CIBERPLUS
CYBER SECURITY SOLUTIONS

PERSPECTIVA DE LA CIBERSEGURIDAD DE MICROEMPRESAS Y AUTÓNOMOS DE TENERIFE

innovalia ASSOCIATION

AÑO 2024

Financiado por el Cabildo Insular de Tenerife

PERSPECTIVA CIBERSEGURIDAD

CONTENIDO

CIBERPLUS

1. INTRODUCCIÓN

El proyecto CIBERPLUS es una iniciativa para la **concienciación, formación, diagnóstico y plan de acción en ciberseguridad.**

Está dirigida a **micropymes y autónomos del sector industrial y artesanal de Tenerife**, para la mejora de su estrategia digital.

Este documento sobre la ***Perspectiva de la Ciberseguridad en Tenerife***, tiene como propósito mostrar información sobre la **situación actual en ciberseguridad de las microempresas y emprendedores autónomos**, tanto **industriales** como **artesanales**, de la isla.

CIBERPLUS

2. RESUMEN EJECUTIVO

El proyecto CIBERPLUS se ha desarrollado de acuerdo al siguiente plan de trabajo:

FASE 1: SENSIBILIZACIÓN Y DIFUSIÓN EN CIBERSEGURIDAD

FASE 2: FORMACIÓN EN CIBERSEGURIDAD

FASE 3: DIAGNÓSTICO Y EVALUACIÓN DE MADUREZ

RESULTADOS

FASE 4: JORNADA DE DIFUSIÓN DE RESULTADOS

FASE 5: GESTIÓN DEL PROYECTO

La perspectiva de la ciberseguridad de microempresas y autónomos de Tenerife se basa en la ejecución y resultados de la **Fase 3**

CIBERPLUS

2. RESUMEN EJECUTIVO

DIAGNÓSTICO. La metodología para la ejecución del diagnóstico se explica a continuación:

- Se realiza una selección de empresas objeto de estudio.
- Se diseña y aplica **una herramienta** para determinar el **nivel de madurez en ciberseguridad** de las empresas participantes.
- **Se realiza el diagnóstico aplicando** un cuestionario de 50 preguntas agrupadas en 10 dimensiones.

PERSPECTIVA CIBERSEGURIDAD

2. RESUMEN EJECUTIVO

- La escala establece niveles de 1 a 5.
- Con los resultados obtenidos se determinó el **nivel de madurez promedio** en ciberseguridad de las empresas de la isla de Tenerife.
- Se realizó un **análisis de los resultados** según las dimensiones estudiadas y según la categoría de las deficiencias que pudieran originar las debilidades.

El **promedio en ciberseguridad en Tenerife** es

Nivel 2

PERSPECTIVA CIBERSEGURIDAD

3. PARTICIPANTES

Perfil

Utilizando las características de los participantes se realizó una selección representativa y balanceada del sector que se quería estudiar.

De esta manera tenemos que,

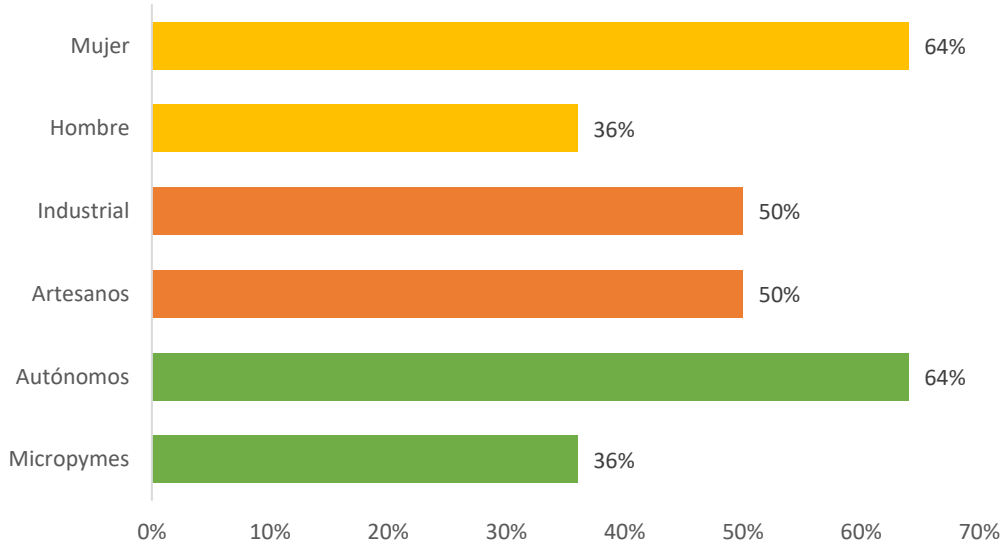
- El 36% son micropymes y el 64% son Autónomos.
- El 50% son artesanos y el otro 50% son industriales.
- El 64% son dirigidos por mujeres y el 36% son dirigidos por hombres.
- La distribución geográfica de los participantes es homogénea y representativa de toda la isla de Tenerife.

PERSPECTIVA CIBERSEGURIDAD

3. PARTICIPANTES

De forma gráfica

Por tamaño		Por sector		Por dirección	
Micropymes	Autónomos	Artesanos	Industrial	Hombre	Mujer
36%	64%	50%	50%	36%	64%



PERSPECTIVA CIBERSEGURIDAD

3. PARTICIPANTES

Distribución territorial de los participantes

La distribución geográfica de los participantes es homogénea y representativa de toda la isla de Tenerife.

PERSPECTIVA CIBERSEGURIDAD

3. PARTICIPANTES: Sectores de actividad de los participantes

Entre los sectores de actividad de los participantes podemos mencionar: trabajo con metales, fundición, fabricación de joyas, cerveza, vino, porcelana, fabricación de calzado, comercio al por menor, confección de prendas de vestir, tejidos, productos para el cuidado de la piel, fabricación y decoración de accesorios, velas artesanales, alfarería, pintura, etc.

PERSPECTIVA CIBERSEGURIDAD

4. DIAGNÓSTICO Y EVALUACIÓN DE MADUREZ

Contenido del diagnóstico

Las dimensiones en las que está estructurado el cuestionario del diagnóstico son las siguientes:

D1 EVALUACIÓN DE RIESGOS
D2 POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD
D3 CONTROL DE ACCESO
D4 PROTECCIÓN DE DATOS
D5 EDUCACIÓN Y CAPACITACIÓN
D6 MONITORIZACIÓN Y AUDITORÍA
D7 PLAN DE RESPUESTAS A INCIDENTES
D8 GESTIÓN DE CONTRASEÑAS
D9 SEGURIDAD DE LA RED
D10 CUMPLIMIENTO NORMATIVO

PERSPECTIVA CIBERSEGURIDAD

4. DIAGNÓSTICO Y EVALUACIÓN DE MADUREZ

Organización de los datos

- Cada dimensión se evalúa sobre **10 puntos**. Consecuentemente, la valoración máxima para una organización es de **100 puntos**.

- Cada dimensión se evalúa a través de 5 áreas específicas.

- La puntuación para cada área sigue la siguiente escala:
  - **Positiva (2 puntos)**. Se asigna un 2 cuando la respuesta es positiva, es decir, el sistema al que se refiere la pregunta es adecuado.
  - **En proceso (1 punto).** Se asigna 1 cuando obtenemos una respuesta intermedia, es decir, que la empresa declara que ya había pensado sobre el sistema y lo va a implantar, pero todavía no lo ha hecho.
  - **Negativa (0 puntos)**. Se asigna un 0 cuando la respuesta es negativa, es decir los sistemas son débiles o inexistentes en cuanto a ciberseguridad.

PERSPECTIVA CIBERSEGURIDAD

4. DIAGNÓSTICO Y EVALUACIÓN DE MADUREZ

Relación entre la puntuación y el nivel de madurez

La relación entre la puntuación y el nivel de madurez en ciberseguridad de cada entidad se determina según los resultados obtenidos, conforme a la equivalencia establecida en la siguiente tabla.

NIVEL		PUNTUACIÓN
1	INICIAL	Entre 1 y 20 puntos
2	GESTIONADO	Entre 21 y 37 puntos
3	DEFINIDO	Entre 38 y 54 puntos
4	GESTIONADO Y MEDIDO	Entre 55 y 70 puntos
5	ADAPTATIVO	Entre 71 y 100 puntos

PERSPECTIVA CIBERSEGURIDAD

4. DIAGNÓSTICO Y EVALUACIÓN DE MADUREZ

Valoración del nivel de madurez.

NIVEL 1: INICIAL (BÁSICO) PUNTUACIÓN entre **1 y 20 puntos**. En este nivel, las prácticas de ciberseguridad son ad hoc y no están documentadas. Las empresas dependen de la conciencia individual y la reacción a incidentes en lugar de procesos predefinidos.

NIVEL 2: GESTIONADO (INTERMEDIO BÁSICO) PUNTUACIÓN entre **21 y 37 puntos**. Los participantes de este nivel, están empezando a implementar políticas y procedimientos básicos de ciberseguridad. La gestión de la seguridad es más organizada, pero aún no está completamente integrada en todos los procesos empresariales.

NIVEL 3: DEFINIDO (INTERMEDIO AVANZADO) PUNTUACIÓN entre **38 y 54 puntos**. La ciberseguridad se convierte en una parte integral de las operaciones diarias de la empresa. Las políticas y procedimientos están bien definidos y son seguidos por toda la organización. Se comienza a implementar tecnología más avanzada y procesos de gestión proactivos.

NIVEL 4: GESTIONADO Y MEDIDO (AVANZADO) PUNTUACIÓN entre **55 y 70 puntos**. La organización tiene una comprensión profunda de su postura de seguridad y utiliza métricas para medir y mejorar continuamente sus prácticas de ciberseguridad. La gestión de la seguridad es proactiva y basada en el riesgo, con un enfoque en la mejora continua.

NIVEL 5: ADAPTATIVO (MUY AVANZADO) PUNTUACIÓN superior a **70 puntos.** Es el nivel más avanzado, la organización es altamente resiliente y puede adaptarse rápidamente a nuevas amenazas. La ciberseguridad es un componente estratégico del negocio, con capacidades de inteligencia y respuesta avanzadas.

PERSPECTIVA CIBERSEGURIDAD

5. RESULTADOS DEL DIAGNÓSTICO

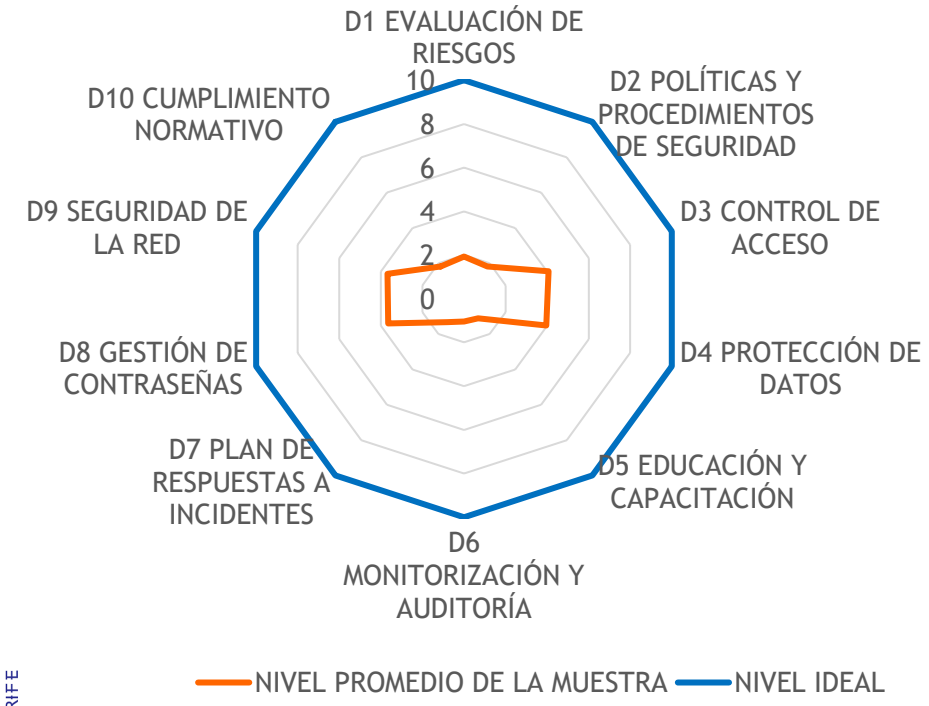
a. Resultados y análisis de la puntuación promedio por dimensión

RESULTADOS PARA TENERIFE PUNTUACIÓN PROMEDIO	
DIMENSIÓN	**PUNTUACIÓN PROMEDIO/DIMENSIÓN**
D1 EVALUACIÓN DE RIESGOS	1,93
D2 POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD	1,82
D3 CONTROL DE ACCESO	4,07
D4 PROTECCIÓN DE DATOS	3,96
D5 EDUCACIÓN Y CAPACITACIÓN	1,11
D6 MONITORIZACIÓN Y AUDITORÍA	1,04
D7 PLAN DE RESPUESTAS A INCIDENTES	1,32
D8 GESTIÓN DE CONTRASEÑAS	3,64
D9 SEGURIDAD DE LA RED	3,68
D10 CUMPLIMIENTO NORMATIVO	1,82
PUNTUACIÓN PROMEDIO TENERIFE	**24,39**

PERSPECTIVA CIBERSEGURIDAD

5. RESULTADOS DEL DIAGNÓSTICO

a. Resultados y análisis de la puntuación promedio por dimensión



Los valores de la tabla anterior se trasladaron a una gráfica radial que muestra la **puntuación promedio de los participantes en cada dimensión (Línea naranja).** La línea azul corresponde al nivel máximo de puntuación que se podría obtener.

Globalmente, **la puntuación promedio de 24,39 puntos sobre 100, equivale a un Nivel 2 de Madurez.** En este nivel, los participantes, están empezando a implementar políticas y procedimientos básicos de ciberseguridad. Por ejemplo, existe alguna gestión de la seguridad, pero aún no está completamente integrada en todos los procesos.

Este resultado muestra que la valoración actual tiene un amplio margen de mejora.

PERSPECTIVA CIBERSEGURIDAD

5. RESULTADOS DEL DIAGNÓSTICO

b. Resultados y análisis global del nivel de madurez en ciberseguridad

Como se puede observar en la gráfica, un 39% alcanzaron el Nivel 1 y otro 39% alcanzó el Nivel 2.

Esto significa que **el 78% de los participantes están ubicados en los niveles 1 y 2, ambos bastante básicos en cuanto a ciberseguridad**.

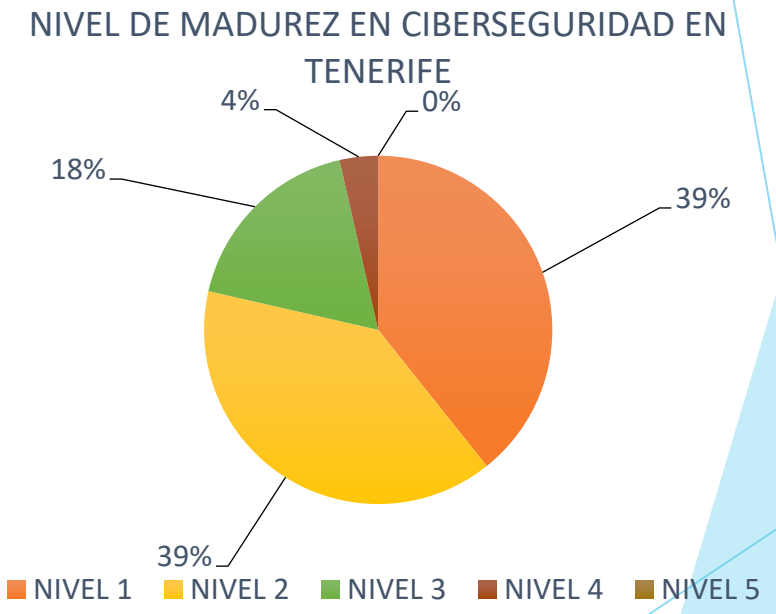
Sólo el 18 % de las empresas alcanzaron el Nivel 3.

Sólo un 4% de las empresas llegó al nivel 4.

Ninguno de los participantes alcanzó el Nivel 5.

Las entidades que alcanzaron el Nivel 3 son en su mayoría micropymes del sector industrial.

Las entidades que alcanzaron el Nivel 4 son en su mayoría del sector industrial.



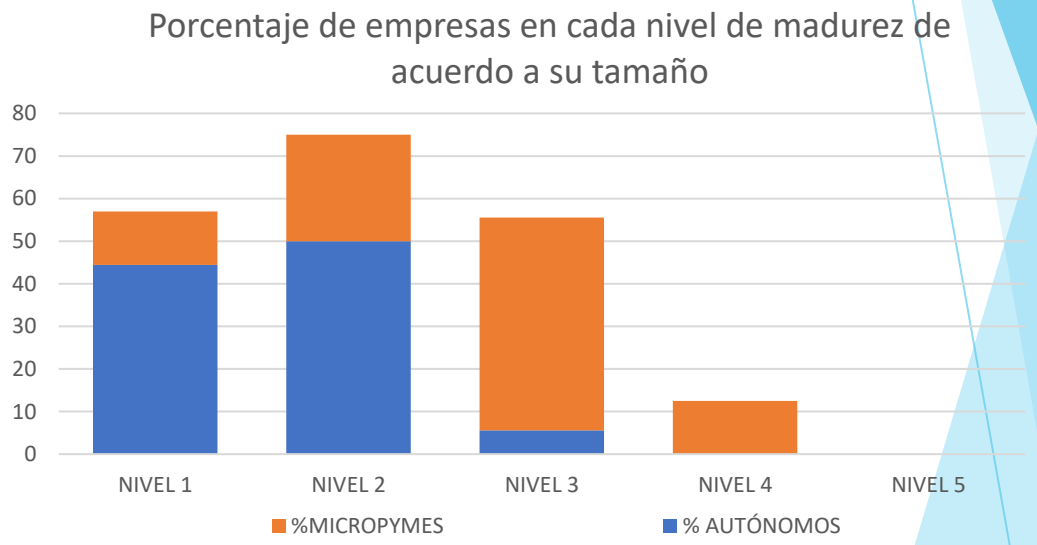
PERSPECTIVA CIBERSEGURIDAD

5. RESULTADOS DEL DIAGNÓSTICO

c. Análisis comparativo del nivel de madurez por tamaño de la empresa

Tamaño empresa	Puntuación promedio	Nivel Promedio
Micropyme	38	Nivel 3
Autónomo	21	Nivel 2

	% AUTÓNOMOS	% MICROPYMES
NIVEL 1	44 %	13 %
NIVEL 2	50 %	25 %
NIVEL 3	6 %	50 %
NIVEL 4	0 %	13 %
NIVEL 5	0 %	0 %



Si analizamos los datos por tamaño de empresa, comparando los autónomos con los que están constituidos como micropymes, encontramos los siguientes resultados.

Un 94% de los Autónomos (área azul de la gráfica) **están entre el Nivel 1 y 2.**

Por su parte, **63 % de las Micropymes** (área naranja de la gráfica) están entre los **Niveles 3 y 4.**

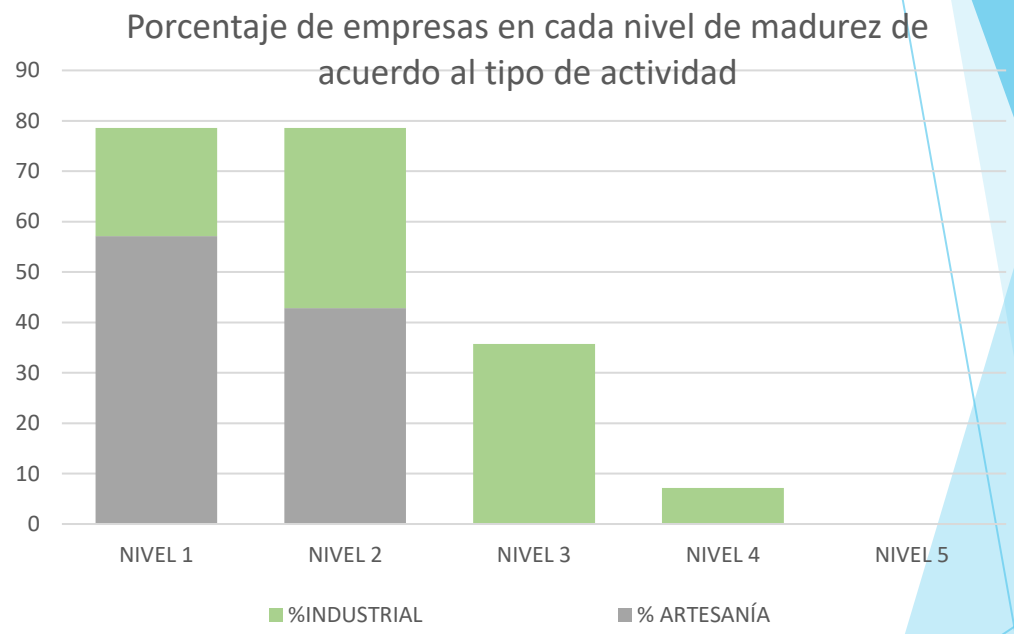
PERSPECTIVA CIBERSEGURIDAD

5. RESULTADOS DEL DIAGNÓSTICO

d. Análisis comparativo del nivel de madurez por sector de actividad

Sector de la empresa participante	Puntuación promedio	Nivel Promedio
Artesanía	18	Nivel 1
Industrial	31	Nivel 2

	% ARTESANÍA	% INDUSTRIAL
NIVEL 1	57 %	21 %
NIVEL 2	43 %	36 %
NIVEL 3	0 %	36 %
NIVEL 4	0 %	7 %
NIVEL 5	0 %	0 %



Si analizamos los datos por tipo de actividad de las empresas, encontramos que:

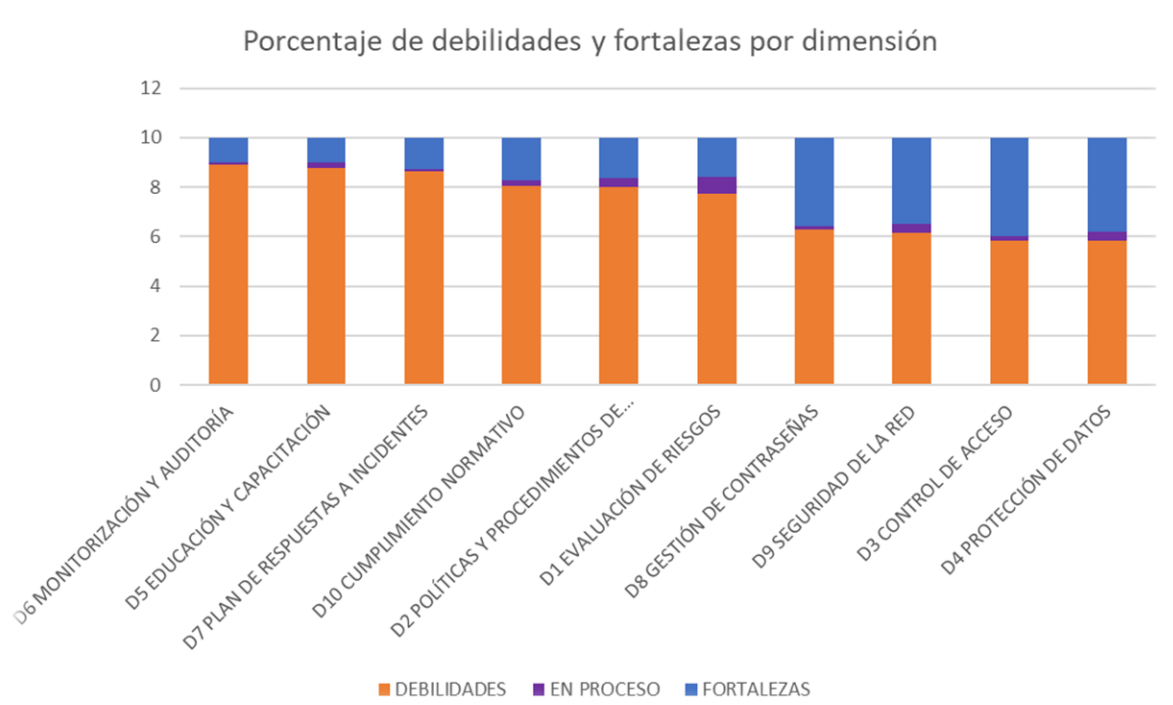
Todos los **Artesanos** (color gris en la gráfica) están entre el **Nivel 1 y 2.**

Por su parte, el **70% de los Industriales** (color verde) se encuentran repartidos entre el **Nivel 2 y el 4.**

PERSPECTIVA CIBERSEGURIDAD

5. RESULTADOS DEL DIAGNÓSTICO

e. Resultados y análisis de debilidades por dimensión



En la gráfica, la **zona naranja** representa el porcentaje de respuestas negativas (que se relacionan con **debilidades**).

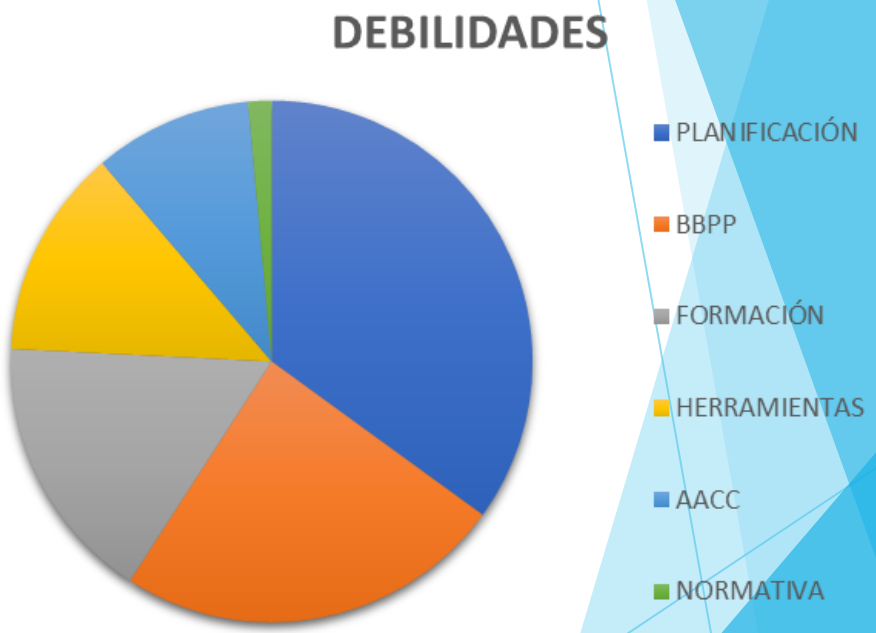
Las principales debilidades se centran en las dimensiones de **Monitorización y Auditoría, Educación y Capacitación, y Planes de Acción ante Emergencias, aunque ninguna destaca de forma significativa.**

PERSPECTIVA CIBERSEGURIDAD

5. RESULTADOS DEL DIAGNÓSTICO

f. Resultados y análisis de acuerdo al tipo de debilidad

Para facilitar el análisis se identificó la relación entre cada dimensión, el tipo de debilidad en categorías y su causa. Estas categorías fueron definidas como:

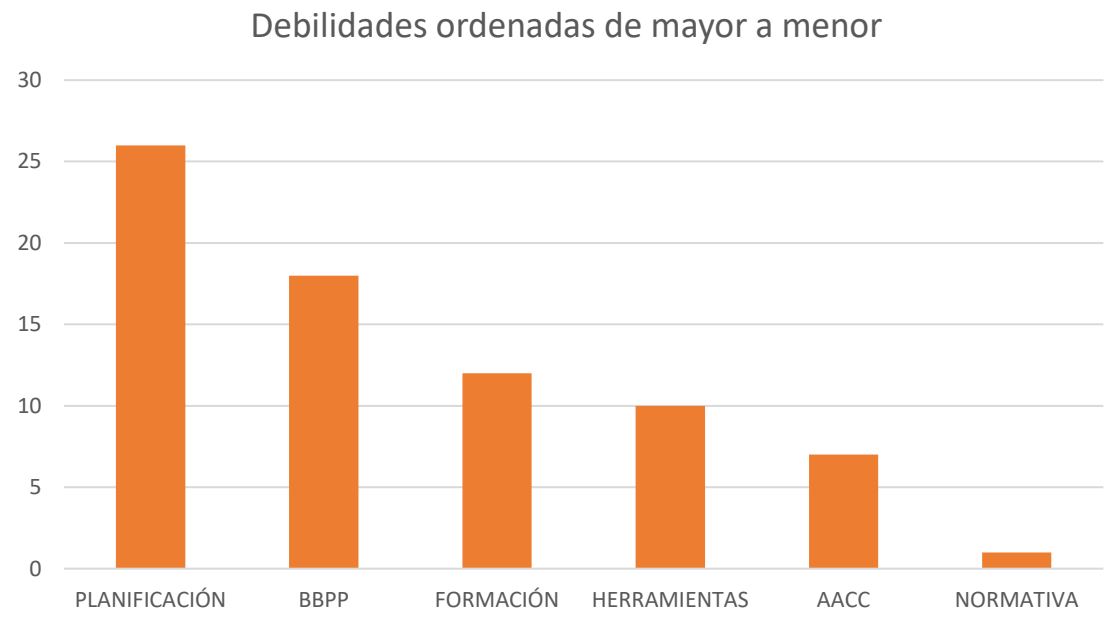


- **BUENAS PRÁCTICAS** (BBPP): corresponde a, formas de hacer, frecuencias, cumplimiento de normas internas, por ejemplo, borrar datos que no se estén utilizando, no usar redes públicas, hacer copias de seguridad con cierta frecuencia, etc.
- **NORMATIVA**: cumplimiento con normas y leyes externas públicas europeas aplicables.
- **PLANIFICACIÓN**: en general, si se tiene establecido o no un sistema de gestión que incluya normas internas, políticas internas, documentos, instrucciones de trabajo, definición de los procesos adecuados para llevar a cabo una actividad
- **HERRAMIENTAS**: uso de software o apps, por ejemplo, uso gestor de contraseñas, uso de doble autenticación.
- **FORMACIÓN**: se refiere a si la gente está formada, si han realizado cursos de ciberseguridad, conocimiento de las normas internas.
- **ACCIONES CORRECTIVAS** (AACC): Se toman medidas cuando se presentan problemas.

PERSPECTIVA CIBERSEGURIDAD

5. RESULTADOS DEL DIAGNÓSTICO

f. Resultados y análisis de acuerdo al tipo de debilidad



En esta gráfica se ordenaron de mayor a menor sólo los datos correspondientes a los tipos de debilidades.

Como resultado se muestra claramente que las **debilidades se concentran en las categorías de Planificación, Buenas Prácticas y Formación.**

PERSPECTIVA CIBERSEGURIDAD

6. RESULTADOS DESTACADOS

El **Nivel de madurez en ciberseguridad** de autónomos y micropymes que se desempeñan en los sectores artesanal e industrial de la isla de Tenerife es de

NIVEL 2: Intermedio básico

Las **principales debilidades** se encontraron en las siguientes áreas:

- **Planificación**
- **Buenas prácticas**
- **Formación**

- **En cuanto al sector,** se encontró que **todos los artesanos** están entre el **Nivel 1 y 2** y el **70% de los industriales** están entre el **Nivel 2 y el 4.**
- **En cuanto al tamaño,** se encontró que el **94% de los autónomos** están entre el **Nivel 1 y 2,** y el **63 % de las micropymes** están entre los **Niveles 3 y 4.**

PERSPECTIVA CIBERSEGURIDAD

6. RESULTADOS DESTACADOS

a. Lecciones aprendidas

- Se ha detectado una alta vulnerabilidad ante ciberataques en las micropymes y autónomos de Tenerife.
- Son personas/empresas que en buena medida no tienen conocimientos específicos en este campo, ni recursos ni tiempo para establecer mecanismos de protección.
- En este sentido, se considera que estos sectores requieren un importante soporte técnico y tecnológico, para superar las debilidades identificadas y avanzar en su nivel de madurez en ciberseguridad.

ESTE DOCUMENTO SOBRE LA PERSPECTIVA DE LA CIBERSEGURIDAD DE MICROEMPRESAS Y AUTÓNOMOS DE TENERIFE SE HA ELABORADO DENTRO DEL PROYECTO CIBERPLUS