Ciberseguridad (Avanzado)

La finalidad de la categoría «Ciberseguridad, Avanzado» es diseñar un plan especializado para aquellas empresas que ya cuentan con una protección básica y un plan de ciberseguridad en marcha, pero que, a pesar de estas medidas, desean ir más allá. Estas empresas buscan no solo mantener su seguridad, sino también reforzarla, explorando y adoptando sistemas de protección más avanzados que les permitan estar mejor preparadas frente a las amenazas cibernéticas emergentes. El objetivo es brindarles las herramientas y el conocimiento necesario para evolucionar su estrategia de ciberseguridad, garantizando que estén equipadas con las tecnologías y prácticas más sofisticadas del mercado, con el fin de mejorar su capacidad de respuesta ante posibles ataques y asegurar una defensa integral en un entorno digital cada vez más complejo y desafiante.

Ciberseguridad Avanzado
- Evaluar y realizar pruebas de penetración, así como un análisis de las posibles vulnerabilidades de la empresa, teniendo en cuenta su entorno tecnológico y operativo: Se llevará a cabo una evaluación detallada del entorno tecnológico en el que opera la empresa, realizando pruebas de penetración para identificar puntos débiles y vulnerabilidades que puedan ser explotadas. Este análisis permitirá comprender mejor las áreas de riesgo y las amenazas específicas a las que la empresa está expuesta.
- Implementar procedimientos y herramientas de ciberseguridad para la gestión diaria, adquisición, configuración, protección preventiva, y para la detección y respuesta ante incidentes: Se establecerán procedimientos claros y se desplegarán herramientas avanzadas de ciberseguridad para cubrir todas las fases críticas de la operación empresarial, desde la adquisición y configuración de sistemas hasta la protección proactiva y la capacidad de respuesta ante incidentes de seguridad.
- Proteger de manera proactiva a la pyme contra ataques dirigidos a sus datos, mejorando la resiliencia y la capacidad de respuesta ante amenazas: Se adoptarán medidas proactivas para salvaguardar los datos de la empresa frente a ataques dirigidos, fortaleciendo su capacidad para resistir y responder eficazmente ante posibles amenazas, con el objetivo de minimizar el impacto de cualquier incidente de seguridad.
- Sensibilizar a los empleados sobre la importancia de la ciberseguridad y fomentar una cultura organizacional centrada en la seguridad y la gestión de riesgos: Se promoverá la concienciación entre los empleados sobre los riesgos cibernéticos y la importancia de la ciberseguridad, impulsando una cultura organizacional que priorice la seguridad en todas las operaciones y decisiones empresariales, y que integre la gestión de riesgos en el día a día de la empresa.
- Identificar oportunidades o posibles aplicaciones de la inteligencia artificial en el ámbito de la ciberseguridad: Se explorarán y se identificarán posibles formas de integrar la inteligencia artificial en las estrategias de ciberseguridad, aprovechando sus capacidades para mejorar la detección de amenazas, automatizar la respuesta a incidentes y optimizar la protección de la empresa.
- Desarrollar y ejecutar un caso de uso personalizado para el negocio, aplicando las técnicas adecuadas en el área de ciberseguridad: Se diseñará y llevará a cabo un caso de uso específico que esté alineado con las necesidades del negocio, utilizando las técnicas más apropiadas en ciberseguridad, con el fin de demostrar la efectividad de las medidas adoptadas y mejorar la protección general de la empresa. Importe de la ayuda

Segmento A: 10 < 50 empleados (6.000€)

Segmento B: 50 < 100 empleados (6.000€)

Segmento C: 100 < 250 empleados (6.000€) << SOLICITAR MAS INFORMACIÓN >>correo@ampinformatica.com