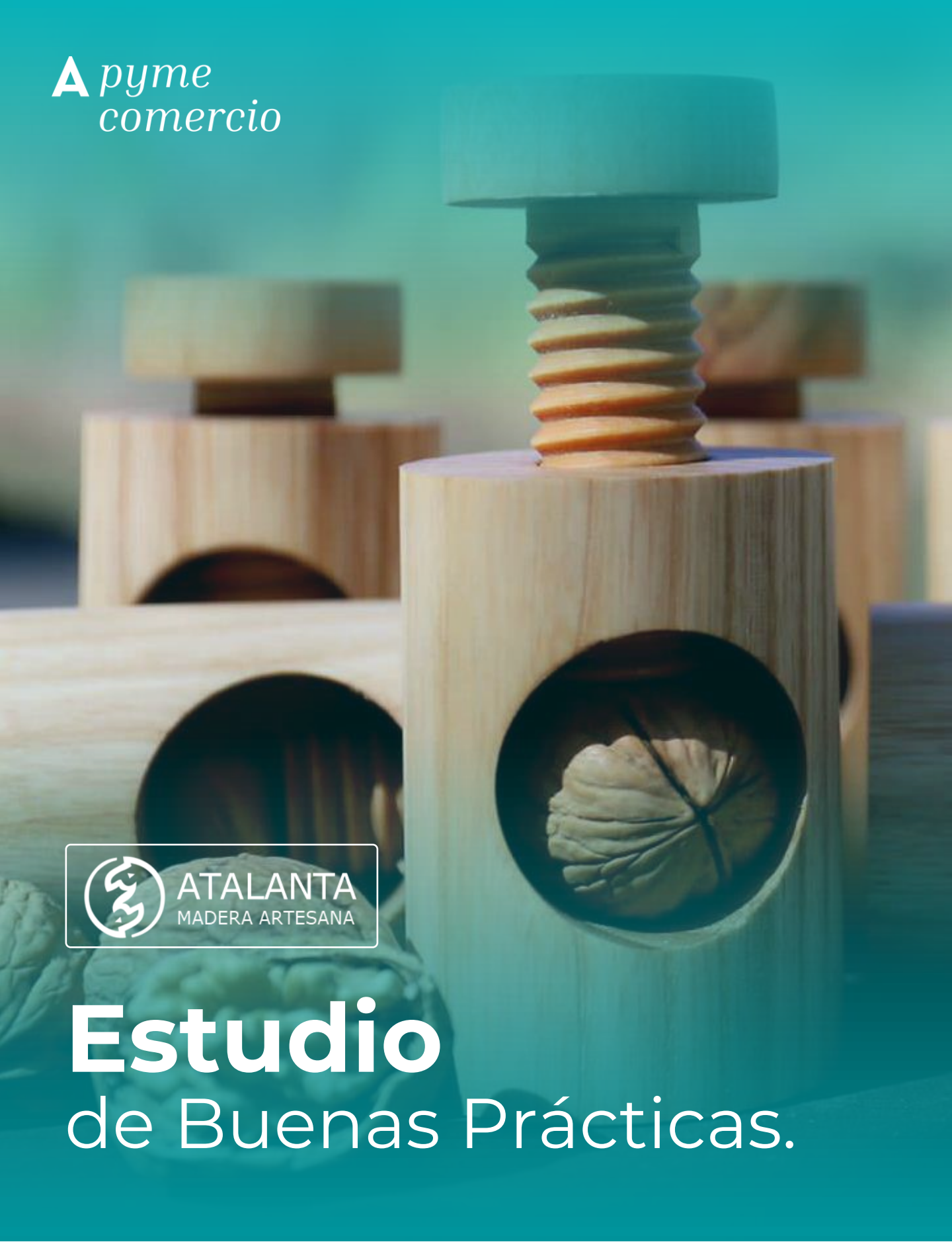
A pyme comercio



ATALANTA
MADERA ARTESANA

Estudio
de Buenas Prácticas.

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

Estudio de Buenas Prácticas.

El estudio de buenas prácticas tiene como objetivo presentar un caso de éxito de una empresa que ha iniciado su camino hacia un negocio digital con el propósito de darse a conocer y potenciar sus ventas.

Atalanta Madera es un negocio familiar de tornería artesanal en madera, en el que dos hermanas, Isabel y Ana Neira se encargan de todo desde principio a fin. Desde el diseño, al torneado, al acabado de cada objeto, y la gestión empresarial.

Para el desarrollo de este estudio se ha tomado como punto de partida la identificación de las inquietudes de pymes de comercio de diversos sectores. Las empresas manifestaron su interés por conocer buenas prácticas en los ámbitos de la ciberseguridad, entre otras.

A lo largo del estudio te contamos cómo, con distintas acciones de ciberseguridad, han conseguido hacer crecer su negocio y han aumentado tanto su tranquilidad como la de sus clientes.

ATALANTA
MADERA ARTESANA

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

Información de la Compañía.

DIRECCIÓN WEB >

www.atalantamadera.com

AÑO DE FUNDACIÓN >

2004

LOCALIZACIÓN >

Lugar Mouteira, 10 – Berres
36688 A Estrada
(Pontevedra)

NÚMERO DE EMPLEADOS >

2

TIPO DE SOCIEDAD >

Sociedad Limitada

ACTIVIDADES PRINCIPALES >

Negocio de tornería artesanal

SECTOR >

Comercio

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

Problema o necesidad

Desde Atalanta Madera, son conscientes de los riesgos que pueden derivarse de la red. Por esa razón, querían que sus clientes se sintieran seguros navegando por su web, del mismo modo que a ellas les gusta sentirse seguras en webs ajenas.

La seguridad fue prioritaria para ellas cuando implementaron su tienda online, dándole mucha importancia al tratamiento de datos de sus clientes y al posible robo de los mismos.

Proceso de implementación y solución

En general, afirman que hacen uso del sentido común, fijándose en quién emite los correos, las extensiones y los archivos que reciben. Es un negocio pequeño, en el que conocen a la mayor parte de sus proveedores. Por eso, les resulta más sencillo identificar correos fraudulentos de manera casi inmediata. En caso de tener dudas, suelen llamar por teléfono para asegurarse de que se trata de una comunicación real e inofensiva. De cara a evitar el phishing[1], hacen lo mismo con las interacciones con los bancos.

Explican que procuran tener claves seguras, actualizarlas con regularidad y tener claves diferentes para procesos dispares. Por otro lado, diversifican sus cuentas de correo electrónico. Por ejemplo, tienen un correo para los pedidos que reciben de sus clientes; otro para los presupuestos (interno); otro para dar información general a los (potenciales) clientes. También tienen uno para las comunicaciones con empresas de servicios (gas, luz, teléfono, etc.). En este caso, si reciben una comunicación de su proveedor de luz y les llega en la dirección de los pedidos específicos para los clientes, ya están en alerta automáticamente.

Otra de sus acciones consiste en hacer uso de VPN con el fin de encriptar la información que emiten y reciben desde el PC o teléfono inteligente. En el caso del PC, señalan que suelen tener el antivirus actualizado. No obstante, con los teléfonos inteligentes, eso no es tan común y les preocupa que no se suele actualizar los sistemas operativos con la misma frecuencia. Por ese motivo, tienen habilitado el uso de la VPN en sus teléfonos inteligentes, asegurándoles una mayor tranquilidad.

[1] **Phishing:** El phishing es una técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo. - INCIBE

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

La página web está basada en un servidor seguro e informan a sus clientes que sus datos solo se utilizan para procesar los pedidos.

Para los pagos en su tienda online han habilitado la opción de pago mediante PayPal. Han detectado que, al menos para el primer pago, sus clientes lo demandaban para sentirse más seguros.

Conforme iban desarrollando su web y tienda online, fueron implementando medidas de ciberseguridad en paralelo. Este proceso les llevó aproximadamente unos seis meses.

Tecnologías y herramientas empleadas

- VPN
- Servidor seguro en la página web
- Antivirus actualizado
- Actualización sistemas operativos
- Banca electrónica segura con VPN en el PC en la oficina para el pago de facturas, etc.
- Forma de pago segura a través de PayPal
- Copias de seguridad tanto en la nube como en local en distintos dispositivos

Estas tecnologías son de bajo coste, y algunas incluso gratuitas. El servidor seguro entra por defecto en el coste del hosting y el dominio de una web. En su caso, pagan 15-20€ de forma bienal por el dominio y 75-100€ de forma anual por la página web. Estos costes son asequibles para la mayoría de negocios.

> ***"La VPN que usamos tanto para móviles como PC son gratuitas y tener un servidor seguro entra dentro del coste del mantenimiento normal de la página web por defecto."***

GOBIERNO DE ESPAÑA · VICEPRESIDENCIA PRIMERA DEL GOBIERNO · MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL · red.es · UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

> *“Realmente todo es ponerse y luego simplemente sistematizar los procesos y ser constante.”*

Retos u obstáculos

Para ellas, el principal reto es el que a la implementación de métodos de ciberseguridad pueda resultar desconocida y tediosa.

Esto puede conducir a que se posponga la implementación de medidas de ciberseguridad. Sin embargo, les merecía la pena a cambio de la tranquilidad que les aportaba a su negocio.

Tras iniciarse, no les supuso mucho más trabajo añadido. Tan solo tenían que ser constantes y sistematizar los procesos.

Por otro lado, antes, la TPV virtual no requería la doble verificación en los pagos inferiores a 50€. Consideraron que podía suponer una brecha de ciberseguridad, por ello, han habilitado la opción de que siempre se solicite la doble verificación.

Resultados

Los resultados obtenidos no se materializan tanto en beneficios directos, si no en una mayor tranquilidad tanto para el negocio como para sus (potenciales) clientes. De esta manera, tienen menor riesgo, mayor concienciación, mayor rapidez y agilidad de respuesta antes posibles brechas y riesgos de ciberseguridad.

En general, consideran que todo el proceso de implementación y mantenimiento es sencillo y asumible aun contando con pocos conocimientos, pero siendo diligentes.

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

Lecciones aprendidas

En primer lugar, es importante no dejarse llevar por las barreras iniciales y pensar en todas las ventajas y la gran disminución de riesgos que su implantación conlleva. Por otro lado, también es esencial implementar medidas de seguridad a tiempo y no esperar a tener un susto que pueda acabar con el negocio. Seguir una serie de normas básicas puede traer consigo una serie de beneficios que no implica una gran pérdida de tiempo para la empresa.

Planes de futuro

Actualmente no cuentan con planes definidos, más allá de mantenerse actualizados y siguiendo boletines semanales que alertan de posibles riesgos y brechas de ciberseguridad.

El estudio de buenas prácticas ha mostrado cómo, siendo constantes y siguiendo una serie de pasos, contar con una estrategia de ciberseguridad, es algo que está al alcance de cualquier negocio a muy bajo coste.

De este modo, se aumenta la confianza del cliente, y se reducen los riesgos.

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"

Acelera *pyme*

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
"Una manera de hacer Europa"