

PLAN DE CONCILIACIÓN LABORAL Y FAMILIAR

**PROTOCOLO ADOPTADO POR LAS SOCIAS DE ARNAIZ 4.0.
A.I.E. PARA LA IMPLANTACIÓN DE LA MODALIDAD DE TRABAJO
A DISTANCIA (“TELETRABAJO”)**

Contenido

1. MOTIVOS Y CONVENIENCIA DEL PLAN	4
1.1. ANTECEDENTES.....	4
1.2. MARCO NORMATIVO.....	4
1.3. OPORTUNIDAD DE SU IMPLANTACIÓN	5
2. PLAN DE ETAPAS.....	6
3. MEDIOS TECNOLOGICOS.....	7
4. RELACIONES LABORALES	7
5. POLÍTICA DE MEDIOS Y SEGURIDAD	8
6. CONFIDENCIALIDAD	10
7. IMPLANTACION.....	10
8. CONSOLIDACION, SEGUIMIENTO Y MEJORAS DEL SISTEMA.....	11
ANEJOS.....	12
ANEJO I Y II DE SEGURIDAD INFORMATICA.	12
ANEJO AL CONTRATO DE TRABAJO EN EL QUE SE RECABA DE CADA TRABAJADOR LA ACREDITACION DE CONOCER Y ASUMIR LAS RECOMENDAIONES Y NORMAS DE SEGURIDAD CONTENIDAS EN EL ANEJO ANTERIOR DENOMINADO “ANEJO I Y II DE SEGURIDAD INFORMATICA”.	15

1. MOTIVOS Y CONVENIENCIA DEL PLAN

1.1. ANTECEDENTES

Con independencia de que ARNAIZ 4.0. A.I.E. es una agrupación de empresas muy permeables e innovadoras en cuanto al uso de las tecnologías, la situación de la pandemia COVID ha supuesto, además de un escenario contextual convulso, un entorno de nuevas experiencias -forzosa muchas de ellas- en el que ha tenido una presencia destacada el vulgarmente denominado teletrabajo.

Así, y durante al menos 6 meses de forma continua, la plantilla laboral y los colaboradores externos asociados a alguno o algunos de los proyectos desarrollados por las socias de ARNAIZ 4.0. A.I.E. se han visto abocados a la prestación a distancia de su cometido profesional.

El “reverso de la moneda” es el esfuerzo tecnológico y de medios materiales que las agrupadas han tenido que realizar en muy pocos días para no interrumpir el curso de sus trabajos y encargos con el objeto de dar cumplimiento a las obligaciones contractuales previamente concertadas.

La experiencia “accidental” de ese trabajo a distancia durante la pandemia arraigó en la cultura de las socias de tal manera que hoy en día es un uso común y cotidiano de las TIC’s al servicio del teletrabajo.

1.2. MARCO NORMATIVO

Como se intuye de lo dicho en el epígrafe anterior, la norma interna, se ha ido haciendo sobre la marcha y a medida que las condiciones del confinamiento y las circunstancias de la pandemia han ido evolucionando. Con todo y con ello, los orígenes normativos de esta modalidad no presencial de prestación laboral no son nuevos ni nacen con la COVID-19. Este es el marco regulatorio:

•Normativa de ámbito europeo:

✎ Acuerdo Marco Europeo sobre Teletrabajo, los agentes sociales (CES, UNICE/UEAPME y CEEP) han firmado el Acuerdo Marco Europeo sobre Teletrabajo, de 16 de julio de 2002.

•Normativa de ámbito estatal:

✎ Ley 10/2021, de 9 de julio, de trabajo a distancia.

✎ Real Decreto Ley 29/2020, de 29 de septiembre, de medidas urgentes en materia de teletrabajo en las Administraciones Públicas y de recursos humanos en el Sistema Nacional de Salud para hacer frente a la crisis sanitaria por la COVID-19.

✎ Real Decreto Ley 28/2020, de 22 de septiembre, del trabajo a distancia.

✎ Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

✎ RDL 8/2015, de 30 de octubre, por el que se aprueba el Texto Refundido de la Ley General de la Seguridad Social.

✎ Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el Texto Refundido de la Ley del Estatuto Básico del Empleado Público.

✎ Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el Texto Refundido de la Ley del Estatuto de los Trabajadores.

✎ Real Decreto Ley 3/2012, de 10 de febrero, de medidas urgentes para la reforma del mercado laboral (el artículo 6 modifica el artículo 13 del TRET).

- Real Decreto 1215/1997, de 18 de julio, por el que se establecen las disposiciones mínimas de seguridad y salud para la utilización de los equipos de trabajo por parte de los trabajadores.

- Real Decreto 486/1997, de 14 de abril, por el que se establecen las disposiciones mínimas de seguridad y salud en los puestos de trabajo.

- Real Decreto 488/1997, de 14 de abril, por el que se establecen las disposiciones mínimas de seguridad y salud relativas al trabajo con equipos que incluyen pantallas de visualización.

- Real Decreto 39/1997, de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención.

- Ley 31/1995, de 8 de noviembre, de prevención de riesgos laborales.

Todo ello, sin perder de vista que el artículo 13 del Estatuto de los trabajadores (Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores) ya tenía prevista esta modalidad de prestación, aunque en aquel momento esa posibilidad pareciese un modelo de relación un tanto pintoresco y circunscrito casi en exclusiva al ámbito de las nuevas tecnologías o a determinadas profesiones liberales.

1.3. OPORTUNIDAD DE SU IMPLANTACIÓN

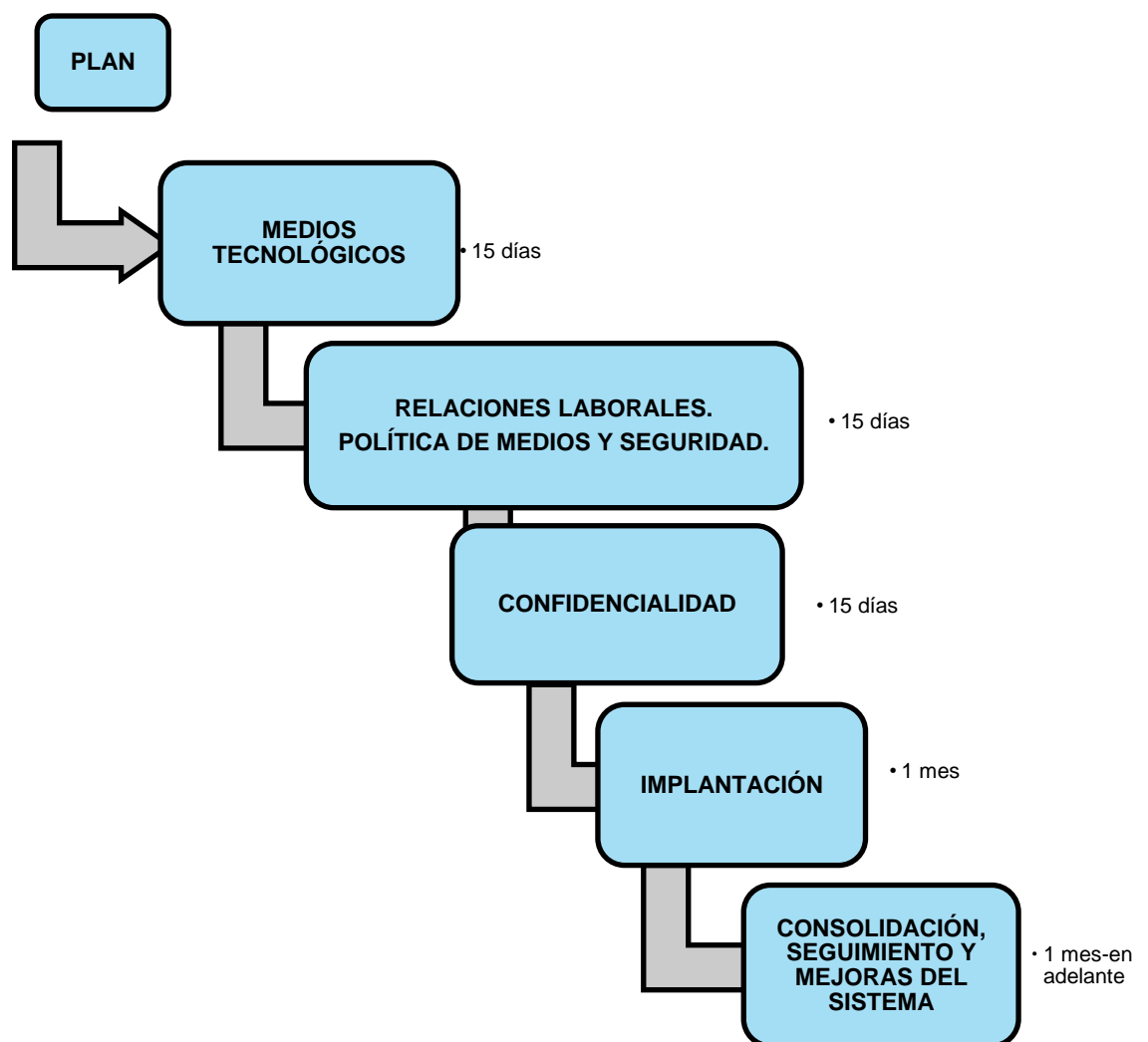
Con los antecedentes y régimen jurídico antes apuntado, parece lógico que, las socias de ARNAIZ 4.0. A.I.E. consoliden de una forma estructurante lo que en su momento resultó ser una experiencia puntual y transitoria que, sin embargo, la realidad demuestra que se ha convertido en una modalidad más de prestación laboral.

Y ello unido a la filosofía fuertemente sensibilizada con el criterio de conciliación de la vida familiar y laboral, así como con la salud laboral, tienen como fruto este plan que expresa las normas y criterios que definitivamente regulen la implantación y mantenimiento de la modalidad de prestación del trabajo a distancia.

2. PLAN DE ETAPAS

El plan de etapas previsto debe conciliar no solo los requerimientos tecnológicos sino, especialmente, el grado de afectación de los recursos humanos y la calidad y cantidad de la producción.

En tal sentido, el esquema de implantación de este “Plan de teletrabajo” se llevará a término en las siguientes etapas:



Todo lo anterior con el detalle y alcance que se contiene en los epígrafes que siguen.

3. MEDIOS TECNOLOGICOS

En el plazo de dos semanas desde la suscripción de este Plan, se obtendrá de la empresa proveedora de servicios informáticos, un informe-auditoria en el que se contraste la suficiencia de la infraestructura material actual, de las herramientas y materiales disponibles, de las aplicaciones de telecomunicación y de la suficiencia de todo lo anterior para el mantenimiento de una prestación laboral “a distancia” en las actuales condiciones.

El informe, deberá indicar las deficiencias materiales y, en su caso, plantear y cifrar el coste de las medidas y medios complementarios necesarios para la puesta en marcha del sistema de teletrabajo en estándares de eficiencia y sin menoscabo de los umbrales de producción actuales.

4. RELACIONES LABORALES

Durante los primeros dos meses de 2022 y siguiendo con el calendario de etapas del Plan, se informará a los trabajadores de las socias de ARNAIZ 4.0. A.I.E., de los requisitos de la modalidad de prestación laboral a distancia.

En paralelo, se elaborarán los documentos contractuales para formalizar la nueva relación laboral.

Los modelos de contrato plantearán un sistema mixto de prestación (presencial/no presencial) para su correspondiente negociación. Las cuotas de trabajo presencial y no presencial no serán, en ambos casos, nunca inferiores al 10%.

Se desarrollará una labor didáctica relacionada con condiciones de la prestación, derecho a la desconexión, política tecnológica, política de medios y seguridad y salud en los puestos individuales a distancia.

A partir de la segunda quincena del mes en el que comience a informarse de los requisitos, se llevará a cabo la redacción y suscripción de contratos laborales ad hoc.

En la última quincena del mes en que arranque el plan, se darán instrucciones y se facilitarán los formularios y normas que rigen la seguridad y salud del “puesto a distancia” (auto plan de seguridad y salud individual).

5. POLÍTICA DE MEDIOS Y SEGURIDAD

Esta política se aplica a todos los trabajadores, estableciendo los requerimientos para acceder a cualquier plataforma proporcionada por los proveedores de servicios informáticos de las socias de ARNAIZ 4.0. A.I.E., así como de los canales de esta última.

Cualquier trabajador que contravenga esta política podrá, según las circunstancias, ser remitido a los servicios jurídicos, pudiéndose aplicar las medidas legales oportunas.

El trabajador debe actuar legalmente en todo momento, ejerciendo un buen uso de la información, dispositivos y tecnología, es responsable de comunicar con prontitud cualquier anomalía, sospecha o errata ocurrida durante su uso. Se prohíben los siguientes comportamientos:

- Cualquier acción que viole las políticas de las entidades agrupadas.
- Acceso a información, dispositivos o tecnología con fines ilegales, como violar las leyes de derecho de autor, ganancia de capitales o su uso con fines de minería de moneda digital.
- Acceder, descargar, almacenar o distribuir materiales pornográficos, obscenos, difamatorios, discriminatorios y cualquier otro material inapropiado.
- Adquirir o utilizar tecnología de terceros, incluidos servicios en la nube que no han sido proporcionados por las entidades agrupadas.
- Realización de evaluaciones de vulneraciones no autorizadas o pruebas de penetración contra los elementos proporcionados por las entidades agrupadas.
- Desinstalar, deshabilitar o eludir software de seguridad implementado.
- Permitir acceso a los dispositivos, información o tecnología a cualquier Colaborador, salvo por resolución de incidencia.
- Poner en peligro la reputación de las entidades agrupadas, acosar a personas mediante la transmisión de mensajes pudiéndose considerar calumniosos, amenazantes, abusivos o inapropiados.
- El trabajador, es el único responsable del equipamiento, plataforma y cuentas asignadas por las entidades agrupadas.
- Es obligatorio el uso de software original.
- Se recomienda la configuración de sistemas Firewall y antivirus que serán suministrados por la empresa proveedora de servicios tecnológicos.
- Se recomienda el uso de claves complejas en el acceso a los dispositivos.
- El trabajador debe utilizar identificaciones únicas y autenticación de múltiple factor en la medida de lo posible. Dichas contraseñas e identificaciones son personales e intransferibles. Las contraseñas deben cumplir los valores mínimos de complejidad, una longitud mínima de 8 caracteres y debe contener, mayúsculas, minúsculas, números y signos. Las contraseñas se deben cambiar siempre que exista sospecha de que se encuentre comprometida. No se deben utilizar las mismas contraseñas en servicios personales y servicios dentro de las plataformas o canales de las entidades agrupadas.
- Los equipos móviles deben encontrarse en todo momento vigilados. Se debe activar la opción buscar/localizar, para, en caso de pérdida, poder ser localizado.
- Se deben bloquear las sesiones cuando el trabajador deje de utilizar el equipamiento o se mueva a otra ubicación.
- El trabajador debe actuar como custodio de la información.

- El uso y la difusión de la información debe limitarse y cumplir con la responsabilidad legal establecida.
- Se limita el uso de almacenamiento al proporcionado por las entidades agrupadas como almacenamiento seguro.
- La utilización de dispositivos de almacenamiento externo se debe regir únicamente por las entregas de proyecto que lo requieran y siempre será custodiado por el responsable hasta su entrega.
- El uso de información en papel se limitará a entregas de proyectos o bien cuando por razones de actividad así lo requiera, siendo destruido y “NO ALMACENADO” una vez finalizado su uso.
- Los documentos no deben dejarse desatendidos o visibles ni en impresoras, fax, plotter, etc..., ni en puestos de trabajo o lugares públicos.
- Toda la documentación generada en las diferentes plataformas y almacenado fuera de lo establecido, es de propiedad de las entidades agrupadas.
- El trabajador debe informar de inmediato de los incidentes tecnológicos o de seguridad utilizando la cuenta de correo **support@servigesbox.es** proporcionada por el proveedor de tecnología autorizado.

Se adjunta al presente Plan dos anejos correspondientes a la política de medios y seguridad:

- Anejo I y II de Seguridad Informática.
- Anejo al contrato de trabajo en el que se recaba de cada trabajador la acreditación de conocer y asumir las recomendaciones y normas de seguridad contenidas en el anejo anterior denominado “Anejo I y II de Seguridad Informática”.

6. CONFIDENCIALIDAD

La información total o parcial con la que el trabajador entre en contacto por razón del desempeño de su actividad laboral podrá tener tanto el formato de datos que conformen el repositorio documental alojado en plataformas colaborativas a las que se abra acceso, como contenidos de correos electrónicos, pero también aquella otra información oral o escrita a la que tenga acceso al margen de los medios informáticos.

El trabajador únicamente utilizará la información a la que ha accedido para los fines propios de desarrollo de su actividad laboral, comprometiéndose a mantener la más estricta confidencialidad y secreto respecto de dicha información, advirtiendo de dicho deber de confidencialidad y secreto a sus empleados, asociados, subcontratados y a cualquier persona implicada directa o indirectamente en su actividad laboral y sobre la que ejerza algún grado de influencia o tenga punto de conexión laboral o mercantil.

El trabajador se compromete a no usar para sí, ni revelar a terceros todo o parte de los contenidos de los archivos de datos ni ningún otro tipo de información a la que hubiese tenido acceso en el desempeño de su tarea; lo que incluye también el secreto sobre identidades de personas físicas o jurídicas; datos económicos; ubicaciones; mediciones y características técnicas. Se compromete a su vez a no revelar la identidad de los asistentes a reuniones presenciales o virtuales ni los contactos tanto del primero, como del resto de implicados en el proyecto.

El trabajador no podrá reproducir, copiar, modificar, hacer pública o divulgar a terceros dicha información.

El trabajador adoptará respecto de dicha información las mismas medidas de seguridad que adoptaría normalmente respecto a la información confidencial de su propia Empresa, evitando en la medida de lo posible su pérdida, robo o sustracción.

En caso de que la información resulte revelada o divulgada o utilizada por el trabajador de cualquier forma, ya sea de forma dolosa o por mera negligencia, supondrá una práctica contraria a las obligaciones laborales concertadas que habilitarán a la dirección de la empresa al ejercicio de acciones judiciales, en su caso.

7. IMPLANTACION

Según el plan de etapas descrito en el epígrafe segundo, durante el mes siguiente al de adopción de este plan se habrán culminado los siguientes hitos necesarios para la puesta en marcha del sistema de trabajo a distancia:

- Acciones de información y divulgación sobre el nuevo sistema.
- Negociación de contratos laborales.
- Suscripción de contratos y formalización de documentación complementaria.
- Entrega de material informático y apertura de red y repositorios documentales informáticos.
- Entrega de escritorios virtuales y de aplicaciones informáticas.
- Entrega de elementos periféricos cuando fuesen requeridos,
- Divulgación y formación en materia de directivas de seguridad y privacidad en el uso de TIC's.

8. CONSOLIDACION, SEGUIMIENTO Y MEJORAS DEL SISTEMA

A partir del mes siguiente al de la definitiva implantación, se inicia una nueva etapa en la que la realidad del trabajo a distancia sea, por así decirlo, una experiencia común y cotidiana.

Es a partir de este momento, el periodo en la que podrán detectarse las carencias y/o suficiencia del modelo al que se refieren los epígrafes anteriores.

Por este motivo, es voluntad de las direcciones de las entidades agrupadas, coordinar los servicios externalizados de recursos humanos y de medios informáticos para que, a lo largo del primer semestre a partir de la entrada en vigor de este plan, se realice un informe sobre carencias y debilidades técnicas del sistema. También será el momento en el que se puedan evaluar los estándares de productividad alcanzados tanto global como individualmente para, en su caso, redefinir los contornos del modelo de prestación.

Ese informe deberá contener a su vez propuestas de mejora y/o de aquellos cambios que aconseje la experiencia vivida, así como, en su caso, las modificaciones que aquellos aconsejen en la vigencia de este plan.

De esta forma, este Plan estará sujeto a revisiones, por lo que sus postulados actuales no pueden considerarse inamovibles.

Las entidades agrupadas de ARNAIZ 4.0. A.I.E.

En Madrid a 03 de enero de 2022.

ANEJOS

ANEJO I Y II DE SEGURIDAD INFORMÁTICA.

ANEJO I

RECOMENDACIONES DE ACCESO Y PAUTAS PARA LA CORRECTA CONSERVACIÓN, MANTENIMIENTO Y BUEN USO DE LA PLATAFORMA 365.

- Se debe evitar la duplicidad de archivos e información, con el objetivo de no cargar el sistema innecesariamente.
- Se deben cerrar todas las conexiones que no sean estrictamente necesarias.
- Se deben cerrar todas las aplicaciones cuando no se estén utilizando.
- Toda información incompleta, obsoleta o en desuso debe ser suprimida y no distribuida para no sobrecargar el sistema.
- Se ha de limpiar continuamente el buzón de correo electrónico con el fin de mantener espacio disponible para la recepción de nuevos mensajes.
- Se han de seguir las instrucciones marcadas por LA EMPRESA PROVEEDORA DE SERVICIOS INFORMÁTICOS para la correcta actualización del sistema y funcionamiento del mismo. Entre las instrucciones podemos encontrar el correcto apagado y encendido de los equipos o la realización de un análisis de antivirus.

ANEJO II

DIRECTRICES Y PROTOCOLOS DE SEGURIDAD DE EQUIPOS Y RECURSOS TECNOLÓGICOS

- No se ha de hacer uso del autoguardado de contraseñas. Tras finalizar el acceso a cualquier navegador, ha de ser eliminado el historial.
Las claves de acceso y contraseñas de carácter personal y/o corporativo han de ser almacenadas o guardadas en un lugar seguro de difícil acceso por terceros, jamás en lugares visibles como escritorios.
- Tras la finalización de la jornada laboral se ha de cerrar la sesión correctamente, previo cierre de todas las conexiones y; por último, se ha de realizar el apagado del equipo, incluidas las pantallas para evitar ingresos no autorizados.
- No dar nunca datos personales a menos que se esté seguro de quién los solicita.
- Disponer de más de una cuenta de correo, estando muy diferenciadas las de trabajo con la personal.
- Rechazar los correos spam y no abrir nunca los ficheros desconocidos y notificar la existencia de los mismos.
- Las contraseñas se deben cambiar frecuentemente y alternar mayúsculas, minúsculas y números e inmediatamente desde que se sospeche que las mismas hubiesen sido descubiertas o involuntariamente reveladas.
- Evitar el acceso a webs no oficiales cuya única misión es copiar los datos personales y financieros para posibles estafas.
- No se deben compartir las contraseñas con nadie.
- Los usuarios son responsables de todas las actividades llevadas a cabo con su usuario.
- Los sistemas informáticos puestos a disposición del usuario deben emplearse exclusivamente para asuntos relacionados con la actividad laboral y el correcto desempeño de las funciones inherentes al puesto de trabajo.
- Los equipos y herramientas informáticos suministrados no deben ser alterados en ninguna forma: tanto en su configuración software como hardware.
- Los empleados, colaboradores o terceros de la sociedad deben comunicar inmediatamente a la sociedad LA EMPRESA PROVEEDORA DE SERVICIOS INFORMÁTICOS cualquier daño o pérdida del equipo, software o información; así como cualquier violación de seguridad o sospecha de la misma.
- Se permite el uso personal ocasional de los sistemas, herramientas y equipos, siempre y cuando dicho uso no suponga un problema de seguridad o legalidad.
- Si se detecta un virus informático, debe notificarse inmediatamente a LA EMPRESA PROVEEDORA DE SERVICIOS INFORMÁTICOS para que informe al resto de usuarios de la red.
- No se debe fumar, comer y beber cerca de los equipos informáticos.
- No se permite copiar, transferir o divulgar software proporcionado por la sociedad LA EMPRESA PROVEEDORA DE SERVICIOS INFORMÁTICOS en ningún medio de almacenamiento magnético o sistema de comunicación.

- No se permite adquirir, poseer, comercializar o usar herramientas de hardware o software que pudieran emplearse para evaluar o comprometer la seguridad de los sistemas de información.
- La sociedad LA EMPRESA PROVEEDORA DE SERVICIOS INFORMÁTICOS se reserva el derecho de examinar todos los datos guardados y comunicaciones transmitidos en o por sus sistemas a los efectos de auditar el entorno o aplicar directivas de seguridad.
- Las conexiones a redes externas de tiempo real deben pasar siempre por un punto adicional de control como firewall o VPN y deben ser siempre previamente aprobados por LA EMPRESA PROVEEDORA DE SERVICIOS INFORMÁTICOS, con el fin de no comprometer la seguridad interna de la información de la Empresa. LA EMPRESA PROVEEDORA DE SERVICIOS INFORMÁTICOS se reserva el derecho de cancelar y terminar la conexión a sistemas que no cumplan con los requerimientos internos de seguridad.
- En lo que se refiere al teletrabajo, se debe asegurar un entorno de seguridad física e informática para los recursos informáticos de LA EMPRESA PROVEEDORA DE SERVICIOS INFORMÁTICOS. Se ha de priorizar la seguridad de la propiedad de LA EMPRESA PROVEEDORA DE SERVICIOS INFORMÁTICOS para evitar robos, daños y/o mal uso a los equipos, el software y de la información.
- Se aconseja por motivos de seguridad la no difusión y divulgación de datos e información de carácter sensible y confidencial.
- Se ha de realizar un uso racional del acceso a Internet. Se ha de evitar el acceso a páginas de internet que no estén relacionadas con las funciones y responsabilidades laborales. Se ha de evitar la descarga de contenido innecesario de Internet (o cualquier otra red pública).
- Los usuarios deben mantener debidamente organizada la información almacenada en la nube, no debiendo ser almacenada en el Escritorio de Windows, ni en ninguna de las carpetas estándar de Windows ("imágenes, documentos, música, video", etc.). Se ha de evitar el almacenamiento de información sensible en sitios públicos gratuitos como son por ejemplo Dropbox, box, Google Drive, Onedrive, etc... Solo pueden ser utilizados los sitios públicos corporativos en la nube que han sido autorizados y puestos a disposición del usuario previamente por LA EMPRESA PROVEEDORA DE SERVICIOS INFORMÁTICOS.

ANEJO AL CONTRATO DE TRABAJO EN EL QUE SE RECABA DE CADA TRABAJADOR LA ACREDITACION DE CONOCER Y ASUMIR LAS RECOMENDACIONES Y NORMAS DE SEGURIDAD CONTENIDAS EN EL ANEJO ANTERIOR DENOMINADO “ANEJO I Y II DE SEGURIDAD INFORMATICA”.

ANEXO AL CONTRATO DE TRABAJO.

Don, _____ con DNI. _____, trabajador, de la empresa . _____, que suscribe al pie, por el presente escrito MANIFIESTA:

I.- Que ha recibido de su empleadora herramientas tecnológicas para el desempeño de sus prestaciones laborales.

II.- Que conoce el contenido de los “Anejos I y II” adoptados por la empresa empleadora por recomendación de la entidad proveedora de servicios informáticos que se unen al presente documento y se compromete a cumplir las directivas de seguridad que allí constan.

Y para que así conste y sirva de Anexo al Contrato Laboral en su día suscrito, firma el presente en Madrid a _____ de xxxxxxxx de 2022.

Fdo. _____