SECURE SOLUTIONS

CYBERSECURITY

# Integración de medidas de seguridad en una empresa

Lukas Clifford Vogdt Torralba

# Introducción

En Secure Solutions, entendemos los desafíos de ciberseguridad que enfrentan las pequeñas empresas. PureOlive, una empresa de exportación de aceite de oliva, ha sufrido intentos de robo de contraseñas corporativas, poniendo en riesgo sus datos y la información de sus clientes. Nuestro objetivo es implementar medidas de seguridad efectivas para proteger su información y garantizar la continuidad de su negocio.

# 1. Investigación y planificación

PureOlive cuenta con las siguientes características:

- Planta de Producción: Utiliza robots para facilitar el proceso de elaboración de aceite de oliva.
- Trabajo Remoto y Coworking: Los responsables y personal de administración trabajan en remoto o desde espacios de coworking, con empleados residiendo en distintas zonas.
- Frecuentes Viajes Internacionales: Especialmente a China, donde realizan reuniones en instalaciones de clientes u hoteles.

Este tipo de trabajo hace que PureOlive sea más vulnerable a ataques cibernéticos. Además, algunos empleados, especialmente los mayores, no tienen mucha formación en ciberseguridad, lo que aumenta los riesgos.

## Identificación de amenazas y riesgos comunes

### Phishing

El phishing es una técnica de ingeniería social que busca engañar a los empleados para que revelen información confidencial, como contraseñas. Este riesgo es especialmente alto en PureOlive debido al trabajo remoto y la dispersión geográfica de los empleados, quienes suelen depender de comunicaciones por correo electrónico y plataformas de mensajería.

### Malware y ransomware

El malware y el ransomware pueden infectar dispositivos mediante archivos adjuntos en correos electrónicos o sitios web comprometidos. En PureOlive, los dispositivos utilizados en la planta de producción y por empleados en remoto son susceptibles a este tipo de ataques.

### Conexiones inseguras en redes públicas

El uso de redes públicas en coworkings, hoteles y durante viajes a China puede exponer las comunicaciones de PureOlive a interceptaciones o ataques de intermediario (Man-In-The-Middle)

## Propuestas de actuación

| AMENAZAS | PROPUESTAS |
|---|---|
| Phishing | Capacitación en Ciberseguridad<br>Autenticación Multifactor (MFA)<br>Política de Contraseñas Seguras |
| Malware y ransomware | Software Antivirus y Antimalware<br>Actualizaciones y Parches de Seguridad |
| Conexiones inseguras en redes públicas | Capacitación en Seguridad de Redes<br>Uso de VPN (Red Privada Virtual)<br>Prohibición de Redes Públicas Inseguras<br>Firewalls y Monitoreo de Red |

# 2. Presentación

**Presentador: Lukas Clifford, Consultor de Seguridad en Secure Solutions**

"Hola, mi nombre es Lukas Clifford y hoy vamos a hablar sobre cómo proteger a PureOlive de las amenazas cibernéticas más comunes. Sabemos que han tenido intentos de robo de contraseñas, y queremos ayudarles a prevenir futuros problemas.

Primero, hablemos de **phishing y robo de credenciales**. Esto ocurre cuando alguien intenta engañar a los empleados para que entreguen información confidencial. Para evitarlo, proponemos capacitación en ciberseguridad, uso de **autenticación multifactor (MFA)** y una política de contraseñas seguras.

**Público**: "¿Cómo funciona la autenticación multifactor?"
**Lukas**: "Buena pregunta. La MFA añade una capa extra de seguridad pidiendo una verificación adicional, como un código en el móvil. Esto hace que sea mucho más difícil que alguien acceda a las cuentas incluso si tiene la contraseña."

Otra amenaza importante es el **malware y ransomware**. Estos programas maliciosos pueden infectar dispositivos o bloquear archivos hasta que se pague un rescate. Para protegernos, recomendamos **software antivirus y antimalware**, así como mantener actualizados todos los sistemas.

**Público**: "¿Realmente es necesario actualizar tan seguido?"
**Lukas**: "¡Absolutamente! Las actualizaciones arreglan errores de seguridad que los hackers podrían aprovechar. No actualizar es como dejar la puerta abierta a los atacantes."

Por último, debemos hablar de conexiones no seguras en **redes públicas**. Esto es un riesgo cuando los empleados viajan y se conectan desde hoteles o cafeterías. La solución es usar **VPNs** para proteger las conexiones, prohibir el uso de redes públicas para asuntos de trabajo y mantener **firewalls** activados para monitorear la red.

Si tienen preguntas adicionales, estaré encantado de responderlas. ¡Gracias por su atención!"

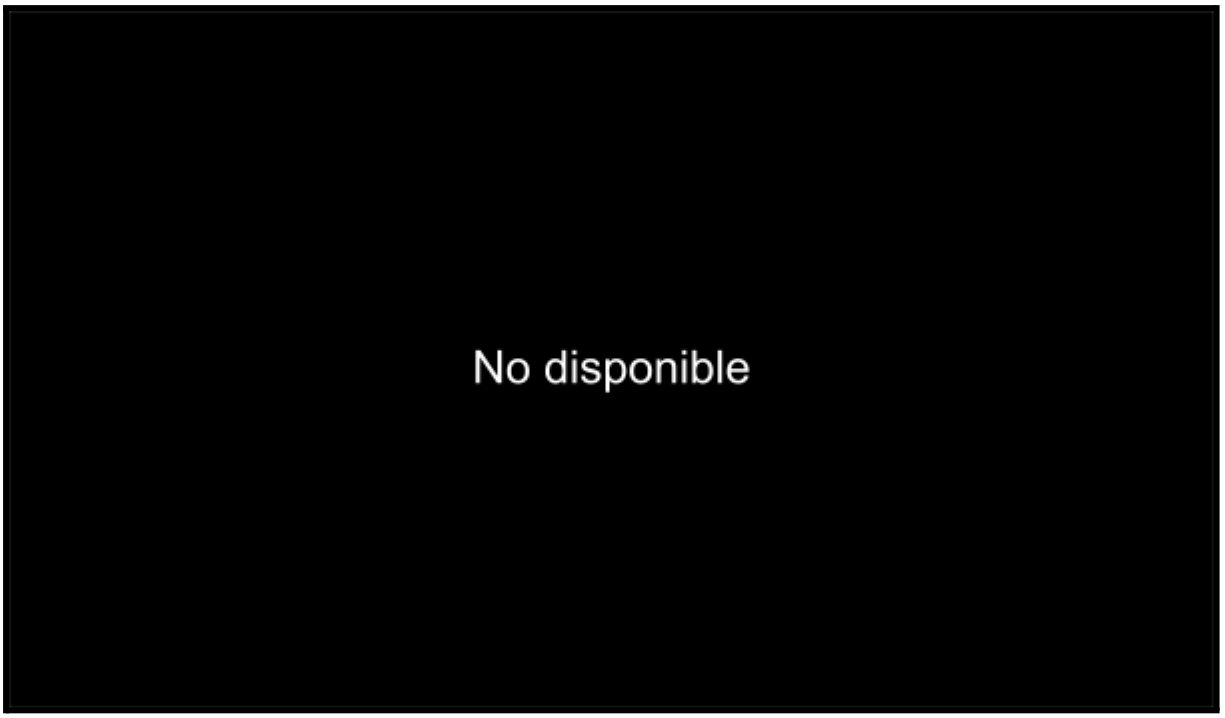
# 3. Puesta en práctica

## Cuestionario:

1) **Cual de estos dos correos electrónicos es falso**

a)


b)



2) **Crea una contraseña segura. Debe tener mínimo 12 caracteres, combinación de mayúsculas, minúsculas, números y símbolos.**

_____

3) **Un empleado de la empresa se encuentra en un hotel y necesita acceder a documentos sensibles en su portátil. ¿Cuál de las siguientes opciones es la más segura para conectar su dispositivo a la red y acceder a esos documentos? Marque la respuesta correcta.**

a) Conectarse a la red Wi-Fi pública del hotel sin utilizar ninguna medida de seguridad.

b) Conectarse a la red Wi-Fi del hotel y usar una VPN (Red Privada Virtual) para proteger la conexión.

c) Usar datos móviles para acceder a los documentos sin necesidad de una VPN.

d) Conectarse a la red Wi-Fi pública del hotel y luego hacer clic en enlaces no verificados para asegurarse de que está usando una red legítima.

4) **Un empleado de la empresa recibe un correo electrónico con un archivo adjunto que parece provenir de un proveedor de servicios. El archivo tiene un nombre que parece legítimo, como "Factura_Proveedor_X.pdf". El empleado abre el archivo y, en ese momento, su computadora comienza a comportarse de manera extraña (lentitud, ventanas emergentes, y error al abrir otros documentos).**

**Responde las siguientes preguntas en base al caso planteado.**

1. **¿Qué debe hacer el empleado al recibir un correo electrónico con un archivo adjunto sospechoso?**

2. **Si el archivo ya ha sido abierto y el sistema comienza a comportarse de manera extraña, ¿qué debe hacer el empleado primero**?

3. **¿Cuál es el siguiente paso que debe seguir el empleado para proteger el sistema?**

4. **¿A quién debe notificar el empleado sobre este incidente?**

5. **¿Qué debe hacer el equipo de TI después de recibir la notificación del empleado?**

6. **¿Qué acción debe tomar el empleado con respecto al archivo malicioso después de haber sido informado por TI?**

**Evaluación de la Presentación**

- ¿Te ha parecido útil la información presentada? (Sí / No)
- ¿Consideras que las propuestas son aplicables en tu trabajo diario? (Sí / No)
- ¿Recomendarías esta formación a otros compañeros? (Sí / No)
- Comentarios adicionales:

SECURE SOLUTIONS
CYBERSECURITY

Secure Solutions
Protección avanzada en ciberseguridad para tu empresa.

Dirección: Calle de la Seguridad Cibernética, 404, puerto 80 | Córdoba, 14005, España
Teléfono: +34 168 192 0 99 | Email: contacto@securesolutions.com
Web: www.securesolutions.com

Redes Sociales:
Facebook: @SecureSolutions | Twitter: @Secure_Solutions | LinkedIn: Secure Solutions

Atención al cliente: Lunes a Viernes: 9:00 - 18:00 | Sábados: 10:00 - 14:00