GUÍA DE TELETRABAJO PARA EMPLEADOS PÚBLICOS DE LA DIPUTACIÓN DE OURENSE

CONTROL DE VERSIÓNES Y DISTRIBUCIÓN	
NOMBRE DEL DOCUMENTO:	**VERSIÓN:** 01.00
CODIFICACIÓN DEL DOCUMENTO:	
ELABORADO POR:	**FECHA:**
VALIDADO POR:	**FECHA:**
APROBADO POR:	**FECHA:**

REGISTRO DE CAMBIOS		
Versión	**Causa de la nueva versión**	**Fecha de aprobación**

Resumen
Índice

Tabla de contenido

1. Introducción.

La situación actual, provocada por el COVID-19, ha obligado a que los/as empleados/as de la administración provincial tengan la posibilidad de acogerse a esta modalidad de trabajo a distancia. Es por ello, que el objetivo de esta guía es ayudar en la preparación de un entorno seguro y eficiente para realizar estas tareas, junto con las herramientas tecnológicas necesarias para facilitar esta transición a aquellos empleados/as que opten por esta forma de trabajar.

2. ¿Qué se necesita para teletrabajar?

Para teletrabajar en la Diputación de Ourense va a ser necesario disponer de los siguientes elementos:

- Un teléfono de contacto a donde poder desviar las llamadas entrantes al terminal de la oficina o donde se le pueda localizar.
- Un equipo informático con las características suficientes para el acceso a internet.
- Un acceso remoto seguro (VPN), para acceder a los recursos de la red interna de la Diputación de Ourense.
- Acceso remoto al escritorio del ordenador de trabajo para disponer de los recursos que se proporcionan desde el puesto de trabajo de la oficina.
- Certificado digital, si va a firmar documentos o utilizar un servicio que así lo requiera.

En los siguientes apartados de este documento se facilita información sobre cómo configurar las herramientas necesarias, así como los principales recursos a los que se puede acceder.

Solo con disponer de acceso a internet ya puede acceder a algunas de las herramientas básicas de uso cotidiano en la jornada de trabajo común, como es el caso del correo corporativo. Correo DPOU

3. ¿Cómo conectarse a la red de la Diputación de Ourense?

3.1. Acceso a la red interna.

Para trabajar accediendo a todas las herramientas y aplicaciones que están disponibles dentro de la red interna de la Diputación de Ourense, deberá solicitar y configurar en su equipo un acceso remoto seguro (VPN). Esto le permitirá acceder, por ejemplo, a la intranet corporativa o a todas aquellas aplicaciones que solo están disponibles dentro de la misma (Ej. MyTao, unidades compartidas, etc.).

Si, a mayores de esto, conecta de forma remota el equipo de casa con el de su puesto de trabajo, se igualan prácticamente las condiciones de trabajo habituales, disponiendo de todos los programas, recursos, accesos a carpetas compartidas, documentos y permisos que usa diariamente.

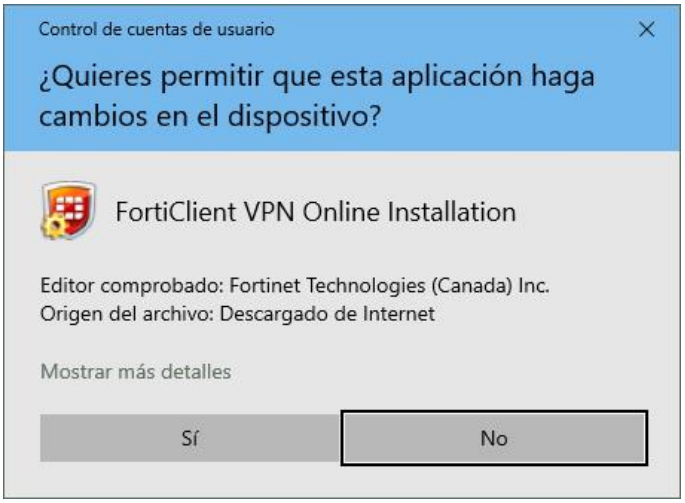
En los siguientes apartados se describen los pasos para acceder a los servicios que se ofrecen desde la red interna de la Diputación de Ourense.

3.1.1. Solicitar el acceso a la red interna. Conexión VPN.

- Una vez que se tenga concedido el teletrabajo se deberá enviar un correo a la dirección atga_ts@depourense.es indicando su nombre completo, área o servicio, número de trabajador y una dirección de correo.
- Después de las correspondientes verificaciones, se proporcionará en un mensaje de correo electrónico las instrucciones que deberá aplicar en su equipo para disponer del servicio.

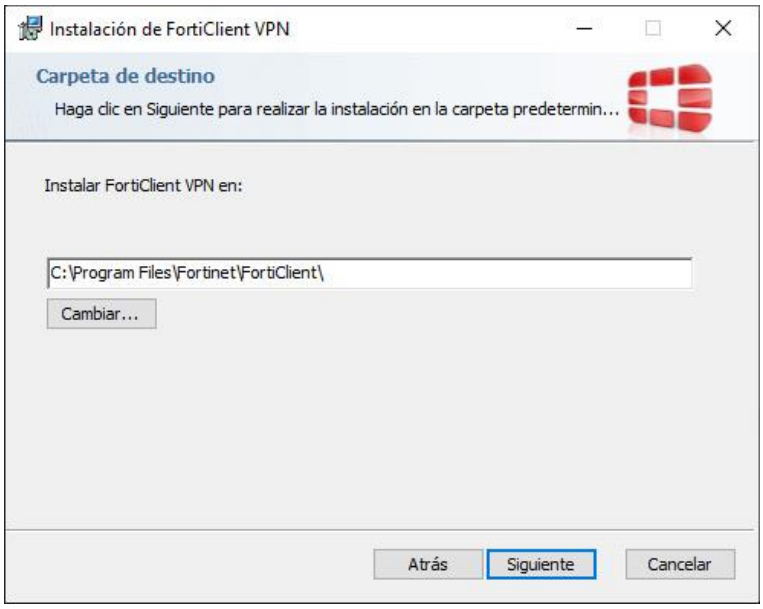
3.1.2. Configurar el equipo de casa

- En primer lugar, se debe instalar en el ordenador de casa la aplicación que permitirá conectarse. Deberá ser descargada desde la siguiente dirección: www.depourense.es/asistencia.
- Seguidamente, una vez descargada, se ejecuta siguiendo las siguientes indicaciones:
  - Pulsar “SI”

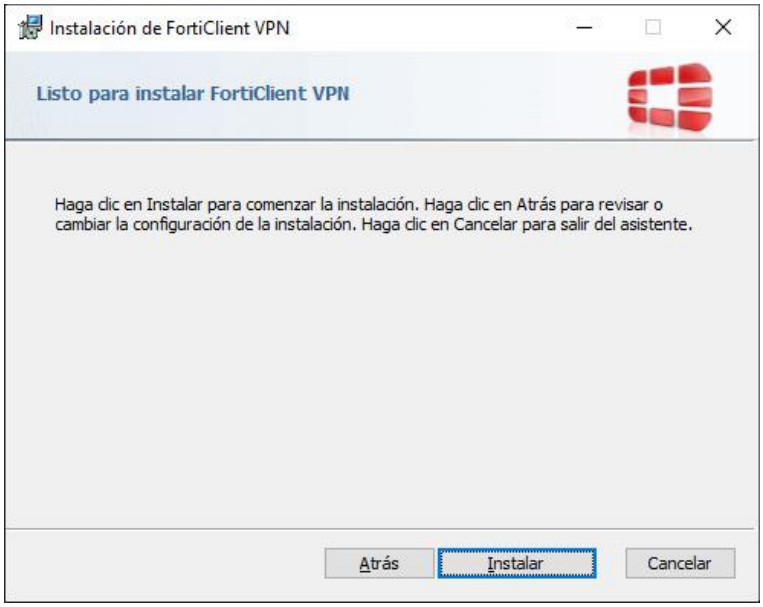


  - Seleccionas “SI, HE LEIDO Y ACEPTADO EL ACUERDO DE LICENCIA” y pulsas “SIGUIENTE”

- Pulsas “SIGUIENTE”

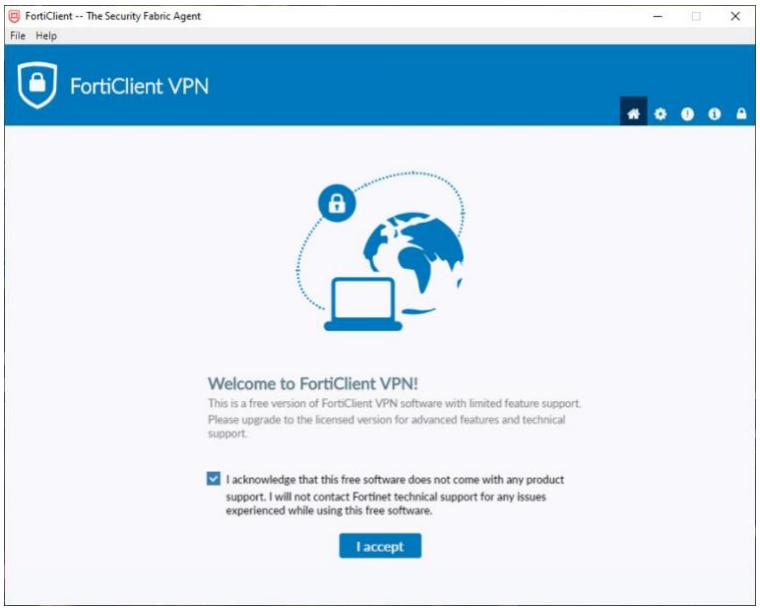


- Pulsas “INSTALAR”

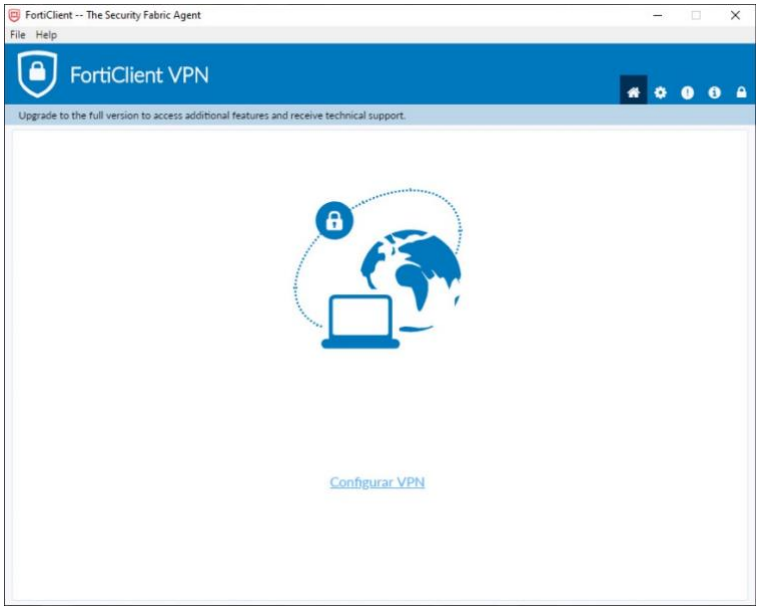


- A continuación, para configurar la conexión en la aplicación estos son los pasos:
  - Ejecutas el aplicativo haciendo doble click en el icono “FortiClient VPN” que se ha creado en el escritorio

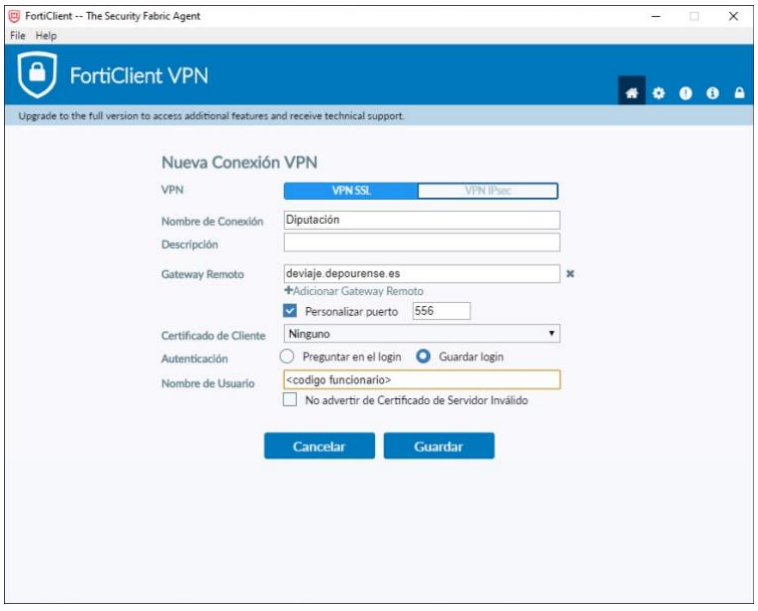
  - Seleccionas la casilla “I ACKNOWLEDGE THAT THIS FREE …” y pulsas “I ACCEPT”



  - Pulsas en “CONFIGURAR VPN”



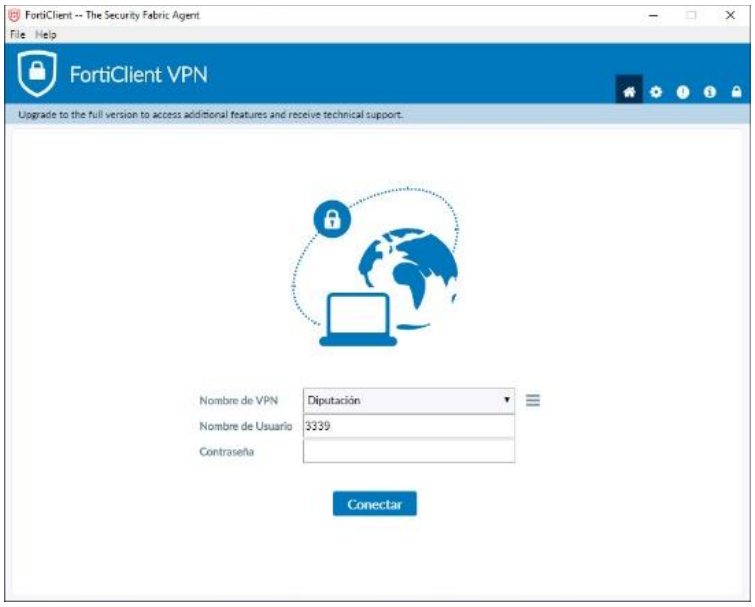
- Rellenas con los siguientes datos:
  - "NOMBRE DE CONEXIÓN": **DIPUTACIÓN**
  - "GATEWAY REMOTO": **deviaje.depourense.es**
  - Seleccionar "**PERSONALIZAR PUERTO**" e indicar **555**
  - En "**AUTENTICACIÓN**" seleccionar "**GUARDAR LOGIN**"
  - En "**NOMBRE DE USUARIO**" indicar el número de funcionario
  - Pulsar "**GUARDAR**"



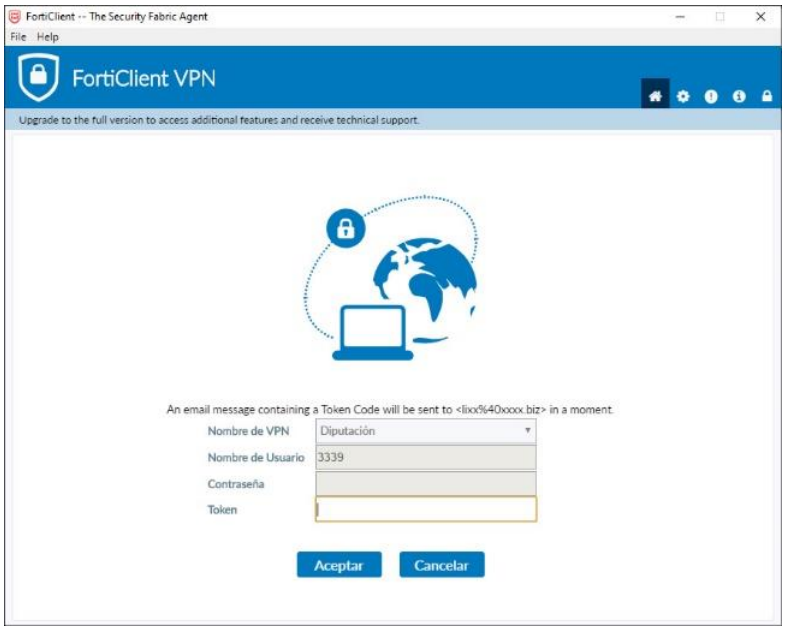
3.1.3. Conectar el equipo de casa a la red corporativa

- En primer lugar, será necesario identificarse a través de la aplicación que descargó en el paso anterior utilizando para ello su usuario y contraseña.
  - Se ejecuta el aplicativo haciendo doble click sobre el icono "FortiClient VPN" que aparece en el escritorio.

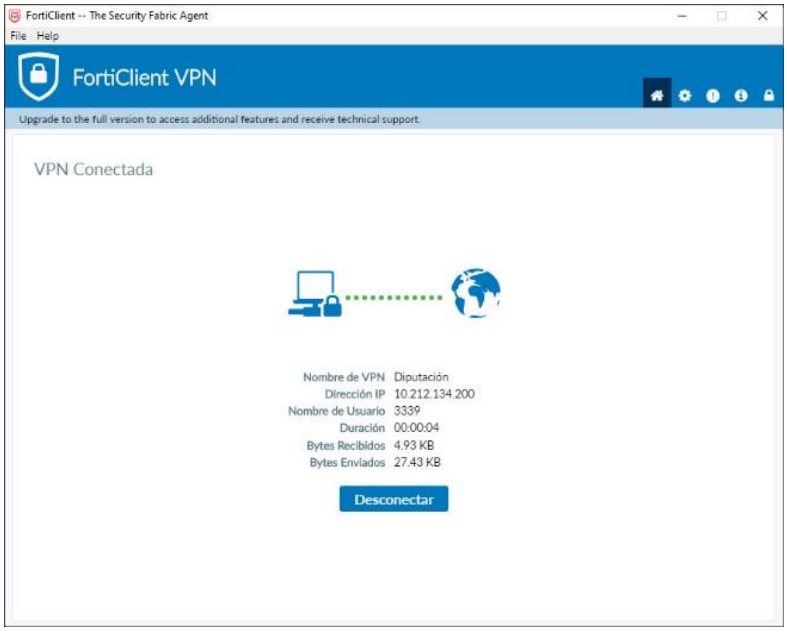
- Se introduce usuario y contraseña y, seguidamente, se presiona en “CONECTAR”



- A continuación, se solicitará un “TOKEN” de acceso que habrá sido enviado a la cuenta de correo electrónico facilitada en la solicitud de acceso y, que se enviará cada vez que se realice una conexión. Este código ha de introducirse en la casilla “TOKEN”. Y, para finalizar se ha de pulsar el botón aceptar.



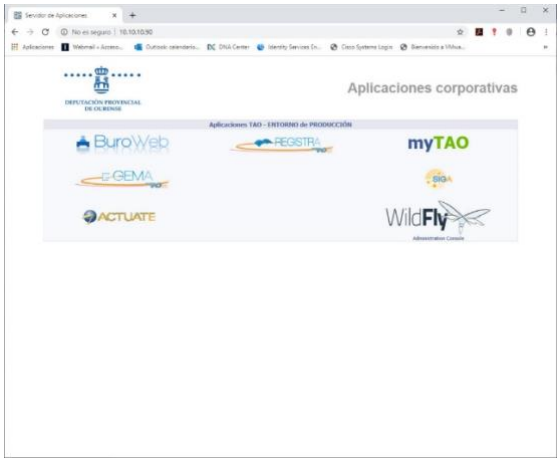
- Una vez que se realiza la conexión la pantalla indicará “VPN CONECTADA”

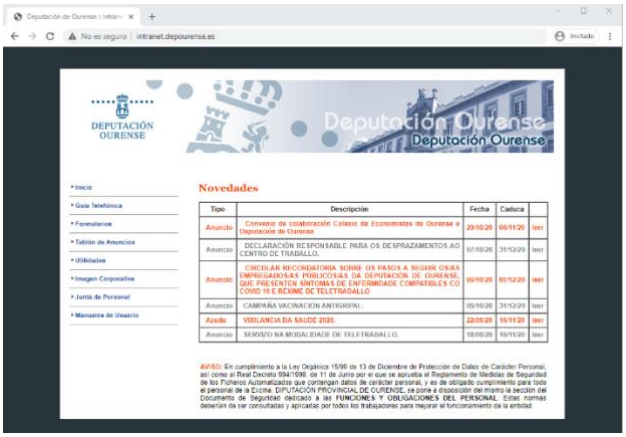


- Ahora el equipo ya está conectado a la red de la Diputación. Esta ventana puede mantenerse minimizada.

3.1.4. Acceder a los aplicativos

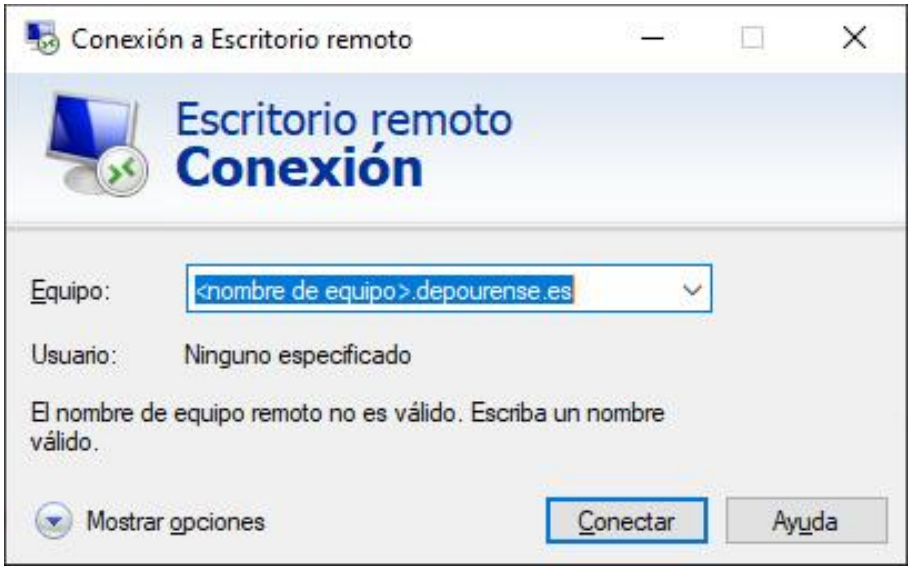
- El acceso a los servicios de administración electrónica se puede realizar introduciendo en un navegador la siguiente dirección: http://10.10.10.90
- También se puede acceder a la intranet corporativa a través de la dirección: http://intranet.depourense.es.



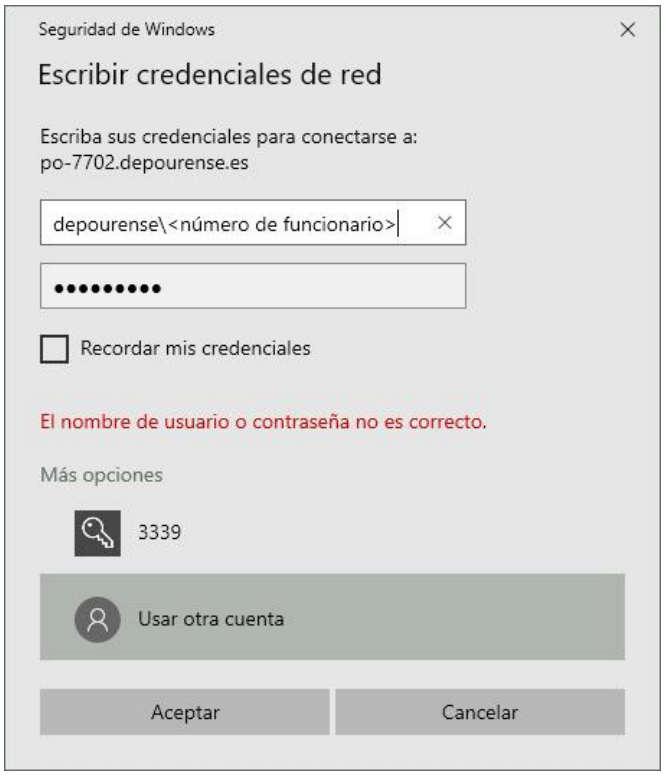


3.1.5. Acceder al equipo del trabajo

- A través de la opción "Conexión a escritorio remoto" de su equipo personal, es posible tomar el control del ordenador de su puesto de trabajo. Podrá usar todos los programas y recursos de los que dispone en él.
- Para el acceso al escritorio se debe utilizar el programa “CONEXIÓN A ESCRITORIO REMOTO” e introducir el <nombre de equipo> en el cuadro de diálogo.



- A continuación, se ha de introducir el número de funcionario y contraseña. Es necesario tener en cuenta que el número de funcionario hay que introducirlo de la siguiente forma: depourense\<número de funcionario>



3.2. Acceso a la red telefónica.

Para emplear el teléfono fijo del puesto de trabajo en la Diputación de Ourense puede desviarlo a otro teléfono, ya sea corporativo o personal, y de esta manera se podrá atender las llamadas entrantes como si estuviera en la oficina.

3.2.1. Desvío del teléfono fijo

El desvío de su teléfono permite que las llamadas telefónicas que entran en el teléfono de su puesto de trabajo sean recibidas en otro número, de tipo fijo o móvil (corporativo o personal). De esta forma podrá recibir llamadas sin tener que encontrarse físicamente en la oficina.

3.2.2. ¿Cómo se configura?

En el apartado “Guía telefónica” de la intranet de la Diputación se pueden encontrar los manuales y guías rápidas de los diferentes modelos de teléfonos que están en uso actualmente.

El propio interesado o un/a compañero/a puede configurar el desvío siguiendo los pasos para el modelo correspondiente. En el siguiente enlace se pueden consultar dichos manuales: Manuales teléfonos.

4. Recomendaciones de ciberseguridad.

En el desempeño del teletrabajo es importante seguir una serie de recomendaciones de ciberseguridad con el fin de proteger la información y los servicios de los riesgos que se pueden generar.

Los medios de protección de un equipo fuera de las instalaciones del organismo pueden ser menores que cuando se está dentro del perímetro de seguridad del organismo. Es por ello que, si se conecta a la red corporativa de la Diputación de Ourense y se accede al equipo del puesto de trabajo desde el personal, es importante que se tengan en cuenta estos consejos:

- Acceder desde una conexión a internet de confianza, es decir, se utilizará preferiblemente la red doméstica, ya que sobre esta se tiene un mayor control y se evitará utilizar redes wifi públicas.
- Utilizar las herramientas corporativas puestas a disposición por la Diputación de Ourense para el trabajo remoto, evitando utilizar plataformas ajenas que podrían implicar riesgos de seguridad (técnicos y normativos).
- Acceder a la red corporativa y al equipo de su puesto de trabajo solo durante la jornada laboral (períodos de interconexión). Evitar, por lo tanto, que la conexión quede abierta fuera de ella o cuando no sea necesario su uso.
- En la medida de lo posible es necesario que se mantenga actualizado el equipo informático personal. Para ello, se recomienda que se ejecuten todas las actualizaciones de seguridad de los programas que se utilicen en el equipo. También debe contar con un antivirus instalado y permanentemente actualizado.

  En este punto, recordar que, para mejorar la seguridad sobre los equipos destinados al teletrabajo, se ha proporcionado un antivirus profesional de forma gratuita durante el tiempo que dure esta situación. Este se encuentra accesible en la siguiente dirección: http://www.depourense.es/asistencia/installer.exe
- Seguir unas pautas seguras cuando navegue por internet, para así evitar la infección del equipo.
- Se debe proteger el equipo con una contraseña para evitar accesos no deseados.

- Mientras se utiliza la conexión corporativa no se debe, simultáneamente, realizar con el mismo equipo actividades ajenas a las propias del trabajo (por ejemplo, acceder a páginas web no relacionadas con la actividad, ejecutar aplicaciones o abrir documentos que no sean corporativos...).
- Siempre que sea posible, no copie información en el disco local del ordenador que se esté utilizando en casa. Lo recomendable es conectarse por escritorio remoto al ordenador del trabajo y seguir almacenando toda la información en los repositorios corporativos habituales.
- En el uso del correo electrónico recordar estar alerta ante cualquier correo sospechoso. En caso de recibir alguno con estas características siga estas pautas:
    - No hacer clic en ningún enlace.
    - No abrir los ficheros adjuntos.
    - No introducir credenciales (usuario o contraseña) en páginas de dudosa legitimidad. Fíjese bien que en la dirección que se muestra en la barra de navegación se use el protocolo seguro HTTPS y verifique el certificado asociado a la página web.
    - Verificar el campo "de" del correo y comprobar cuál es la dirección de correo del remitente, más allá del "alias" que emplee. En caso de duda, se recomienda llamar o contactar previamente con el remitente para confirmar la legitimad del correo.
- Se debe sospechar en general, de:
    - Correos con faltas de ortografía u otros errores de redacción, así como cualquier otro elemento sospechoso
    - Enlaces cortos o de aquellos en los que, al pasar el puntero del ratón por encima de ellos, apunten a una dirección que no sea conocida.
    - Ante cualquier duda, si se sospecha que ha podido ser víctima de un correo fraudulento o en el caso de querer comunicar una incidencia de seguridad informática póngase en contacto con los técnicos del área de Transparencia e Goberno Aberto.