CyberCan

PROMOVIENDO LA CIBERSEGURIDAD
EN CANARIAS

TALLER

cidihub

CANARY ISLANDS DIGITAL INNOVATION HUB

"Digitalización Segura: Claves para un Entorno Empresarial Seguro"

27 de Junio 2024

Gobierno de Canarias

Consejería de Economía, Conocimiento y Empleo

Agencia Canaria de Investigación, Innovación y Sociedad de la Información

Título curso / taller

Datos Generales

Socio CIDIHUB: Centro Tecnológico de Ciencias Marinas (CETECIMA)
Título: Digitalización Segura: Claves para un Entorno Empresarial Seguro
Fecha de inicio: 27/06/2024
Formato: Online
Lugar: Microsoft Teams
Enlace de Inscripción: **https://forms.gle/KQoJHg1XuWqmcG4W9**

Antecedentes

El Centro de Innovación Digital de Canarias, CIDIHUB, es un consorcio de organizaciones y centros competenciales especializados en digitalización empresarial, que aportan infraestructuras y recursos clave para la transformación digital de empresas privadas y entidades públicas, opera principalmente en la región de Canarias, aunque también colabora y trabaja con entidades de otras regiones y de otros países dentro y fuera del continente europeo.

CYBERCAN es una iniciativa promovida por CIDIHUB orientada a informar, formar y demostrar la necesidad de desarrollar una política de ciberseguridad en todo tipo de organizaciones, haciendo especial hincapié en las pymes y la administración pública canaria.

Esta jornada se enmarca en las actividades definidas dentro del proyecto CYBERCAN a llevarse a cabo durante el lapso 2023-2024.

Objetivos

El objetivo principal del taller es proporcionar a los participantes **una comprensión integral de los principios y prácticas necesarias para digitalizar datos y procesos empresariales de manera segura**. Esto incluye la identificación y mitigación de riesgos asociados con la digitalización, así como la implementación de medidas de seguridad efectivas para proteger la información digital, asegurando la integridad, confidencialidad y disponibilidad de los sistemas.:

1. **Comprender las Amenazas y Vulnerabilidades Digitales:** Familiarizar a los participantes con los diferentes tipos de amenazas cibernéticas, como malware, phishing y ransomware, y las vulnerabilidades comunes en sistemas y redes que pueden ser explotadas por atacantes.

2. **Adquirir Conocimientos en Ciberseguridad Básica:** Enseñar los principios fundamentales de la ciberseguridad y las mejores prácticas para mantener sistemas seguros, incluyendo la importancia de la actualización y mantenimiento de los sistemas informáticos.

3. **Aprender sobre la Protección de Datos:** Explicar la importancia de proteger datos personales y sensibles, así como las regulaciones y leyes relevantes (como GDPR y CCPA), y presentar métodos para proteger los datos, tales como el cifrado y la anonimización.

4. **Desarrollar Habilidades en la Gestión de Riesgos Digitales:** Instruir a los participantes sobre cómo identificar, evaluar y mitigar los riesgos digitales, y cómo crear planes efectivos de respuesta a incidentes y recuperación ante desastres.

5. **Conocer las Mejores Prácticas para la Seguridad en la Nube:** Proporcionar conocimientos sobre los beneficios y riesgos del uso de servicios en la nube, y las mejores prácticas para asegurar los datos y seleccionar y gestionar proveedores de servicios en la nube.

6. **Implementar Métodos de Autenticación y Control de Acceso:** Detallar los diversos métodos de autenticación (como contraseñas, autenticación de dos factores y biometría) y la gestión de identidades y accesos (IAM), y cómo implementar políticas de control de acceso para proteger la información y los sistemas de accesos no autorizados.

7. **Fomentar una Cultura de Seguridad en la Organización:** Resaltar la importancia de la concienciación y la formación en seguridad dentro de la organización, incluyendo programas de capacitación y sensibilización para empleados, y cómo crear y mantener una cultura organizacional orientada a la seguridad.

Esta estructura permitirá que los participantes obtengan una visión completa y práctica de la seguridad de la información y física, capacitándolos para implementar y mantener medidas preventivas efectivas en sus entornos laborales y personales

Público objetivo

Esta jornada está dirigida principalmente a emprendedores, autónomos y empresas que quieran adquirir conocimientos sobre conceptos fundamentales, tipos de amenazas, herramientas, soluciones informáticas y buenas prácticas que les ayuden a garantizar la seguridad y la continuidad de sus compañías. No se requerirán conocimientos técnicos previos.

Docentes / Profesores / Facilitadores

- ✓ **Alberto Suárez Rosales** es Técnico en Administración de Sistemas Informático en Red, que ha trabajado durante 4 años en el sector de la ingeniería eléctrica gestionando los recursos informáticos, así como mejorando los procesos internos de la empresa a nivel digital. Actualmente, sigue creciendo como Administrador de Sistemas en Edataconsulting, recorriendo empresas de diferentes sectores dando soporte, analizando, entendiendo sus procesos y flujos de trabajo para poder ofrecer un servicio más completo.

Contenido

CONTENIDOS

INTRODUCCIÓN A LA DIGITALIZACIÓN SEGURA	• Definición de digitalización y su importancia en el entorno actual • Beneficios y riesgos asociados con la digitalización
AMENAZAS Y VULNERABILIDADES DIGITALES	• Tipos de amenazas (malware, phishing, ransomware, etc.) • Vulnerabilidades comunes en sistemas y redes • Casos reales de ciberataques y sus impactos
CIBERSEGURIDAD BÁSICA	• Principios fundamentales de la ciberseguridad • Buenas prácticas para usuarios y empresas • Importancia de la actualización y mantenimiento de sistemas
PROTECCIÓN DE DATOS	• Concepto de datos personales y datos sensibles • Regulaciones y leyes protección de datos (ej. GDPR, CCPA) • Métodos de protección de datos: cifrados, anonimización, etc.
GESTIÓN DE RIESGOS DIGITALES	• Identificación y evaluación de riesgos digitales • Estrategias de mitigación de riesgos • Planes de respuesta a incidentes y recuperación ante desastres
SEGURIDAD EN LA NUBE	• Beneficios y riesgos del uso de servicios en la nube • Mejores prácticas para la seguridad en la nube • Selección y gestión de proveedores de servicios en la nube
AUTENTICACIÓN Y CONTROL DE ACCESO	• Métodos de autenticación (contraseñas, autenticación de dos factores y biometría) • Gestión de identidades y accesos (IAM) • Implementación de políticas
CULTURA DE SEGURIDAD EN LA ORGANIZACIÓN	• Importancia de la concienciación y formación en seguridad • Programas de capacitación y sensibilización para empleados • Creación de una cultura organizacional orientada a la seguridad

Estructura del Taller:

1. **Introducción (5 minutos):**
    - Bienvenida y presentación del taller.
    - Objetivos y agenda del taller.
2. **Bloques Temáticos (110 minutos):**
    - Cada tema se abordará en bloques de 20 minutos, incluyendo presentaciones teóricas breves y discusiones rápidas.
    - Pausa breve de 5 minutos después de los primeros 60 minutos.
3. **Sesión de Cierre (5 minutos):**
    - Resumen de los puntos clave tratados.
    - Preguntas y respuestas rápidas.
    - Evaluación del taller y comentarios de los participantes.

Cronograma

DIGITALIZACIÓN SEGURA: CLAVES PARA UN ENTORNO EMPRESARIAL SEGURO

FECHA DE INICIO: 27/06/2024

FECHA DE FINALIZACIÓN: 27/06/2024

FECHA	HORARIO	DOCENTE	LUGAR
27/06/2024	**14:30-17:30**	**Alberto Suárez Rosales**	**Teams**