PROYECTO RETAIL

CONTENIDOS ADICIONALES

Ciberseguridad en el proceso de digitalización

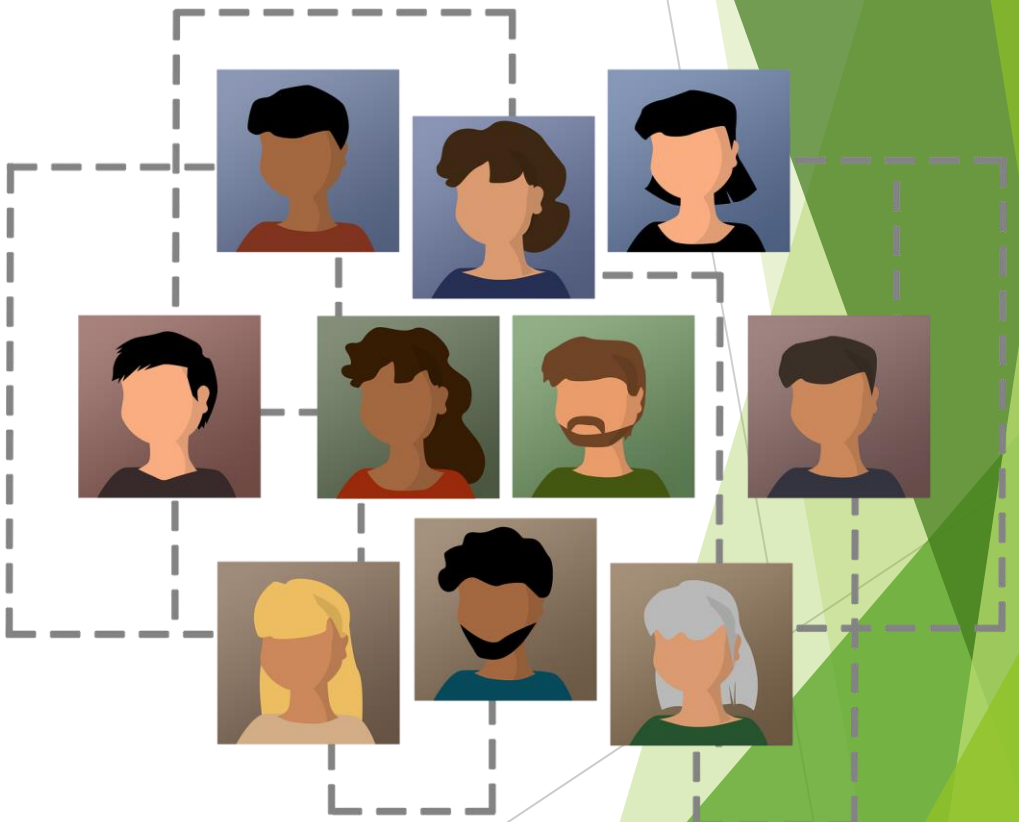
PROYECTO RETAIL

Erasmus+	Proyecto financiado por: **Erasmus+ / Acción Clave 2 - Cooperación para la innovación y el intercambio de buenas prácticas; Asociaciones estratégicas para la educación VET**

Proyecto Retail www.retail.erasmus.site

1. Introducción del tema
2. Contenidos de Aprendizaje
- Capítulo1: Las amenazas cibernéticas más comunes
- Capítulo 2: ¿Cómo proteger tu negocio?
- Capítulo 3: Nuevas tecnologías y ciberseguridad
3. Actividad práctica
4. Herramientas útiles
5. Fuentes

1. Introducción al tema



El Covid-19 ha obligado a muchas empresas a acelerar su transición digital.

La digitalización puede respaldar las operaciones de una empresa y permitirle crecer de una manera sin precedentes; sin embargo, también puede ser una puerta de entrada a los ataques cibernéticos o al robo de datos. Por lo tanto, es importante prepararse para esta posibilidad y saber cómo podemos asegurar nuestros negocios.

Naturalmente, cada empresa debe realizar acciones adaptadas a su perfil y nivel de digitalización, pero hay algunos puntos en común a tener en cuenta a la hora de trabajar para garantizar la ciberseguridad.

2. Contenidos

Este módulo adicional se dividirá en 3 capítulos, una actividad práctica, referencias y otras herramientas.

- Capítulo 1: Las amenazas cibernéticas más comunes.
- Capítulo 2: ¿Cómo proteger su negocio?
- Capítulo 3: Nuevas tecnologías y ciberseguridad

2.1. Las amenazas cibernéticas más comunes

CONTENIDO DEL CAPÍTULO 1
Las amenazas cibernéticas más communes.

1. Malware

Malware es la abreviatura de "software malicioso" y puede ser un fragmento de código/programa cuyo propósito es interrumpir las operaciones, robar datos o dañar el hardware. Estos incluyen troyanos, gusanos y software espía populares.

2. Phishing

Esto es hacerse pasar por una persona o institución e intentar extorsionar al usuario con dinero o datos.

3. “Hombre en el medio”

Un pirata informático "entra" entre las interacciones de 2 entidades a través, por ejemplo, de una conexión Wi-Fi mal protegida con la intención de robar información, datos personales, etc.

2.2.1. ¿Cómo proteger tu negocio?

Básicamente, hay dos elementos principales a los que debe prestar atención:

Recursos Humanos

Las estadísticas muestran que la gran mayoría de las amenazas cibernéticas se deben a una formación deficiente de los empleados y a errores humanos.

Recursos de Hardware

Esto incluye todos los ordenadores portátiles, software, antivirus y posibles pasarelas utilizadas para ataques de piratas informáticos.

CONTENIDO DEL CAPÍTULO 2
¿Cómo proteger tu negocio?
Recursos humanos y ciberseguridad
Recursos de hardware y ciberseguridad
Protección de datos personales

2.2.2. Recursos Humanos y ciberseguridad

Los recursos humanos juegan un papel fundamental para garantizar la seguridad cibernética

Se estima que hasta el 90% de los problemas de ciberseguridad están relacionados con errores humanos. Las amenazas de seguridad pueden manifestarse en una variedad de comportamientos (potencialmente peligrosos) como: conectar dispositivos externos (como unidades USB) que pueden llevar malware peligroso o abrir correos electrónicos que provienen de fuentes desconocidas. Existen muchas prácticas peligrosas, pero la fuente más común del problema son las brechas en la educación de los empleados sobre seguridad cibernética.

Para contrarrestar esto en las pymes se recomienda que:

- Crea un plan de políticas, procedimientos y contramedidas de seguridad.
- Asegúrate de que haya simulacros a los empleados profesionales en el lugar de trabajo con demostraciones de los diversos comportamientos peligrosos que deben evitarse.

2.2.3. Recursos de hardware y ciberseguridad

Los recursos de hardware deben estar debidamente protegidos para proteger los datos recopilados por la empresa.

Es muy importante asegurarse de que tu equipo está debidamente protegido contra posibles ciberataques. Hay una variedad de herramientas disponibles para este propósito. La protección más obvia es tener un software antivirus. Puedes encontrar una lista de ejemplos aquí: https://www.usnews.com/360-reviews/antivirus

Los cortafuegos también son una necesidad. Aunque su eficacia no es tan alta como antes y un pirata informático experto puede evitarlos, siguen siendo la primera línea de defensa y pueden evitar la entrada no autorizada al sistema. Si decide operar en línea, esto, por supuesto, abre un nuevo conjunto de desafíos de seguridad (especialmente para los clientes). Debe comenzar por asegurarse de que su tienda está debidamente protegida con SSL y TLS (la tecnología responsable del cifrado y HTTPS, el popular candado junto a la dirección del sitio web).

2.2.4. Protección de datos personales

Preocuparse por la seguridad cibernética también implica preocuparse por los datos y la información que almacena, incluida la información personal de sus clientes y empleados.

El GDPR (Reglamento General de Protección de Datos) ha estado en vigor en la Unión Europea desde 2018 (el reglamento completo está disponible aquí).

Esto significa que el almacenamiento de datos debe cumplir con determinadas medidas de protección.

El GDPR ha introducido nuevos derechos para los ciudadanos (por ejemplo, el "derecho al olvido") y nuevas obligaciones para las empresas tanto en sus operaciones físicas como online. Entre esas obligaciones se encuentra, por ejemplo, la obligación de introducir principios de privacidad en la etapa de diseño (por ejemplo, de una tienda). Estos son: privacidad por diseño o privacidad por defecto.

2.3. Nuevas tecnologías y ciberseguridad

CONTENIDO DEL CAPÍTULO 3
Nuevas tecnologías y ciberseguridad

La cuarta revolución industrial (Industria 4.0) está llevando a las empresas a una nueva era de dispositivos conectados. Si bien sus aspectos positivos son numerosos, también conlleva ciertos riesgos.

Uno de ellos está conectado con el Internet de las cosas, que, en términos simples, implica conectar una multitud de dispositivos que pueden interactuar sin la participación humana.

Esto conlleva el riesgo de que una cantidad tan grande de dispositivos conectados (se estima que habrá hasta 25.400 millones de dispositivos IoT en 2030) será una puerta de entrada para los piratas informáticos que, al irrumpir en los dispositivos menos seguros, podrán acceder a los elementos más importantes de la infraestructura en las empresas.

3. Actividad Práctica

Para practicar, piensa en el nivel de seguridad cibernética de tu empresa

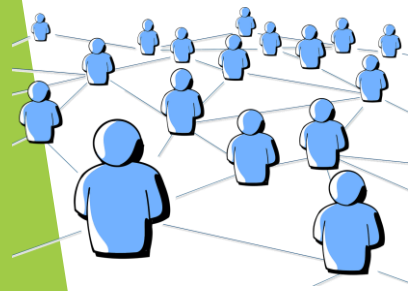
1. ¿Qué formación estás proporcionando a tus empleados?
2. ¿Cómo puede mejorar tus propias competencias en seguridad cibernética?
3. ¿Están bien protegidos los datos de sus clientes?
4. ¿Está utilizando un software antivirus actualizado?
5. ¿Tiene un plan en caso de que ocurra un incidente cibernético?

4. Herramientas útiles

GDPR
Link: https://gdpr-info.eu/

Video sobre ciberseguridad
Link: https://www.youtube.com/watch?v=inWWhr5tnEA

Ciberseguridad para pequeñas empresas
Link: https://www.fcc.gov/general/cybersecurity-small-business



5. Fuentes

Cybersecurity 101: Introducción a los 10 tipos más comunes de ataques de ciberseguridad:
Link: https://www.infocyte.com/blog/2019/05/01/cybersecurity-101-intro-to-the-top-10-common-types-of-cyber-security-attacks/

Por qué educar a sus empleados sobre la ciberinteligencia y la seguridad reducirá el riesgo :
Link: https://www.cybintsolutions.com/employee-education-reduces-risk/

Qué es GDPR
Link: https://www.powerdata.es/gdpr-proteccion-datos

PROYECTO RETAIL
Partenariado

Proyecto Retail www.retail.erasmus.site