sedian

Seguridad Digital
de Andalucía

Ficha técnica

Gestión de acceso lógico en el ENS. Acceso a la información, servicios y sistemas por ciudadanos, personal interno y externo.

Acción formativa en modalidad Charla Virtual.
29 de septiembre de 2023.

Junta de Andalucía

1 DATOS BÁSICOS DE LA ACCIÓN FORMATIVA

Nombre de la acción formativa: Gestión de acceso lógico en el ENS. Acceso a la información, servicios y sistemas por ciudadanos, personal interno y externo

Modalidad: Charla Virtual.

Fecha de celebración: 29 de septiembre de 2023.

Horario: 09:00 a 10:30 A.M.

Dirigido a: Profesionales TIC de la Junta de Andalucía y entidades vinculadas.

Número máximo de personas participantes: 100.

2 DESCRIPCIÓN

En el campo de la seguridad, se denomina sistema de control de acceso a cualquier tecnología que modere de forma intencional el acceso a activos digitales como, por ejemplo, redes, sitios web y recursos en la nube.

Los sistemas de control de acceso aplican principios de ciberseguridad como la autenticación y autorización para garantizar que los usuarios son quienes dicen ser y que tienen derecho a acceder a ciertos datos basándose en las directivas predeterminadas de identidad y acceso.

Con la aprobación y publicación del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), se han producido modificaciones en lo que compete a la gestión de los accesos (lógicos) a la información, servicios y sistemas que se encuentren afectados por el ENS respecto al RD anterior.

Los cambios no sólo afectan a las medidas de seguridad enmarcadas en el grupo de Control de Acceso [op.acc] sino que se extiende al articulado del RD y otras medidas de seguridad relacionadas con el acceso lógico a información, servicios y sistemas por parte de ciudadanos, personal propio del organismo y personal externo.

3 OBJETIVOS

Generales

• Aprender los casos de uso y ejemplos de regulaciones de acceso e intrusiones en las administraciones públicas.

Específicos

• Analizar el Marco Normativo más relevante

• Estudiar las amenazas.

• Entender cómo el ENS nos ayuda a protegernos ante riesgos y amenazas.

4 CONTENIDOS

- Introducción: la necesidad de requisitos regulatorios.
- Modificaciones en la gestión de los accesos lógicos
- Medidas de seguridad recomendadas.
- Diferencias entre públicos objetivo de control.
- Conclusiones y preguntas abiertas para discusión.

5 TEMPORALIZACIÓN

Fecha: 29/09/2023. **Horario:** 09:00 a 10:30 (90 minutos). **Modalidad**: Charla Virtual.

PLANIFICACIÓN HORARIA

2 MINUTOS.	Presentación.
8 MINUTOS.	Introducción: la necesidad de requisitos regulatorios
15 MINUTOS.	El ambiente regulatorio nacional y europeo.
30 MINUTOS.	Ecosistema de amenazas ante las que protegernos: Caso Ransomware.
20 MINUTOS.	Las medidas del ENS contra el Ransomware.
15 MINUTOS.	Conclusiones y preguntas abiertas para discusión.

6 METODOLOGÍA

La sesión formativa se desarrollará en **modalidad Charla Virtual**, es decir, un seminario impartido en línea donde la interactividad con el alumno es en tiempo real de forma virtualizada con herramientas informáticas diseñadas para tal fin. La herramienta usada para esta sesión se denomina **GoToWebinar**.

7 DOCENTE

IMPARTIDO POR: Antonio Villanueva Sánchez

Ingeniero T. Industrial con Máster Oficial en Gestión de la Tecnologías de la Información y Comunicación. Universidad de Sevilla, Especialista en Gestión de Sistemas y Tecnologías de la Información en la empresa. CEPADE (Universidad Politécnica de Madrid), Diploma en Dirección de Empresas. Instituto Internacional San Telmo (Sevilla).

Certificaciones: PMP, PRINCE2, ITIL Foundations, ITIL Intermediate y BPM

Cursos de especialización:
Máster en Gestión y Mejora de Procesos,
COBIT® 2019 Design & Implementation,
Implementing the NIST Risk Management Framework,
Implementing the NIST Cybersecurity Framework (CSF),
ISOIEC 27002:2022. Information security controls,
ISOIEC 27001:2022. Information Security Management System,
Sarbanes-Oxley (SOX) ITGC Audit Concepts and Coordination,
ISO-IEC 20000-1-2018. Service management system,
ISO-IEC 27701-2019. Privacy Information Managementn System,
ISO-IEC 27005. Information security risk management,
Gestión de Seguridad de la Información - ISO 27001,
Business Continuity Management BCMS & ISO 22301
Masterclass, ISO 22301-2019. Business continuity management system,
Introducción a la Gestión de Riesgos,
ISO-IEC 27001 Implementando Seguridad de la Información,
Introducción a la Gestión de Servicios, Implementación y Cumplimiento del Estándar PCI DSS,
Gestión de RIESGOS - ISO 31000:2018,
Curso de ISO/IEC 27001:2013 - Seguridad de la información,
COBIT versión 5 Fundamentos,

Desarrollados trabajos en diferentes países (Europa y América):

España, Portugal, Holanda, Alemania.

EE.UU., México, San Martín (Caribe), Colombia, Brasil, Argentina, Uruguay, Chile y Perú.

8 EVALUACIÓN

Para la evaluación de la Charla Virtual se tendrán en cuenta las siguientes variables: la asistencia y el tiempo de conexión a la Charla Virtual, que deberá ser igual o superior al 50%.

✓ Asistencia a la jornada con un tiempo de conexión superior al 50%.

✓ Superar el cuestionario de conocimientos con un porcentaje de acierto del 60% o superior (en un plazo de 72 horas tras el evento).

Los valores de estas variables serán extraídos de diferentes informes generados por la herramienta **GoToWebinar** usada para celebrar la sesión.

Criterios de evaluación

Evidencias para la evaluación	Peso
Asistencia	**50%**
Evaluación de Conocimientos	**50%**

Sistema de evaluación.

Valoración de Asistencia.

Cálculo realizado a partir de los informes extraídos de la plataforma **GoToWebinar** denominados:

✓ Informe de Rendimiento.

✓ Informe de Asistentes.

Valoración de Conocimientos.

Indicador obtenido a partir de un cuestionario de 10 ítems sobre aspectos tratados durante la sesión.