POLITICA DE DESCONEXION , USO DE DISPOSITIVOS DIGITALES Y PROTOCOLO PARA LA REGULACION DEL TELETRABAJO de la empresa "General Mills San Adrián S.L.U."

I.- POLITICA DE DESCONEXION DIGITAL :

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los derechos digitales (LOPDGDD) regula en sus artículos 87 a 91 el derecho a la desconexión digital, el derecho a la intimidad en el uso de los dispositivos digitales de videovigilancia y geolocalización y establece la obligación empresarial de elaborar una política interna que regule la desconexión digital a fin de garantizar el respeto a disfrutar de manera efectiva del tiempo de descanso y vacaciones, así como a la intimidad personal y familiar recogido igualmente en el artículo 20 bis del Estatuto de los Trabajadores.

Para favorecer por tanto la conciliación de la vida personal, familiar y laboral, se debe garantizar el descanso de los empleados y reconocerse expresamente su derecho a la desconexión digital una vez finalizada su jornada laboral.

A tal fin, la empresa General Mills San Adrián S.L.U.___ en su compromiso con la cumplimentación de la normativa vigente sobre protección de datos personales, ha elaborado la presente política interna de medidas en materia del ejercicio del derecho a la desconexión digital, derecho a la intimidad en el uso de dispositivos digitales y sistemas de videovigilancia y geolocalización, de aplicación a todo el personal de la empresa.

Además, se incluyen las medidas concretas adoptadas por la empresa para

I.- AMBITO Y PERIODO DE APLICACIÓN

Las medidas recogidas en la presente política son de aplicación a toda la plantilla, tanto las que hacen referencia a la desconexión digital en el tiempo de descanso como las de utilización de los dispositivos digitales en el ámbito laboral si bien se aplicarán en función de las disponibilidades de acceso y uso de los dispositivos y sistemas digitales conforme a los puestos de trabajo, funciones desempeñadas y departamentos de la empresa.

Esencialmente las medidas de desconexión digital se centran en el uso de los sistemas de información por parte de la plantilla durante el tiempo de descanso, bien propio, bien de los otros empleados. Se define tiempo de descanso, como todo periodo que no sea tiempo de trabajo, que generalmente coincidirá con el horario fuera de la jornada habitual de trabajo, según el convenio colectivo que resulta de aplicación

La totalidad de los sistemas de información, servicios, elementos y recursos informáticos de la empresa tienen la consideración de medios de trabajo. El empleado queda por tanto advertido de que deberán ser utilizados durante el tiempo de trabajo, salvo causa de fuerza mayor o circunstancias excepcionales.

Las medidas propuestas a lo largo del presente documento buscan facilitar una aproximación práctica y efectiva al derecho de desconexión digital, pero debe tenerse en cuenta que se trata de directrices generales que podrán ser actualizadas periódicamente y en caso de estimarse necesario podrán ser excepcionadas en supuestos de fuerza mayor o ante acontecimientos excepcionales no previstos en las mismas.

Al efecto la empresa como Responsable el Tratamiento facilita a todos y cada uno de los integrantes de la plantilla en su calidad de usuarios para su firma, el documento **ANEXO I** de COMPROMISO DE CONFIDENCIALIDAD, SECRETO E INFORMACION DE LA POLITICA de DESCONEXION Y USO DE DISPOSITIVOS DIGITALES

II.- DESCONEXION DIGITAL

Para el establecimiento de medidas efectivas en relación con el respeto al derecho a la desconexión digital, se requiere tener en cuenta que todas las partes intervinientes en la comunicación digital son titulares del derecho a la desconexión digital.

Por tanto, al enviar o iniciar una comunicación, es importante tener en cuenta si el destinatario puede estar disfrutando de su tiempo de descanso.

Para la comunicación interna, ya que podrá resultar difícil su determinación cuando los destinatarios sean terceros ajenos a la empresa, deberán observarse las siguientes medidas:

1. .- No existirán limitaciones al uso de los medios de comunicación profesionales entre empleados de la organización ni con terceros ajenos a ésta dentro del horario de la empresa.

2.- Respecto a los empleados de los perfiles profesionales que se determinan a continuación, que por su puesto, funciones, y responsabilidad, deba extenderse el tiempo de trabajo, podrán ser contactados, observando en todo caso los principios de proporcionalidad y excepcionalidad:

.- Gerencia
.- Dirección de departamento o área de la empresa
.- .....

3.-En el caso de que el empleado a quien se dirige la comunicación se encontrase en tiempo de descanso (reducciones de jornada, jornada intensiva, vacaciones, baja por enfermedad...) se dirigirá la misma a su superior jerárquico o a la persona de referencia que el destinatario hubiera designado.

4.- Fuera del tiempo oficial de trabajo se recomienda no emplear los medios de comunicación profesionales salvo necesidad derivada del trabajo, causa de fuerza mayor o circunstancias excepcionales.

III .- EXCEPCIONES

En su caso, se podrá contactar con el personal fuera de su horario laboral en un supuesto excepcional y con carácter de urgente necesidad, que pueda resolverse mediante una llamada o mensaje corto y que, si no se resuelve de forma inmediata, podría implicar un perjuicio para la entidad. En estos supuestos, podrá suscribirse, si es necesario, un acuerdo en el que se fije una hora u horquilla horaria para revisar los dispositivos digitales.

IV.- TELETRABAJO Y DESCONEXIÓN

En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia, así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

A dichos empleados les será a aplicación los criterios de desconexión digital indicados anteriormente, pudiendo concretarse, en cada caso particular, cuál es la franja horaria de "desconexión", en la que no se podrá contactar con el trabajador en cuestión, salvo las excepciones contempladas en el punto anterior.

La empresa ha elaborado como **ANEXO 3 BIS** el **PROTOCOLO DE REGULACION DEL TELETRABAJO** que regula las condiciones para la realización del teletrabajo que será aplicable a todos los trabajadores de la empresa con los que se llegue al acuerdo individual de realización total o parcial de la jornada laboral a distancia, mediante dispositivos electrónicos, facilitados o no por parte de la empresa.

V.- SISTEMAS DE GEOLOCALIZACION:

La Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDPGDD), regula en su artículo 90 el "Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral" y establece:

> *Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.*
>
> *Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión*

Un "sistema de geolocalización" consiste en la instalación de un sistema GPS de localización, cuya finalidad principal es el control empresarial de la actividad laboral de sus empleados.

Los pasos que debe seguir el responsable que pretenda tratar los datos que se obtienen de los sistemas de geolocalización para el ejercicio de funciones de control laboral, son los siguientes:

1. Informar con carácter previo de forma expresa, clara e inequívoca al personal, acerca de su existencia y características.
2. La legitimación del tratamiento, no será el consentimiento del personal, sino el interés legítimo del empresario, amparado en el art.20.3 del Estatuto de los trabajadores, atendiendo los límites inherentes a la ley.
3. Adecuar el tratamiento de los datos al principio de proporcionalidad, es decir que sean adecuados, pertinentes y no excesivos.
4. Informar además al afectado del ejercicio de los derechos de acceso, rectificación, limitación y supresión.

Para su cumplimiento la empresa como responsable cumplimenta el **ANEXO 2** sobre información previa del sistema de geolocalización empleado, que deberá ser presentado a toda la plantilla para su firma.

VI.- INFORMACION DE DERECHOS

La empresa se compromete a cumplir con su deber de información previo al cualquier tratamiento de datos y para ello informará de modo claro y preciso de lo siguiente:

.- La existencia de un tratamiento de datos, la finalidad del mismo y los destinatarios de la información.

.- La identidad del responsable del tratamiento.

.- De la posibilidad de ejercitar los derechos que les asisten a los empleados como personas interesadas, en relación con el Responsable, de acuerdo con el RGPD y que son:

Derecho a solicitar el acceso a los datos personales relativos al interesado,
Derecho a solicitar su rectificación,
Derecho de supresión (olvido),
Derecho a solicitar la limitación de su tratamiento,
Derecho a oponerse al tratamiento,
Derecho a la portabilidad de los datos;

Dichos derechos son personalísimos e independientes entre ellos, por lo que el ejercicio de alguno de los mismos no es requisito previo para el ejercicio de otro.

Se establece el siguiente procedimiento para la gestión de los derechos de los empleados/interesados:

.- Para el correcto ejercicio de los derechos es necesario que el empleado/interesado realice una solicitud dirigida al responsable de los tratamientos que contenga los datos del formulario que se ha creado para el ejercicio de cada derecho.

.- El responsable de los tratamientos contestará al empleado/interesado en el plazo de 1 mes con carácter general, desde la recepción de la notificación, tanto en los casos en que consten datos del solicitante como en el caso de que no fuera así, solicitando la subsanación de los requisitos formales de la solicitud en caso de inexactitud.
.- El responsable de los tratamientos debe adoptar las medidas oportunas para garantizar que todas las personas de su organización conozcan la existencia de dicho procedimiento y cómo actuar en caso de recibir una solicitud de ejercicio de derechos.
.- Cualquier empleado/usuario que reciba una solicitud de ejercicio de derechos deberá comunicarlo inmediatamente al Responsable de Seguridad para su gestión.

VII.- ACCIONES DE SENSIBILIZACION Y FORMACION

Todos los empleados deben conocer esta política de desconexión digital en el ámbito laboral.

Para ello, la empresa adoptará las siguientes acciones:

1º.- Informará y concienciará, tanto a los empleados existentes, como a los nuevos que se incorporen a la empresa acerca de este derecho y, en su caso, del uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En especial, a los que ocupen puestos directivos o de mando.

2º.- Sensibilización de la plantilla, mediante la realización de sesiones informativas sobre la importancia de la desconexión digital, para plantearse si realmente todos los mails y/o llamadas que hacen o reciben fuera del horario convencional son necesarios, si se tiende o no a hacer llamadas y/o enviar mails a los empleados que tienen bajo su mando fuera de su horario laboral....

3º .- Incorporación en boletines internos, intranet, plataforma del empleado de mail periódicos desde el Dpto. de RRHH de comunicación de que la empresa está firmemente comprometida con el cumplimiento de la normativa en materia de desconexión digital.

VIII.- INTERPRETACION, SEGUIMIENTO Y VIGENCIA

El contenido de la presente política de desconexión digital, y de uso de dispositivos digitales, junto con sus anexos. estará vigente en tanto pueda ser modificada, ampliada, conforme surjan interpretaciones, modificaciones legales, resoluciones administrativas o judiciales que aconsejen su interpretación, modificación, o ampliación.

IX.- NORMAS DE USO DE LOS DISPOSITIVOS DIGITALES

1. Acceso al contenido de los dispositivos digitales

Tal y como establece el artículo 87 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, la organización podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

En este sentido, la empresa se reserva la posibilidad de adoptar las medidas que estime más oportunas de vigilancia y control, como son las revisiones de los dispositivos proporcionados o del servidor de correo electrónico, los recursos utilizados o las conexiones a Internet realizadas, entre otras, para verificar el cumplimiento, por parte del empleado usuario, de sus obligaciones y deberes laborales, con los límites establecidos por la ley y la jurisprudencia.

2. Equipamiento informático y recursos

Con carácter general, en la empresa General Mills San Adrian S.L.U. está prohibido utilizar para fines privados los recursos informáticos y telemáticos de la empresa, incluido Internet y el correo electrónico, pues su cometido es que se utilicen exclusivamente para actividades directamente relacionadas con el puesto de trabajo del usuario y con la cuenta de correo electrónico facilitada por la organización.

La empresa se reserva el derecho de cambiar, eliminar, reemplazar el servicio, equipo, compañía proveedora, etc., así como las condiciones y restricciones vigentes.

3. Alcance

Destinatarios/as de las medidas:

Las medidas adoptadas y los principios definidos se aplican a los empleados/as a quienes la empresa ha determinado asignar un medio tecnológico móvil para el correcto desempeño de su trabajo. Se considera que un empleado necesita un equipo de telefonía móvil cuando realiza su trabajo en movilidad, es decir, fuera de nuestras instalaciones, viaja con cierta regularidad, realiza trabajos de guardia, no dispone de telefonía fija o necesita estar comunicado en todo momento.

Serán también aplicables a los trabajadores que desarrollen su trabajo, previo acuerdo con la empresa, mediante el teletrabajo, entendido como aquel trabajo a distancia que se lleva a cabo mediante el uso exclusivo o prevalente de medios y sistemas informáticos, telemáticos y de telecomunicación, desde el domicilio del trabajador o desde un espacio designado por la empresa, y sometido a las medidas organizativas de utilización de dispositivos y softwares de vigilancia y de registro de la jornada laboral.

Responsabilidad de la medida:

La actualización y revisión de la presente medida es responsabilidad del Área de Recursos Humanos o Gestión de Personas y se definen conjuntamente con el Departamento de Tecnologías de la Información.

4. ROLES Y RESPONSABILIDADES

4.1. Departamento de Tecnologías de la Información

Se encarga de determinar los medios tecnológicos más adecuados en función de las necesidades de cada puesto de trabajo.

Mantiene un registro de inventario activo del parque de dispositivos móviles.

Es el Departamento responsable del mantenimiento de los dispositivos.

4.2. Departamento de RRHH o Gestión de Personas

Es el encargado de establecer los niveles que corresponden a cada usuario, así como de solicitar los medios que va a necesitar la persona en su incorporación a la empresa.

Es a quien se le informa de posibles incumplimientos de la política por parte de los empleados/as para su valoración y correspondiente actuación.

5. DOCUMENTACIÓN DE CONTROL DE ENTREGA Y DEVOLUCIÓN

Nuevas incorporaciones:

El Departamento de TI es el encargado de enviar/dar en mano junto a la entrega el documento de entrega de dispositivos que deberá firmar el usuario. La custodia / archivo del documento lo realizará el Departamento de Compensación y Beneficios junto al expediente del empleado/a (firma digital – exportación de datos SAP)

De igual modo, a la desvinculación contractual, el empleado/a deberá firmar el documento de devolución de medios tecnológicos y los devolverá junto a los accesorios que le fueron entregados, debidamente a su Responsable Inmediato / Dpto. Gestión de Personas quien a su vez los hará llegar al Departamento de Tecnologías de la Información para su borrado de datos, adecuación y nueva puesta a disposición de un nuevo usuario.

Colaboradores/as en plantilla:

Cuando el terminal deba ser reemplazado por algún motivo, se actualizará el documento y se llevará igualmente a firma por parte del colaborador/a.

6. RENOVACIÓN DE TERMINALES

La renovación de terminales se realiza a criterio del Departamento de Tecnologías de la Información, bien porque el terminal ha dejado de cubrir las necesidades en cuanto a funcionalidad para el correcto desempeño del puesto, o bien porque el terminal se ha considerado irreparable desde el Servicio Técnico.

El terminal antiguo, salvo pacto expreso en contrario, se deberá devolver al Departamento de Tecnologías de la Información.

Como regla general, la sustitución por un terminal nuevo no tendrá lugar hasta la finalización del periodo establecido como vida útil del mismo. La empresa considera que la vida útil mínima de los dispositivos es la siguiente:

- Telefonía móvil: 2 años
- Tablet: 3 años
- Portátil: 4 años

7. MANTENIMIENTO DE LOS DISPOSITIVOS

El usuario es el responsable de los medios tecnológicos puestos a disposición por la empresa para el correcto desempeño de sus tareas. Por tanto quien debe garantizar el buen uso y la seguridad tanto del equipo como de la información que contiene.

Cuando el dispositivo deje de funcionar con normalidad, se informará al Dto. TI, quien se encargará de gestionar su reparación y hará entrega de un terminal de sustitución que cubra sus necesidades.

La empresa se hace cargo del coste de las reparaciones derivadas de un normal uso y desgaste del dispositivo. En caso contrario, si se considera que la reparación se debe a un uso indebido o negligente por el usuario, deberá ser a cargo de éste, en la manera que se determine por la Dirección e RRHH o Gestión de personas

8. DEVOLUCIÓN DEFINITIVA DE MEDIOS TECNOLÓGICOS

La devolución definitiva de los medios tecnológicos puestos a disposición del empleado/a se realizará:

- Cuando cese la relación contractual del empleado/a
- Cuando el empleado/a cambie de nivel o cargo y ello conlleve una reasignación de medios distintos.
- Cuando por sus actividades deje de requerirlo.
- Cuando finalice el periodo de teletrabajo acordado con la empresa

- Cuando así lo requiera la Organización por renovación contractual con proveedores tecnológicos o inadecuación de estos.

La devolución de cualquier dispositivo conlleva que éste sea devuelto con los mismos accesorios que fueron entregados, y que así constarán en el acta de entrega (cargadores, fundas, etc.). En caso contrario el usuario deberá responder en la manera que se determine por la Dirección e RRHH o Gestión de personas de la reintegración de su costo.

9. CONTRATACIÓN DE SERVICIOS EXTRAORDINARIOS

Los servicios de itinerancia (roaming) están por defecto deshabilitados, por lo que, en caso de necesitar activarse, se solicitan vía correo electrónico con copia al responsable inmediato o al Dpto. de TI, quien se encargará de dar de alta/baja el servicio. En el mail debe indicarse el rango de fechas de estancia en el extranjero, así como país de destino.

El resto de servicios no contratados a nivel corporativo por defecto (llamadas internacionales, desvíos, datos adicionales) deberán solicitarse con carácter excepcional al Superior inmediato o al Dpto. TI. Por mail.

10. USO DE DISPOSITIVOS MÓVILES NO CORPORATIVOS

La empresa permite al empleado/a utilizar sus propios dispositivos, teniendo en cuenta la siguiente regulación a fin de garantizar la seguridad de la información:

Bloqueo programado. Configuraremos el dispositivo para que se bloquee automáticamente tras un periodo de inactividad.

Desconexión wifi y Bluetooth. Se desactivará en el teléfono la búsqueda de redes wifi y de dispositivos vía Bluetooth cuando no sean necesarios.

Proceso de borrado de la información al extinguirse la relación contractual. El Dpto. de TI podrá realizar un borrado remoto de datos si así se precisa.

11. TRANSPORTE Y CUSTODIA

Los equipos no deben quedar expuesto a altas temperaturas que puedan dañar sus componentes.

El usuario debe impedir que se pueda acceder a la información almacenada en el mismo. En ningún caso se debe descuidar el portátil si se viaja en transporte público. Tampoco se ha de guardar en el coche ni dejarlo visible o fácilmente accesible.

Si se trabaja en lugares donde no se garantiza la custodia del equipo, este debe quedar anclado con un candado de seguridad o guardado en un armario de seguridad. En caso de robo o pérdida del equipo se debe notificar de manera inmediata al Dpto. TI.

12. MEDIDAS DE SEGURIDAD INFORMÁTICA

El empleado/a es el responsable de actuar con las debidas precauciones para evitar que personas no autorizadas, sean o no empleados/as de la empresa accedan a sus equipos informáticos.

Medidas:

1. **Contraseñas en dispositivos**

Utilización obligatoria en todo dispositivo tecnológico puesto a disposición del empleado/a, y en cualquier software o aplicación que contenga datos de la empresa.

El terminal debe tener activo el bloqueo automático de acceso con contraseña conocida únicamente por el usuario/a.

Cada empleado/a es responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá cambiarla y comunicarlo con la mayor brevedad posible al Dpto. de TI. A fin de garantizar la confidencialidad de las contraseñas, queda prohibido escribirla en cualquier tipo de soporte físico (papel) o lógico (archivos). Asimismo, deberá informar a la empresa de la contraseña de desbloqueo cuando ésta así lo decida.

2. **Acceso a internet /correo electrónico corporativo**

El acceso a internet/correo electrónico corporativo, está destinado a uso profesional. En este sentido el empleado/a conoce que se trata de un sistema monitorizado, pudiéndose auditar/limitar o anular su uso en casos justificados.

3. **Configuración de equipos**

Los equipos son entregados al empleado/a con los programas y aplicaciones acordes a la necesidad del propio puesto de trabajo. Si éste precisara de nuevas aplicaciones, antes de ser instaladas deberán ser conocidas y aprobadas por el Dpto. TI.

4. **Pérdida, sustracción o robo**

El empleado/a aplicará las medidas de seguridad que eviten la pérdida, hurto o robo de los equipos que la empresa le cede para realizar sus funciones.

En caso de pérdida, sustracción o robo, deberá comunicarlo de forma inmediata al responsable inmediato y al Dpto. TI, aportando la siguiente documentación:

- Denuncia Policial
- Informe vía mail de lo ocurrido

Para estos casos, los dispositivos móviles estarán dotados de un sistema de borrado remoto que el usuario tendrá que mantener activo mediante el procedimiento que la empresa designe.

5. Ficheros de trabajo

Los ficheros con información y datos de interés profesional han de ubicarse en las unidades de red donde tienen garantizado su mantenimiento y seguridad.

De trabajar con esos ficheros de manera temporal desde otras ubicaciones (escritorio, mis documentos, etc.), es obligado, finalizada la tarea, retornar el fichero a su ubicación en la unidad de red, eliminando cualquier copia de este.

7. Posibles incidencias

En caso de que el empleado/a detecte que se han borrado por error, avería del sistema informático u otra razón datos, ficheros, bases de datos, etc., deberá comunicarlo de inmediato al Dpto. TI para que se proceda, en la medida de lo posible, a recuperar la copia de seguridad más reciente y para, inmediatamente después, proceder a actualizar manualmente los datos que no estuvieran en dicha copia y se hubieran perdido.

El conocimiento de una incidencia que entrañe riesgo para la seguridad de los datos personales será comunicado al Dpto. TI con la mayor celeridad posible. Entre otras, son incidencias los olvidos o conocimientos por parte de usuarios no autorizados de las contraseñas, la creación de ficheros con datos de carácter personal no autorizados, la pérdida de los datos de un fichero o de los soportes que los contienen, la aparición de listados no controlados y cualquier incidencia que no permita acceder a los datos o que permita acceder a ellos de forma teóricamente no permitida, o a datos a los que no se debería tener acceso.

8. Permisos y accesos documentales

La obtención de permisos/accesos a carpetas ubicadas en los servidores centrales de la empresa requerirá la autorización expresa del Director/a Funcional o Responsable asignado por éste, de su área de trabajo.

13. ACTIVIDADES PROHIBIDAS

Está totalmente prohibida la instalación del cualquier software o aplicación que no haya sido previamente autorizada por la organización, así como la utilización de la cuenta de correo electrónico corporativa para fines ajenos a la actividad de la organización, la utilización de cualquier dato de la empresa considerado como Confidencial "en el "Deber de secreto y confidencialidad" del anexo, para su publicación, difusión y comunicación en páginas web, redes sociales de carácter privado y no corporativa.

Las medidas adoptadas para el uso de dispositivos digitales deberán ser facilitadas y firmadas por todos los empleados conforme al ANEXO 3.

II.- PROTOCOLO DE REGULACION DEL TELETRABAJO:

Conforme a la aplicación del Real Decreto-ley 28/2020, de 22 de septiembre (BOE 23-09-2020) que regula el trabajo a distancia y el teletrabajo se entiende por :

- **Trabajo a distancia** : la forma de organización del trabajo o de realización de la actividad laboral conforme a la cual esta se presta en el domicilio de la persona trabajadora o en el lugar elegido por esta, durante toda su jornada o parte de ella, con carácter regular, esto es aquel que se preste, en un periodo de referencia de tres meses, un mínimo del 30% de la jornada o el porcentaje proporcional equivalente en función de la duración del contrato de trabajo.

- **Teletrabajo:** aquel trabajo a distancia que se lleva a cabo de forma regular mediante el uso exclusivo o prevalente de medios y sistemas informáticos, telemáticos y de telecomunicación, desde el domicilio del trabajador o desde un espacio designado por la empresa, y sometido a las medidas organizativas de utilización de dispositivos y softwares de vigilancia y de registro de la jornada laboral.

Además de las medidas establecidas de forma genérica para la utilización de los dispositivos y software de la empresa, para aquellos trabajadores que realicen su trabajo mediante el teletrabajo se les informa de las siguientes obligaciones:

.- Obligación de mantener su deber de secreto y confidencialidad respecto a terceros ajenos a la empresa presentes en el domicilio

.- Obligación de cumplimentar el registro horario de jornada , incluyendo el momento de inicio y finalización de la jornada y los tramos de actividad.

.- Obligación de observar las medidas de vigilancia y control empresarial que implante la empresa en los dispositivos , incluidas de imagen y grabación del sonido en el lugar de trabajo , durante los tiempos de trabajo, y sin perjuicio de los derechos reconocidos a la desconexión digital.

.- Utilizar wifi privado y no público.

.- Tener activados programas antimalware, antivirus y firewall.

.- Autenticarse para acceder a los sistemas en remoto.

.- No descargar en local ficheros con datos de carácter personal.

.- Evitar la instalación de aplicaciones o la navegación por páginas no seguras.

.- Actualizar el sistema operativo y el software a las versiones más recientes.

.- Cerrar todas las conexiones con servidores y webs recurriendo a "cerrar sesión" o "desconectar".

.- Eliminar la información temporal en carpetas de descarga, papelera de reciclaje, etc.

.- Eliminar de sus dispositivos personales todos los datos a los que hubiera tenido acceso de forma legítima. No será posible conservar una copia aunque hubiera descargado la información en su equipo u otro dispositivo.

.- Borrar el historial de navegación, las cookies y otros datos, así como las contraseñas recordadas.

.- Notificar a la empresa cualquier brecha de seguridad que se pueda producir.

.- Bloquear la sesión de trabajo en ausencia del trabajador.

.- No imprimir información con datos de carácter personal.

Las compensaciones por los costes derivados del teletrabajo serán en su caso, establecidas en la negociación colectiva de la empresa

General Mills San Adrián S.L.U--

NORMAS DE USO DE LOS DISPOSITIVOS DIGITALES

1. Equipamiento informático y recursos

Con carácter general, en **GENERAL MILLS SAN ADRIAN S.L.U**. está prohibido utilizar para fines privados los recursos informáticos y telemáticos de la empresa, incluido Internet y el correo electrónico, pues su cometido es que se utilicen exclusivamente para actividades directamente relacionadas con el puesto de trabajo del usuario y con la cuenta de correo electrónico facilitada por la organización.

2. Actividades prohibidas

Está totalmente prohibida la instalación del cualquier software o aplicación que no haya sido previamente autorizada por la organización, así como la utilización de la cuenta de correo electrónico corporativa para fines ajenos a la actividad de la organización.

3. Dispositivos portátiles y móviles

Los dispositivos portátiles y móviles (como ordenadores, tabletas, teléfonos, etc.) que la organización pone a disposición de sus empleados y que, eventualmente, pueden utilizarse fuera de sus instalaciones, podrán ser utilizados por los usuarios para uso privado exclusivamente fuera de horas laborales, con las limitaciones establecidas en el punto anterior.

En caso de que el usuario utilice los dispositivos digitales para uso privado, se recomienda que no almacene información personal propia en dicho dispositivo (como documentos privados, fotografías, etc.), pues puede ser objeto de las revisiones establecidas en el punto siguiente.

4. Acceso al contenido de los dispositivos digitales

Tal y como establece el artículo 87 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, la organización podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

En este sentido, la organización se reserva la posibilidad de adoptar las medidas que estime más oportunas de vigilancia y control, como son las revisiones de los dispositivos proporcionados o del servidor de correo electrónico, los recursos utilizados o las conexiones a Internet realizadas, entre otras, para verificar el cumplimiento, por parte del trabajador, de sus obligaciones y deberes laborales, con los límites establecidos por la Ley y la jurisprudencia.