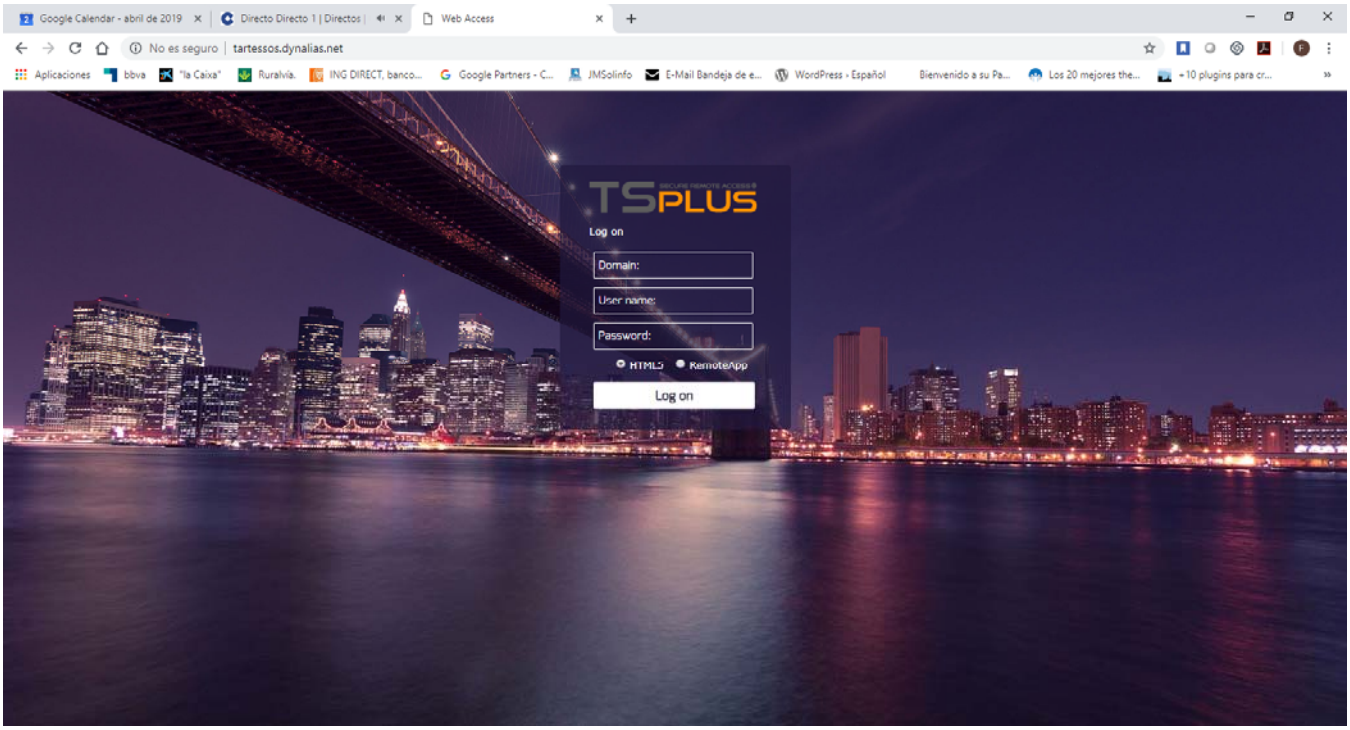
ÍNDICE

Pedidos

Acceso.

1.- Acceso vía web.

Accederemos a la página web ***www.gtartessos.org***, habrá una sección de acceso a usuarios hacer clik.. Aparecerá la pantalla de autentificación, Similar a esta.



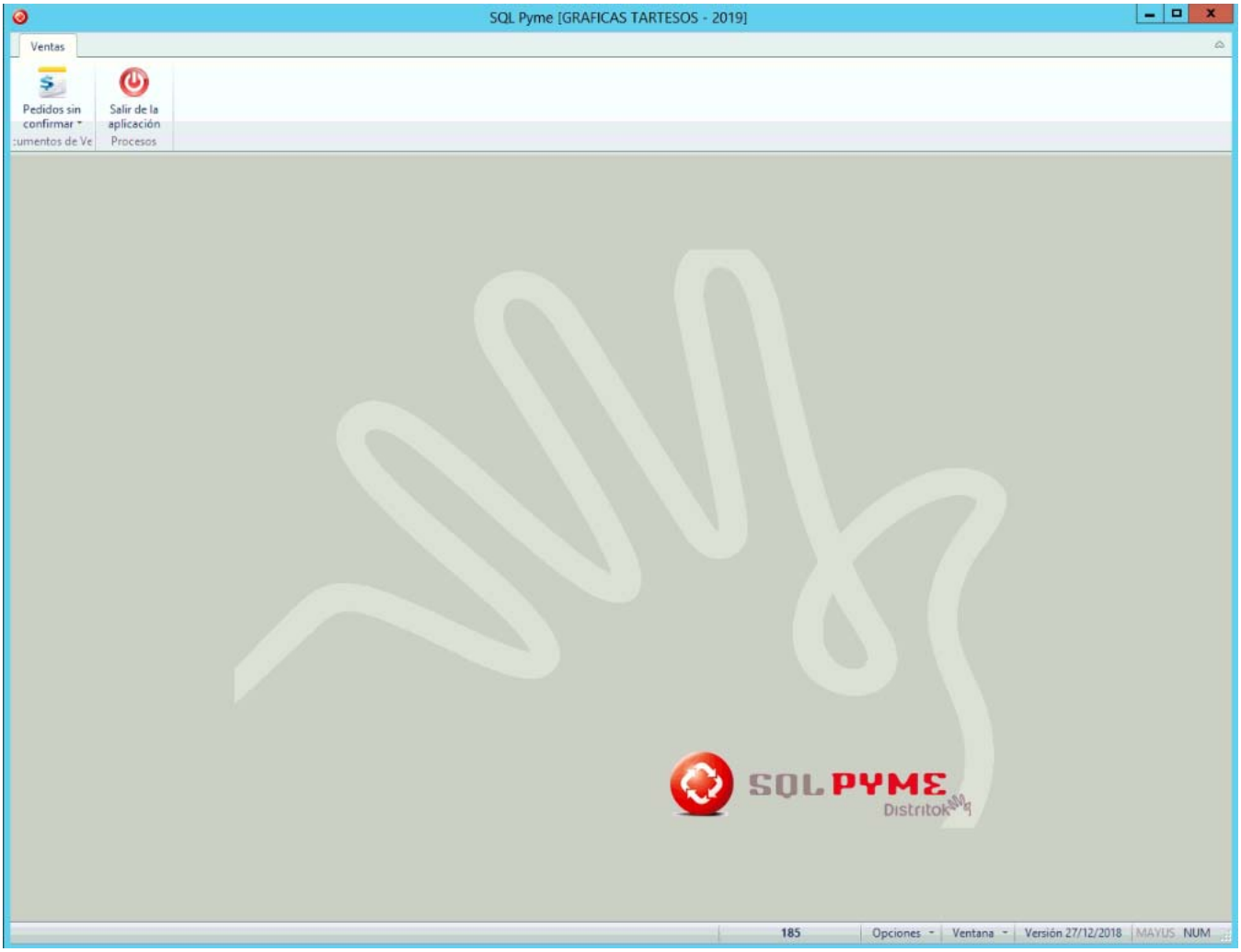
En el Dominio no escribir nada, en usuario (User name) poner el Nº de usuario proporcionado por Graficas Tartessos, y en la contraseña (password) escribir la proporcionada por Graficas Tartessos. La contraseña constará de siete dígitos y tendrá unas características, acorde con los protocolos de seguridad exigidos, ver anexo I.

Pedidos.

1.- Elaboración de pedido

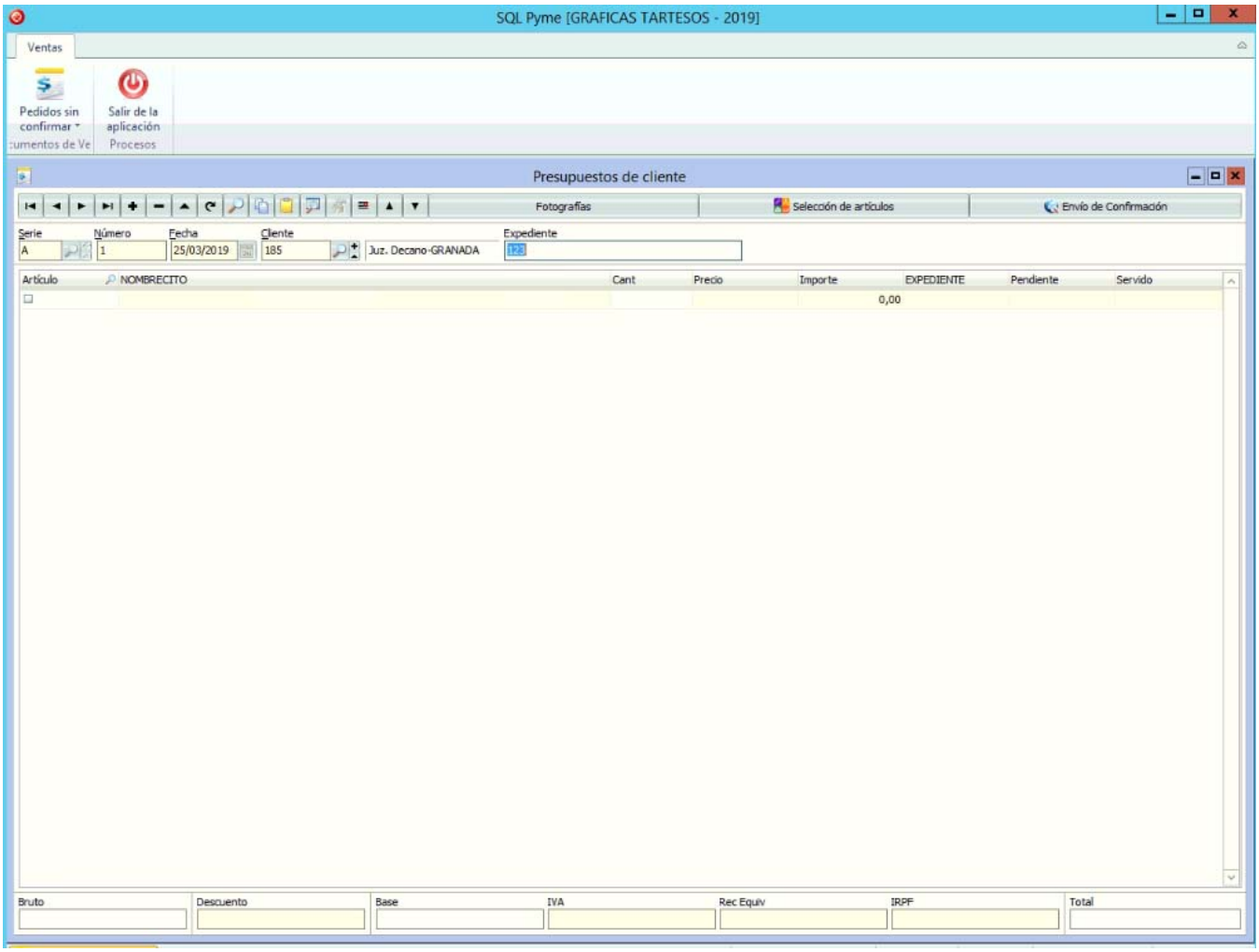
El proceso de pedidos ha sido desarrollado con el objetivo de reducir al máximo la complejidad del proceso, y evitar en la medida del lo posible, la necesidad de pasos adicionales.

Después de acceder al programa se presentará la ventana de inicio, similar a la siguiente:



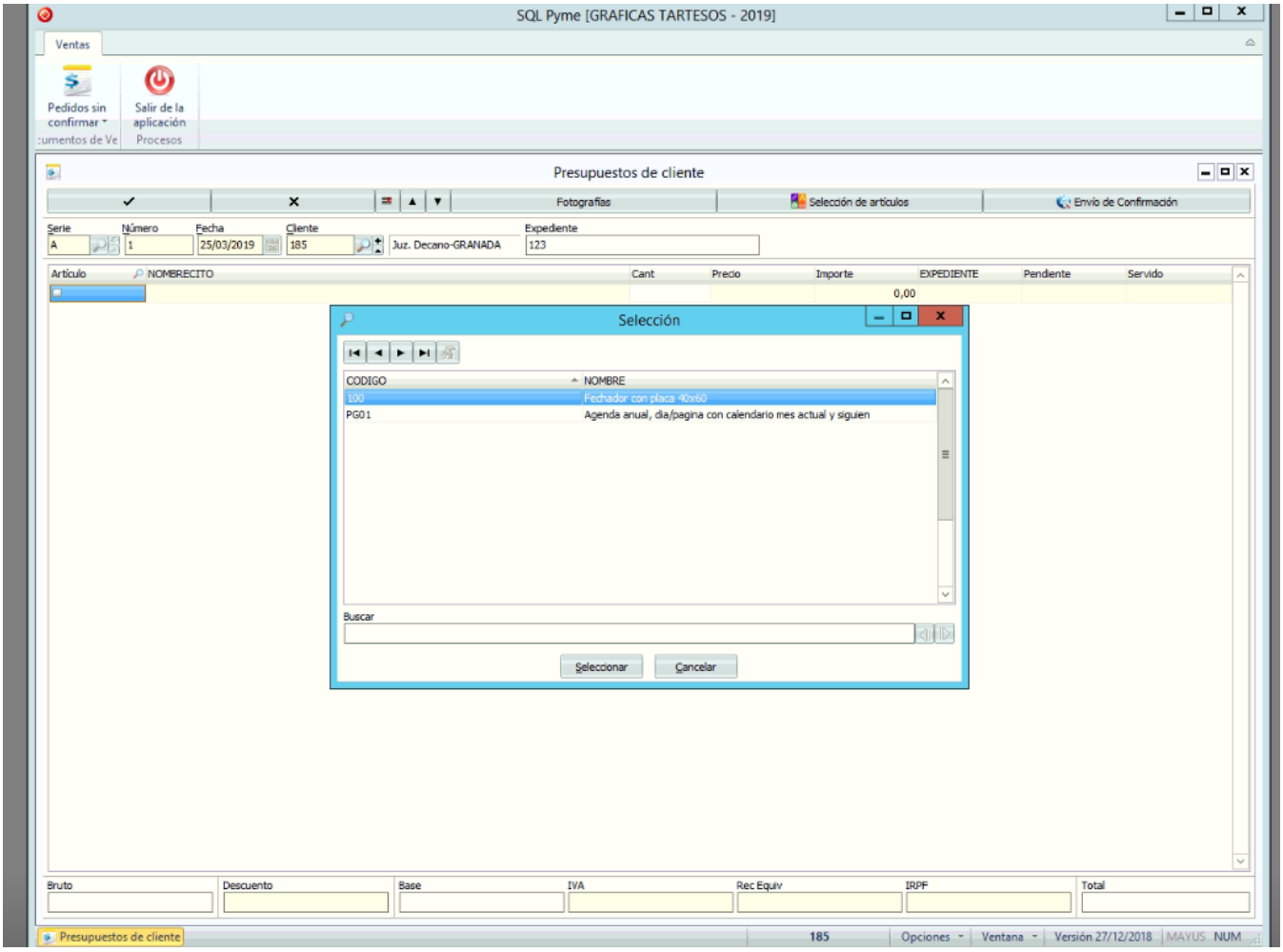
Pulsar el botón de Pedido sin confirmar, será la única opción.

En la siguiente ventana.

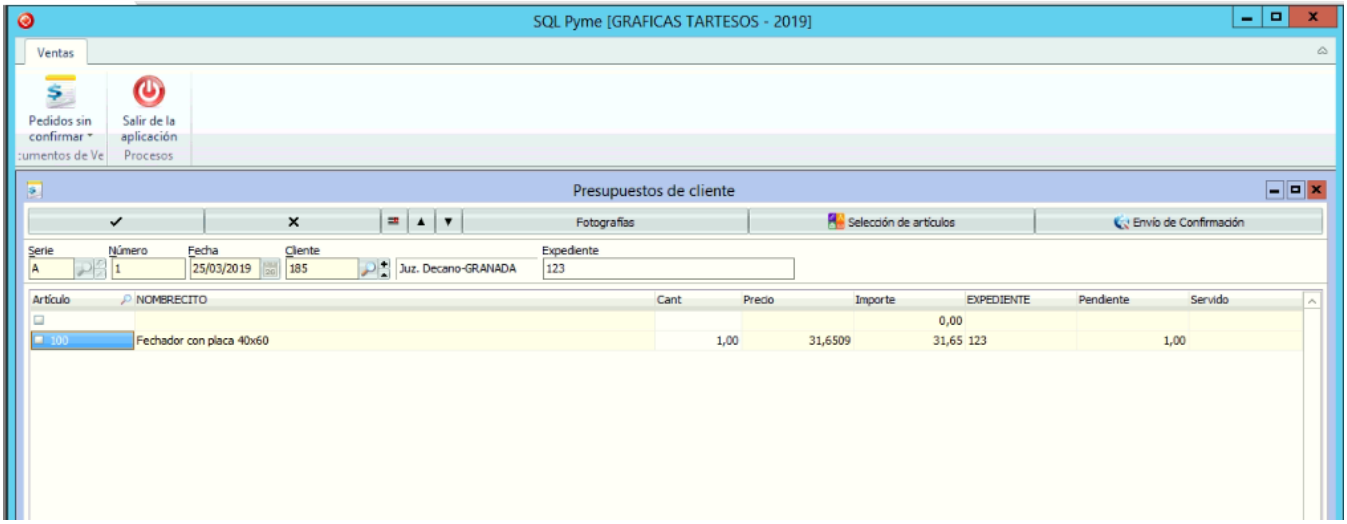


En esta pantalla solo habrá que rellenar el Expediente, **03** "papelería" (p.ej. grapadoras, grapas, bolígrafos, marcadores, etc) y el **04** "impresión" (p.ej. trabajos de impresión en sobres, folios, etc.), aquí pulsaremos la pestaña **selección de artículos**, repetiremos el expediente. Este paso es por motivos de seguridad, y habrá repetirlo en cada línea.

Aparecerá la ventana de búsqueda de artículos será parecido a esta.



La búsqueda será por código, si se quisiera buscar por nombres, solo habría que pinchar en la pestaña nombre, situada sobre en nombre del artículo y buscar el artículo por nombre en la línea de búsqueda. Una vez localizado el artículo, pinchar en seleccionar ó pulsar Intro , aparecerá en la línea de pedido, tal que así



Pulsar intro e introducir cantidad a pedir. En esta búsqueda una vez seleccionado el artículo se verá una imagen del mismo.

Repetir proceso hasta completar pedido.

Una vez completado, pulsaremos la pestaña **Envío de confirmación**, esto enviará un correo a la dirección de E-mail asignada, para la posterior confirmación del pedido.

Anexo I

Contraseñas

Hoy en día, el método más habitual para acceder a la información almacenada en nuestros ordenadores, correo electrónico y otros servicios es mediante contraseña. La contraseña es una información secreta que se nos solicita para acceder a algún tipo de recurso, y que solo debe conocer el propietario del mismo.

Es necesario invertir un poco de tiempo y esfuerzo en generar una contraseña segura. Si un usuario malintencionado consiguiera apoderarse de una contraseña podría acceder a información personal, violando la privacidad, o incluso tener acceso a servicios financieros.

¿Cómo me protejo?

- La longitud de las contraseñas no debe ser inferior a ocho caracteres. A mayor longitud más difícil será de reproducir y mayor seguridad ofrecerá.
- Construir las contraseñas con una mezcla de caracteres alfabéticos (donde se combinen las mayúsculas y las minúsculas), dígitos e incluso caracteres especiales (@, ¡, +, &).
- Usar contraseñas diferenciadas en función del uso (por ejemplo no debe usarse la misma para una cuenta de correo que la usada para acceso a servicios bancarios).
- Un buen método para crear una contraseña sólida es pensar en una frase fácil de memorizar y acortarla aplicando alguna regla sencilla.
- Se deben cambiar las contraseñas regularmente. (Dependiendo de la criticidad de los datos puede ser cada X meses).

- Se debe evitar:
- conyuges, ...). Tampoco una serie de letras dispuestas adyacentemente en el teclado (qwerty) o siguiendo un orden alfabético o numérico (123456, abcde, etc.)
- No se recomienda emplear la misma contraseña para todas las cuentas creadas para acceder a servicios en línea. No utilizar la misma contraseña en sus servicios de la UAL en su banca electrónica, por ejemplo.
- Se deben evitar contraseñas que contengan palabras existentes en algún idioma (por ejemplo “campo”). Uno de los ataques más conocidos para romper contraseñas es probar cada una de las palabras que figuran en un diccionario y/o palabras de uso común.
- No se deben almacenar las contraseñas en un lugar público y al alcance de los demás (encima de la mesa escrita en papel, etc…).
- No compartir las contraseñas en Internet (por correo electrónico) ni por teléfono. En especial se debe desconfiar de cualquier mensaje de correo electrónico en el que le soliciten la contraseña o indiquen que se ha de visitar un sitio Web para comprobarla. Casi con total seguridad se tratará de un fraude. La Universidad de Almería nunca le va a solicitar ese tipo de información.
- No utilizar la opción de “Guardar contraseña” que en ocasiones se ofrece, para evitar reintroducirla en cada conexión.

Política de contraseñas en la UAL

Las contraseñas de los servicios proporcionados por el STIC se ajustan a las siguientes normas:

- **La caducidad de la contraseña es 6 meses**. ¿Porqué se obliga a cambiarla? A pesar de que crea que tiene una contraseña segura, puede que la descubran: se la han podido ver teclear, o capturar mediante programas de escucha. En otras ocasiones se descubre por causa de "logins fallidos", puesto que muchos usuarios se equivocan y escriben el password en vez del Login.
- Debe tener entre 8 y 30 caracteres (al menos 2 números).
- No debe contener la contraseña anterior (ni viceversa).

- Debe diferenciarse del Login en al menos 3 caracteres.
- Debe diferenciarse de la contraseña anterior en al menos 3 caracteres.
- No debe coincidir con ninguna de las 4 contraseñas anteriores.

Más información sobre las contraseñas:

https://docs.microsoft.com/es-es/windows/security/threat-protection/security-policy-settings/password-must-meet-complexity-requirements

Actualizado por: STIC

Fecha: 13 de febrero de 2019