REGISTRO DE ENTREGA DE DISPOSITIVOS AL TRABAJADOR

Con el presente documento queda constancia de que, con fecha ___ de_____ de 20__ se hace entrega a [NOMBRE Y APELLIDO DEL EMPLEADO], con D.N.I. / N.I.E.: _____ quien desempeña el/la [puesto o actividad] en la de la entidad emisora del soporte (empresa)_____, (en adelante la *Entidad)*, para el desarrollo de su puesto de trabajo, el siguiente / los siguientes dispositivo(s):

TIPO	
MODELO	
MARCA	
Nº DE SERIE	
Nº DE LINEA o PUK	

Respecto al dispositivo entregado / de los dispositivos entregados, se informa al trabajador que tiene las siguientes obligaciones:

- Custodiar el dispositivo adecuadamente, evitando que sufra deterioros o daños ocasionados por un mal uso, mala manipulación o incorrecto almacenaje, implementando o manteniendo en el dispositivo todas las medidas de seguridad establecidas por la Entidad.
- No utilizar el dispositivo para fines ilícitos o conductas no permitidas por la Entidad.
- No utilizar para fines personales ni aquellos que no estén relacionados con la ejecución de la actividad laboral.
- Notificar a la Entidad inmediatamente y en un plazo no superior de 24 horas cualquier extravío, robo o incidencia relacionada con el dispositivo, que pueda comprometer la protección de datos de carácter personal.
- Devolver el dispositivo cuando le sea requerido por la Entidad y, en todo caso, al finalizar el servicio para cuya finalidad se haya entregado el dispositivo o cuando se haya resuelto el contrato laboral que tenga suscrito con la misma.

A los efectos del *Reglamento UE 2016/679, de 27 de abril de 2016 (R.G.P.D.)* y la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (L.O.P.D.G.D.D.)* Se le informa que los datos de carácter personal recogidos en el presente documento serán tratados únicamente por la Entidad, con la finalidad de llevar a cabo un adecuado registro del o de los dispositivo(s) entregados a los trabajadores con el fin de gestionar las eventuales violaciones de la seguridad de los datos personales con mayor rapidez y eficacia. Los datos aquí indicados no serán utilizados ni tratados para una finalidad distinta ni cedidos a terceros y serán conservados mientras dure la relación laboral, siempre y cuando no existan acciones legales pendientes de resolución relacionadas con el o los dispositivo(s) que se entrega(n). Podrá ejercitar sus derechos de acceso, rectificación, supresión u oposición, como el resto que le otorga la normativa mencionada a través de un correo electrónico a: info@ceriosrosas.com. Para más información sobre sus derechos puede consultar nuestra política de privacidad de relaciones laborales.

Con la firma del documento el destinatario reconoce que ha sido informado sobre las obligaciones antes indicadas y se compromete a cumplir diligentemente con las mismas; su negativa firmarlo determinará que la Entidad no pueda entregarle el dispositivo.

NOMBRE Y FIRMA TRABAJADOR

EMPRESA
SELLO DE LA ENTIDAD

POLÍTICA

DISPOSITIVOS MÓVILES Y TELETRABAJO

(DOCUMENTO INFORMATIVO)

1. OBJETIVO, ALCANCE Y USUARIOS.

El objetivo de la presente política es, por un lado, establecer un marco de gestión para la implantación de medidas adecuadas de seguridad contra los riesgos que pueda causar la utilización de ordenadores portátiles y comunicaciones móviles y, por otro lado, proteger la información que es o ha sido objeto de acceso, tratamiento y/o almacenamiento en sitios de teletrabajo.

Este Procedimiento es aplicable a todo el personal que desempeñe sus funciones laborales fuera de las instalaciones de la organización y/o utilice dispositivos móviles o tele-trabajo.

2. DISPOSITIVOS MÓVILES.

2.1.Introducción

Dentro de la clasificación de "Dispositivo Móvil" se incluye todo tipo de portátiles, teléfonos móviles (inteligentes o no), tabletas, tarjetas de memoria, pen drives, discos duros externos, CD, DVD y cualquier otro equipo móvil utilizado para almacenamiento, procesamiento y/o transferencia de datos. En adelante denominados indistintamente como el "Dispositivo".

Los móviles y portátiles de empresa, por su propia naturaleza, podrán ser llevados fuera de las instalaciones de la organización sin necesidad de una autorización previa, aunque será obligatorio firmar previamente el registro de entrega de dispositivos.

El resto de Dispositivos, podrán ser llevados fuera de las instalaciones de la organización, solamente con autorización previa del Responsable TIC o de la persona Responsable del S.G.I.

2.2.Reglas

Se debe tener especial cuidado cuando el Dispositivo se encuentra en vehículos (incluyendo automóviles propios y/o de conocidos), espacios públicos, habitaciones de hotel, salas de reunión, centros de conferencias y demás áreas no protegidas, todas ellas exteriores a las instalaciones de la organización.

La persona que utilice dispositivos fuera de las instalaciones debe cumplir las siguientes reglas:

- No utilizar otros dispositivos informáticos diferentes a los suministrados.
- El Dispositivo que contenga información importante, sensible, crítica o datos especialmente protegidos por el R.G.P.D. no debe ser desatendido, quedando en lo

posible resguardado bajo llave. De igual forma se adoptarán, en su caso, trabas especiales para asegurarlo.

- Firmar y aceptar las condiciones de uso, contempladas en el documento *"Registro de Dispositivos".*
- No conectar a internet los dispositivos corporativos utilizando redes WIFI públicas sin utilizar el acceso VPN corporativo.
- Cuando se utilice equipamiento de computación móvil en lugares públicos, se deberá tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.
- Deberán contar con las últimas instalaciones de parches y actualizaciones del sistema operativo, de acuerdo a las actualizaciones periódicas previstas por el desarrollador del sistema.
- Las configuraciones de seguridad deberán venir predeterminadas por el responsable informático de la empresa.
- La protección contra códigos maliciosos debe estar instalada y configurada para que se actualice de forma automática.
- Como regla general, ningún dato de carácter personal deberá ser almacenado en soportes extraíbles. Si llegara a ser necesario utilizar cualquier tipo de soporte extraíble, se deberá solicitar autorización a la persona Responsable del Sistema, quien deberá registrar dicho soporte en el registro de soportes extraíbles.
- La persona que utiliza el "soporte" fuera de las instalaciones es la responsable de realizar periódicamente copias de seguridad de los datos.
- La información sensible, incluyendo los datos de carácter personal que se encuentra en ordenadores portátiles, deben estar encriptados o seunonimizados.
- Como regla general, los soportes no pueden ser desatendidos. En caso de que, de forma excepcional, el "soporte" sea desatendido, se deberán aplicar las reglas para equipamiento de usuario desatendido, de acuerdo a la Política de uso aceptable.
- En caso de extravío, robo, hurto o acceso no autorizado al dispositivo, el trabajador deberá comunicar el acontecimiento de forma inmediata a la persona Responsable del Sistema.

La persona Responsable del Sistema junto con el Director TIC son las personas responsables de la capacitación y concienciación de las personas que utilicen estos dispositivos.

Las actividades relativas a la gestión de la seguridad de la información deben ser coordinadas entre los representantes de los diferentes departamentos de la organización, con sus correspondientes roles y funciones de trabajo. La coordinación en materia de seguridad de la información de las actividades de la Organización será abordada, en primera instancia, por la persona Responsable del Sistema Gestión, supervisada por el Comité de Seguridad de la Información.

3. TELE-TRABAJO.

Tele-trabajo significa que los equipos de información y comunicación se utilizan para permitir que los empleados realicen su trabajo fuera de la organización. El tele-trabajo no incluye el uso de teléfonos móviles fuera de las instalaciones de la organización.

El tele-trabajo debe ser autorizado por Recursos Humanos de forma conjunta con el Director TIC de la organización.

El Director TIC es la responsable de preparar planes y procedimientos, cuando sea necesario aplicar el tele-trabajo, para garantizar lo siguiente:

- Protección del "soporte", de acuerdo a lo indicado en la sección anterior.
- Evitar el acceso no autorizado de personas que viven o trabajan en la ubicación donde se realiza la actividad de tele-trabajo.
- Configuración adecuada de la red local utilizada para conectarse a la Internet.
- Protección de los derechos de propiedad intelectual de la organización, tanto por el software como por otros contenidos que puedan estar protegidos por derechos de propiedad intelectual.
- Proceso de devolución de datos y equipamiento en caso de finalización del empleo.
- Nivel mínimo de configuración de la instalación donde se realizarán las actividades de tele-trabajo.
- Tipos de actividades permitidas y prohibidas.

4. PUBLICACIÓN.

La presente política debe ser conocida y estar accesible para todos los integrantes de la organización, por lo cual se distribuirá la misma a través de los canales habilitados dentro de la organización para ello.

5. HISTORIAL DE CAMBIOS.

Versión	Fecha	Descripción del cambio