moral y las buenas costumbres; de los formatos de imágenes, sonido o vídeo; de virus y códigos maliciosos y en general, todo tipo de programas sin la expresa autorización del coordinador de seguridad.
Queda vetada toda utilización ajena a las actividades de la empresa, de los servicios de chat, foros u otros sitios similares. Tampoco se permite el acceso a páginas de juego en línea, o la descarga de cualquier dispositivo similar.

Uso del sistema informático

Se prohíbe la instalación de cualquier programa o producto informático en el sistema de información, sin la correspondiente autorización del coordinador de seguridad o del responsable en su caso.
Las aplicaciones necesarias para el desempleo de su trabajo, serán instaladas exclusivamente por el coordinador de seguridad o del responsable en su caso.
No se permite la utilización de recursos del sistema informático puesto a disposición por la empresa con fines privados con cualquier otro fin diferente a los estrictamente laborales.
Se prohíbe revelar a persona alguna ajena a la empresa, información a la que haya tenido acceso en el desempeño de sus funciones, sin la debida autorización.
Se prohíbe facilitar a persona cualquiera ningún soporte conteniendo datos a los que hayan tenido acceso en el desempeño de sus funciones sin la debida autorización.
Se prohíbe utilizar cualquier información que hubiese podido ser obtenida por su condición de empleado de la compañía, con cualquier otro fin que no sea el estrictamente necesario para el desempeño de sus funciones.

Uso del correo electrónico

Los trabajadores son responsables de todas las actividades realizadas con las cuentas de acceso y su respectivo buzón de correos provistos por la empresa

Los empleados no deberán permitir la utilización de la cuenta y/o el correspondiente buzón a personas no autorizadas.
Los servicios de correo electrónico suministrados deben destinarse a uso estrictamente laboral.
Está prohibida la utilización, en los equipos provistos por la empresa, de buzones de correo electrónico de otros proveedores de Internet.
No es legal enviar correo a personas que no desean recibirlo. Si le solicitan detener esta práctica deberá hacerlo. Si la empresa recibe reclamaciones sobre esta práctica, se tomarán las medidas sancionadoras adecuadas.
Se prohíbe realizar cualquiera de las siguientes actividades:

- Utilizar el correo electrónico para cualquier propósito ajeno a las actividades laboral
- Participar en la propagación de cartas encadenadas, esquemas piramidales o similares.

- Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para la empresa.
- Falsificar las cabeceras de correo electrónico.
- Recoger correo de buzones de otro proveedor de Internet.
- Difundir contenido ilegal o contrario a la moral y las buenas costumbres.
- Enviar correo propio a través de cuentas ajenas sin consentimiento de su titular.
- Efectuar ataques con objeto de imposibilitar u obstruir sistemas informáticos, dirigidos a un usuario o al propio sistema de correo, así como le envío de un número alto de mensajes por segundo, o cualquier variante que tenga por objeto la paralización del servicio por saturación de las líneas, de la capacidad de la CPU a del servidor, del espacio en disco de servidores, o terminales o cualquier otra práctica similar.
- Enviar a foros de discusión, listas de distribución o grupos de noticias, mensajes que comprometan la reputación de la empresa

Propiedad intelectual

Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia, así como el uso reproducción, cesión o transformación, o comunicación pública de cualquier tipo de programa informático protegido por los derechos de propiedad intelectual o industrial.