Normativa de teletrabajo

Contenido

Fecha	Edición	Revisión	Usuario	Cambios Realizados
17/03/2020	1	0	Govertis y Fernando Gallego	Versión inicial.

1. Objeto

El objeto del presente documento es regular el trabajo del personal del Ayuntamiento de Mislata cuando desarrolle su actividad profesional en modalidad de teletrabajo.

Se ha implantado la siguiente normativa atendiendo al nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas del Ayuntamiento de Mislata, que resulten de la aplicación de las previsiones contempladas en los Anexos I y II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).

El artículo 13 del Estatuto de los Trabajadores recoge la figura del teletrabajo como trabajo a distancia, en los siguientes términos:

<<***1. Tendrá la consideración de trabajo a distancia aquel en que la prestación de la actividad laboral se realice de manera preponderante en el domicilio del trabajador o en el lugar libremente elegido por este, de modo alternativo a su desarrollo presencial en el centro de trabajo de la empresa.***

2. Ámbito de aplicación

Esta normativa es de aplicación a todo el ámbito de actuación del Ayuntamiento de Mislata, y sus contenidos traen causa de las directrices de carácter más general definidas en el ordenamiento jurídico vigente, en la Política de Seguridad de la Información y en las Normas de Seguridad del Ayuntamiento de Mislata.

La presente normativa es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en el Ayuntamiento de Mislata, especialmente, el Responsable de Seguridad, los responsables de Sistemas de Información y los propios usuarios, como actores en sus respectivas competencias, de la especificación de la normativa de control de acceso, de la implantación técnica de dicha normativa, y del cumplimiento de la misma.

En el ámbito de la presente normativa, se entiende por usuario cualquier empleado público perteneciente o ajeno al Ayuntamiento de Mislata, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con el Ayuntamiento de Mislata y que utilice o posea acceso a sus Sistemas de Información.

3. Actualización del documento

Cuando se produzca un cambio significativo en la estructura o en la operativa del Ayuntamiento de Mislata que afecte a esta normativa, deberá producirse una modificación y actualización del mismo.

Se levantará acta de los cambios y modificaciones identificados, y éstos serán incluidos en una nueva versión del documento, así como en el apartado de control de cambios, como evidencia del proceso de actualización realizado y para mantener la trazabilidad entre distintas versiones.

Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

4. Referencias

Las referencias tenidas en cuenta para la redacción de esta normativa han sido:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD), en vigor desde el 24 de mayo de 2016 pero no será aplicable hasta el 25 de mayo de 2018.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- UNE-ISO/IEC 27001:2013 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.
- ISO/IEC 9001:2015 Sistemas de gestión de la calidad.
- Documentos y Guías CCN-STIC.
- 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

5. Roles y Responsabilidades

- El Responsable de la Seguridad de la Información es el encargado de definir la normativa para teletrabajar y velar por su cumplimiento.
- El Responsable del Sistema recomendará al Responsable de la Seguridad de la Información todas aquellas cuestiones que deben considerarse para acceder remotamente a sistemas concretos.
- Los usuarios tienen la responsabilidad de cumplir con la normativa en los casos en que les aplique.

6. Normas previas

La presente Normativa para teletrabajar, complementa en sus aspectos específicos, a las Normas de uso del Sistema de Información, por lo que tal normativa general será de aplicación en los aspectos no señalados en aquella.

7. Normativa

El trabajo fuera de las instalaciones del Ayuntamiento de Mislata comprende tanto el teletrabajo habitual y permanente de los usuarios desplazados, como el trabajo ocasional, usando en ambos casos, dispositivos de computación y comunicación (usualmente: ordenador portátil, Tablet, teléfono móvil, etc.). Este modo de trabajo comprende también las conexiones remotas realizadas desde Congresos o sesiones de formación, alojamientos o, incluso, llamadas telefónicas de contenido profesional que sean realizadas o atendidas en áreas públicas.

El teletrabajo conlleva el riesgo de trabajar en lugares desprotegidos, esto es, sin las barreras de seguridad físicas y lógicas implementadas en las instalaciones del Ayuntamiento de Mislata. Fuera de este perímetro de seguridad aumentan las vulnerabilidades y la probabilidad de materialización de las amenazas, lo que hace necesario adoptar medidas de seguridad adicionales.

Se incluyen seguidamente un conjunto de normas de obligado cumplimiento, que tienen como objetivo el reducir el riesgo cuando se realiza teletrabajo.

- **Uso personal y profesional**. Los dispositivos móviles de computación y comunicación asignados al usuario del Ayuntamiento de Mislata, son para su uso exclusivo y solamente pueden ser utilizados para fines profesionales. No pueden prestarse a terceros salvo autorización expresa, que incluirá en todo caso la definición de las condiciones de uso.
- **Necesidad de autorización**. La salida fuera de las dependencias del Ayuntamiento de Mislata de documentación, equipos y dispositivos informáticos y de comunicaciones precisa autorización previa del Responsable de la Información.
  Asimismo, es necesaria la correspondiente autorización para utilizar equipos personales del usuario en el tratamiento de la información de la organización o en el acceso a recursos o sistemas de información del Ayuntamiento de Mislata.
- **Copias de seguridad**. En el supuesto de almacenar localmente información en los dispositivos móviles, regularmente, debe realizarse copia de seguridad de la información contenida, siguiendo en cualquier caso las indicaciones del departamento de informática. Análogamente, es necesario adoptar las medidas adecuadas para la protección de dichas copias.
- **Uso de los canales de comunicación establecidos**. La transmisión de información y el acceso remoto se realizará únicamente a través de los canales establecidos, siguiendo los procedimientos y requisitos definidos para ello y adoptando las siguientes precauciones:
  - En caso de utilizar contraseñas en la autenticación, estas deben ser robustas.
  - Cerrar siempre la sesión al terminar el trabajo y al ausentarse del lugar en el que se está desarrollando el mismo.
  - Cifrar la información sensible, confidencial o protegida que vaya a ser transmitida a través de correo electrónico o cualquier otro canal que no proporcione la confidencialidad adecuada.
- **Vigilancia permanente**. La documentación y los dispositivos móviles facilitados por la organización deben estar vigilados y bajo control para evitar extravíos o hurtos que comprometan la información almacenada en ellos o que pueda extraerse de ellos. En los desplazamientos en avión, este tipo de equipamiento no debe facturarse y deberá viajar siempre con el usuario.
- **Evitar el acceso no autorizado**. El teletrabajo debe realizarse con la mayor cautela y precaución, evitando que personas no autorizadas vean o escuchen información interna a la organización.
- En relación con el **acceso remoto (vía web)**, deben adoptarse las siguientes cautelas:
  - Los navegadores utilizados para el acceso vía web deben estar permanentemente actualizados a su última versión, al menos en cuanto a parches de seguridad, así como correctamente configurados.

- Una vez finalizada la sesión web, es obligatoria la desconexión con el servidor mediante un proceso que elimine la posibilidad de reutilización de la sesión cerrada.
- Desactivar las características de recordar contraseñas en el navegador.
- Activar la opción de borrado automático al cierre del navegador, de la información sensible registrada por el mismo: histórico de navegación, descargas, formularios, caché, cookies, contraseñas, sesiones autenticadas, etc.
- Salvo autorización expresa, está prohibida la instalación de ***addons*** para el navegador.

- **Transporte seguro**. La documentación y equipos que salgan de las instalaciones del Ayuntamiento de Mislata se deberá transportar de manera segura, evitando proporcionar información sobre el contenido de los mismos y utilizando, en su caso, maletines de seguridad que eviten el acceso no autorizado.
- **Mantenimiento de los equipos**. Los equipos se mantendrán de acuerdo a las especificaciones técnicas de uso, almacenamiento, transporte, etc., proporcionadas por el fabricante. El particular, se evitará su uso en condiciones de temperatura o humedad inadecuadas, o en entornos que lo desaconsejen (mesas con alimentos y líquidos, entornos sucios, etc.).
- **Entorno de trabajo seguro**: Los usuarios se asegurarán de disponer de un entorno de trabajo lo más seguro posible, normalmente en sus domicilios particulares.
- **Normativa interna**. Durante la actividad profesional en modalidad Teletrabajo se seguirán las normas, procedimientos y recomendaciones internas existentes, atendiendo de manera especial a las siguientes:
  - Las contraseñas deberán ser robustas y renovarse periódicamente o cuando se sospeche que pueden estar comprometidas.
  - El almacenamiento de información en soportes electrónicos (CDs, DVDs, memorias USB, etc.), debe caracterizarse por no ser accesible para usuarios no autorizados. Para ello, es necesario aplicar claves de acceso o algoritmos de cifrado cuando la naturaleza de la información así lo aconseje.
  - No desactivar las herramientas de seguridad habilitadas en los dispositivos móviles (ordenadores portátiles, móviles, tablets, etc.) y comprobar que se mantienen actualizadas.
  - No descargar ni instalar contenidos no autorizados en los equipos (tonos de teléfono, aplicaciones para tablets o móviles, etc.).
  - Comunicar cualquier incidencia con la mayor rapidez que sea posible a través del procedimiento de notificación de incidencias.

8. Medidas de Seguridad

El Instituto Nacional de Ciberseguridad (INCIBE) recomienda que tanto los dispositivos móviles personales para uso profesional como el equipamiento que el Ayuntamiento de Mislata haya podido ofrecer al usuario para el Teletrabajo, deben estar protegidos convenientemente, estableciendo unas buenas medidas de seguridad que ayuden a reducir todo lo posible los riesgos a los están expuestos.

A continuación, se detallan algunas medidas que deben tenerse en cuenta para mitigar los riesgos a los que nos enfrentamos. Medidas como:

- La debida protección de la información
- La correcta configuración de los dispositivos o
- La protección de la conexión a redes inalámbricas.

8.1. La protección de la información

Los dispositivos móviles, y la información a la que acceden, tienen un gran riesgo de verse comprometidos. Ya sea por pérdida, robo o por cualquier otro motivo, la confidencialidad de la información se puede ver afectada al ser accedida por personas ajenas a la organización. Para evitar el acceso de personal no autorizado a la información de estos dispositivos, se debe hacer uso de un sistema de cifrado de la información.

Con el sistema de cifrado, transformamos la información de tal forma que solamente aquellas personas que estén autorizadas puedan leerla o manipularla. Ciframos la información con un algoritmo de cifrado y una contraseña que la hace ilegible para todo el que no conozca dicha contraseña.

Todos los sistemas actuales permiten habilitar opciones de cifrado de datos y dispositivos mediante contraseñas de acceso o a nivel de arranque. Desde el Ayuntamiento de Mislata se proporcionarán los mecanismos de cifrado para su uso.

8.2. Configuración de los dispositivos

Podemos minimizar los riesgos derivados del robo de las credenciales de acceso o de la desaparición de los dispositivos, tomando una serie de medidas técnicas que aseguren la integridad de los dispositivos y la confidencialidad de las comunicaciones. Para ello, configuraremos los terminales con una serie de funcionalidades que nos ayudarán a mantener la confidencialidad de la información corporativa que contienen.

8.2.1. Medidas técnicas de configuración

Configuraremos los dispositivos con las medidas técnicas que nos ayuden a proteger los datos. Algunas de estas medidas son:

- Habilitar sistemas de autenticación robustos, apoyándonos en aplicaciones gestoras de contraseñas para asegurarnos la diversidad y dificultad de las mismas.
- Instalar y configurar un antivirus.
- Configurar las actualizaciones del software.
- Configurar el cifrado de datos y comunicaciones.
- Desactivar el permiso de recuerdo de contraseña, obligando a introducirla cada vez que se haga uso de las aplicaciones.
- Configurar correctamente los parámetros de seguridad de los dispositivos.
- Mantener correctamente actualizado el sistema operativo y todas las aplicaciones.

Aplicaremos estas medidas tanto a los dispositivos personales que se utilicen para uso profesional como para los dispositivos facilitados para el teletrabajo.

8.3. Protección de conexiones a redes externas

Debemos buscar los mecanismos para asegurar la confidencialidad de los datos en las comunicaciones realizadas entre los dispositivos móviles y los recursos centralizados corporativos cuando hagamos uso de redes ajenas a la organización que no sean seguras.

8.3.1. Redes wifi

En caso de tener que conectarse a la red mediante una red wifi que no garantice la seguridad, debemos buscar los mecanismos necesarios para que la comunicación se realice de la forma más segura posible.

Debemos ser especialmente cuidadosos con las redes públicas desprotegidas y establecer medidas que nos ayuden a evitar problemas como el robo de credenciales, manipulación de nuestra información de trabajo, etc. Para hacer más segura la conexión en este tipo de redes debemos establecer medidas como las siguientes:

- Desconfiar de las redes wifi públicas o gratuitas.
- Utilizar los canales cifrados seguros de comunicación: VPN o algún otro tipo de cifrado punto a punto, como los sitios web con protocolos SSL y certificados.
- Desconectar la wifi de los dispositivos cuando no la estemos utilizando.
- Preferentemente hacer uso de redes 3G o 4G antes que de redes wifi inseguras.

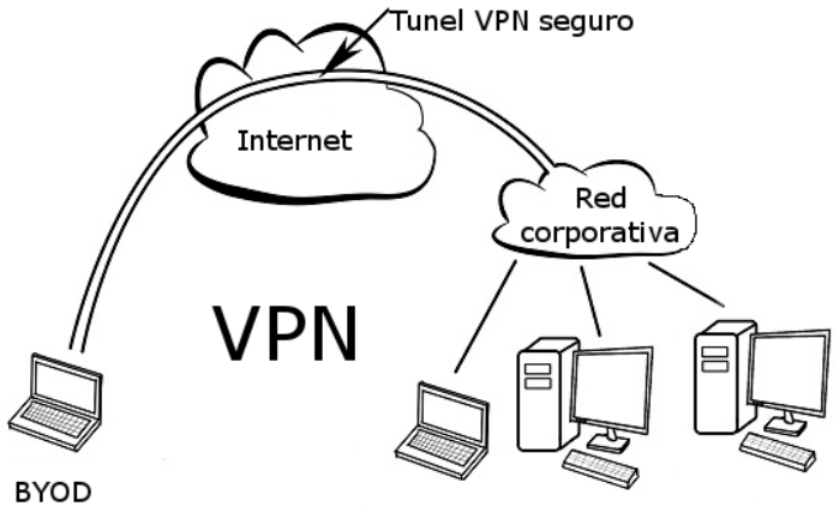
Estas medidas son válidas para todos los dispositivos móviles y en todas las situaciones de uso.

8.3.2. Redes privadas virtuales o VPN

Si necesitamos realizar un acceso mediante una red no segura, deberemos crear canales seguros cifrados de comunicación que garanticen la confidencialidad de nuestra información, mediante el uso de redes VPN (Virtual Private Network).

Una VPN crea un túnel a través de internet, o cualquier otra red no segura, de forma que podemos acceder desde cualquier lugar a los servicios y documentos internos de nuestra organización.

De esta forma nos podemos conectar de forma segura a través de redes (como las wifis domésticas, de cortesía de aeropuertos, hoteles, etc.) cuya seguridad desconocemos, garantizando la confidencialidad e integridad de la información que transmitimos. Con esta medida, también nos aseguramos que la comunicación se está realizando entre dispositivos previamente autorizados.



Anexo I

Medidas de seguridad de aplicación a los dispositivos móviles desplegados en los organismos de las AA.PP. españolas y que puedan contener información corporativa o acceder a recursos corporativos o de otros organismos públicos

Medida	BAJO	MEDIO	ALTO
Configuración del dispositivo			
Se permite el uso de dispositivos móviles rooteados o con jailbreak	En ningún caso		
Software de protección frente a código dañino en el dispositivo móvil	X	X	X
Auto-bloqueo del equipo tras cierto tiempo de inactividad	N/A	X	X
Auto-borrado en caso de varios intentos fallidos de autenticación del usuario	N/A	X	X
Autenticación del dispositivo/usuario			
Sólo los usuarios (o perfiles de usuarios) autorizados por el organismo podrán usar dispositivos móviles	X	X	X
Utilización de PIN/contraseña para acceder al dispositivo	X	X	X
Utilización de contraseña para acceder a los recursos corporativos.	X		
Autenticación basada en certificados digitales instalados en el dispositivo	X	X	
Autenticación basada en tokens externos (certificados digitales externos, por ejemplo)	X	X	X
Almacenamiento			
Se permite el almacenamiento en el dispositivo de información corporativa sin cifrar	X		
Se permite el almacenamiento en el dispositivo de información corporativa, sólo si está cifrada	X	X	X
Borrado de la información			
Borrado simple, en caso de reutilización del dispositivo	X		
Borrado seguro, en caso de reutilización del dispositivo	X	X	X
Posibilidad de borrado remoto del dispositivo en caso de pérdida, compromiso, etc.	N/A	X	X
Aplicaciones			
Se permite la descarga o el uso de cualquier aplicación, sin ninguna restricción.	Totalmente prohibido		
Se permite la descarga sólo de aquellas aplicaciones previamente aceptadas por el organismo (de fuentes aceptadas)	X		
Se permite el uso de determinadas aplicaciones del usuario en el dispositivo móvil, previamente aceptadas u "homologadas" por el organismo y/o con las limitaciones dictadas por el organismo.	X	X	X
Comunicaciones			
Se permiten las comunicaciones del dispositivo móvil con los sistemas corporativos, sin ninguna restricción	X		

Las comunicaciones del dispositivo con los sistemas corporativos deberán realizarse de manera cifrada	X	X	X
Interfaces			
Se permite el uso del interfaz inalámbrico WiFi en el dispositivo, sin restricciones.	X		
Se permite el uso del interfaz inalámbrico WiFi en el dispositivo, con las restricciones impuestas por el organismo	X	X	X
Se permito el uso del interfaz inalámbrico Bluetooth en el dispositivo, sin restricciones.	X		
Se permite el uso del interfaz de Bluetooth en el dispositivo, con las restricciones impuestas por el organismo	X	X	X
Se permite el uso del interfaz USB del dispositivo, sin restricciones	X		
Se permite el uso del interfaz USB del dispositivo, con las restricciones impuestas por el organismo	X	X	X
Formación y concienciación			
Formación y concienciación a los usuarios de dispositivos móviles	X	X	X

Anexo II: Modelo de aceptación y compromiso de cumplimiento

Todos los usuarios de los recursos informáticos y/o Sistemas de Información del Ayuntamiento de Mislata deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Norma, debiendo suscribirla.

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, [personal del Ayuntamiento de Mislata], como usuario de recursos informáticos y sistema de información, declara haber leído y comprendido las Normas para Teletrabajar y se compromete, bajo su responsabilidad, a su cumplimiento.

En _____, a _____ de _____ de 20___

Organismo:	Ayuntamiento de Mislata
Trabajador (Nombre y Apellidos):	
DNI número:	
Número de Registro de Personal	
Firmado:	

Por el Ayuntamiento de Mislata, <<Nombre y Apellidos>>

DNI número: _____.

Número de Registro de Personal: _____

Anexo III. Autorización excepcional de acceso remoto y normas de teletrabajo cuando el mismo se realiza con los medios particulares del empleado

Atendiendo a las excepcionales circunstancias motivadas por el COVID-19 y con el objetivo de lograr una conciliación entre la protección de la salud y el necesario desempeño del trabajo con las debidas garantías de seguridad, procedemos a instaurar el teletrabajo con carácter excepcional para lo cual es necesario establecer un acceso remoto temporal a los servidores del Ayuntamiento de Mislata**.**

De este modo,

- **AUTORIZACIÓN ACCESO REMOTO**

El Ayuntamiento de Mislata autoriza a **NOMBRE TRABAJADOR** a conectarse desde el exterior a los equipamientos del Ayuntamiento de Mislata utilizando sus dispositivos propios, para el desempeño de sus funciones laborales.

La vigencia de la autorización será la siguiente: desde ___/03/2020 hasta ___/04/2020 o hasta nueva comunicación.

- **NORMAS DE USO:**

La persona autorizada se compromete a observar con las siguientes **recomendaciones y normas**:

- el usuario debe proporcionar al personal informático del Ayuntamiento de Mislata la información de los equipos: versión de sistema operativo, características del equipamiento, y toda aquella información relevante que conozca y pueda ofrecer.
- en caso de cambiar modelo de dispositivo o sus características, el usuario deberá comunicarlo al personal informático, a fin de que se le faciliten las mejores medidas de seguridad adecuadas a dichos cambios.
- **la organización se reserva el derecho de no autorizar aquellos dispositivos que por sus características de seguridad no ofrezcan garantías adecuadas.**
- El usuario deberá emplear los mecanismos de cifrado de la información disponibles en su dispositivo, en caso de que vaya a almacenar información del Ayuntamiento en el dispositivo.
- La realización de copias de seguridad de los datos del Ayuntamiento de Mislata es responsabilidad del Ayuntamiento de Mislata salvo que se le indique al usuario otra cosa. El trabajador deberá evitar la realización de copias y deberá verificar que se han eliminado ficheros temporales que se hayan podido generar, quedando siempre los ficheros y documentos almacenados en los sistemas de información y servidores principales del Ayuntamiento de Mislata.
- El usuario se abstendrá de desactivar cualquier mecanismo de seguridad que haya sido habilitado por el Ayuntamiento de Mislata en el dispositivo, tal y como el mecanismo de bloqueo, el sistema de ubicación del dispositivo, el cifrado de los datos, o cualquier otro.
- En caso de avería, malfuncionamiento del dispositivo, el usuario lo notificará inmediatamente al Responsable de Seguridad del Ayuntamiento de Mislata.
- El usuario mantendrá el sistema operativo del dispositivo permanentemente actualizado y con antivirus, mientras trate datos del Ayuntamiento de Mislata.
- El trabajado tiene terminantemente prohibido copiar o almacenar en el dispositivo particular datos de carácter personal que hagan referencia a la ideología, afiliación sindical, religión o creencias, origen racial, salud o vida sexual.

- Recordamos la **obligación de confidencialidad** a la que está sujeto el trabajador del Ayuntamiento de Mislata, no pudiendo divulgar los datos personales, ni tampoco cualquier otra información responsabilidad del Ayuntamiento de Mislata a la que acceda por razón de su puesto de trabajo. Esta obligación de confidencialidad subsistirá incluso después de finalizar su relación con el Ayuntamiento de Mislata.
- Se hará uso de la red doméstica o en su caso de la red 4G proporcionada por el Ayuntamiento y no se está permitida la conexión a wifis públicas.
- Con respecto al acceso al correo electrónico:
  - Sea muy cuidadoso con los correos recibidos: no los abra si no conoce al remitente. No confíe únicamente en el nombre del remitente, compruebe que el dominio del correo recibido es de confianza.
  - Desconfíe de correos que soliciten datos personales o contraseñas de acceso.
  - Malware: no abra enlace alguno ni descargue ningún fichero adjunto procedente de un correo electrónico que presente cualquier indicio o patrón fuera de lo habitual.
  - Antes de abrir cualquier fichero descargado desde el correo, asegúrese de la extensión y no se díe del icono asociado al mismo.
  - No habilite las macros al abrir ficheros adjuntos.
  - No reenvíe correos oficiales a sus cuentas de correo particulares.

Mediante la firma del presente documento, el usuario manifiesta que ha leído, comprendido y aceptado las presentes normas. La vulneración de las mismas podría suponer infracción de la normativa de protección de datos de carácter personal.

Cualquier **incidencia en materia de seguridad** deberá contactar con el departamento de informática según el protocolo vigente.

Para cualquier duda o aclaración, por favor, no dude en contactar con incidencias@mislata.es

Fdo. El trabajador/a

Ayuntamiento de Mislata

_____

_____

_____.