CET OPOSICIONES

FORMACIÓN ONLINE

Resumen Esquemático Conceptos Básicos de Seguridad de la Información y Protección de Datos

Resumen Esquemático Conceptos Básicos de Seguridad de la Información y Protección de Datos

1. Conceptos Básicos de Seguridad de la Información

La **Seguridad de la Información** tiene como objetivo principal la **protección de los datos** para evitar su **pérdida o modificación no autorizada**. Esto incluye garantizar la **confidencialidad**, **integridad** y **disponibilidad** de los datos. Otros requisitos importantes son la **autenticidad** y la **trazabilidad**.

- **Confidencialidad**: Solo las personas **autorizadas** pueden acceder a la información.
- **Disponibilidad**: Los datos deben estar **accesibles** para los autorizados en cualquier momento necesario.
- **Integridad**: Los datos deben ser **exactos y completos**, sin **alteraciones no autorizadas**.

1.1. Principios Básicos de Seguridad de la Información

El objeto último de la **seguridad de la información** es asegurar que una **organización administrativa** pueda cumplir sus objetivos utilizando sistemas de información. Los principios básicos incluyen:

- **Seguridad Integral**: Involucra todos los elementos **técnicos, humanos, materiales y organizativos** relacionados con el sistema. Este enfoque asegura que todos los aspectos del sistema estén protegidos y no se dejen puntos vulnerables.
- **Gestión de Riesgos**: Implica el **análisis y la gestión continua de los riesgos** para mantener un entorno controlado. La gestión de riesgos permite identificar amenazas y vulnerabilidades, evaluar el impacto potencial y desarrollar estrategias para mitigarlos.
- **Prevención, Reacción y Recuperación**: Medidas para **prevenir amenazas**, **detectarlas a tiempo** y **recuperarse de incidentes de seguridad**. Esto incluye la implementación de controles preventivos, mecanismos de detección de intrusiones y planes de contingencia para la recuperación de datos y sistemas.
- **Líneas de Defensa**: Estrategias de protección con **múltiples capas de seguridad**. Estas capas incluyen medidas organizativas, físicas y lógicas que actúan conjuntamente para proteger el sistema de información.

- **Reevaluación Periódica**: **Actualización regular** de las medidas de seguridad para adaptarse a la evolución de los riesgos y las tecnologías de protección.
- **Función Diferenciada**: Separación de **responsabilidades** entre el **responsable de la información**, del **servicio** y de la **seguridad**. Esto asegura que cada aspecto de la seguridad de la información sea gestionado por personal especializado y con competencias claramente definidas.

1.2. La Seguridad como un Proceso Integral

La seguridad debe ser entendida como un **proceso integral** que excluye actuaciones puntuales. Es fundamental la **concienciación** y la **coordinación** de las personas involucradas para evitar riesgos. La aplicación del **Esquema Nacional de Seguridad** está presidida por este principio, lo que implica que todas las acciones de seguridad deben ser parte de un esfuerzo coordinado y continuo.

1.3. Gestión de la Seguridad Basada en los Riesgos

La **gestión de riesgos** es crucial y debe mantenerse actualizada para **minimizar los riesgos** a niveles aceptables. En la Administración de la **Junta de Comunidades de Castilla-La Mancha (JCCM)**, esta gestión es esencial y continua, involucrando a **responsables de información y servicios**, así como al **responsable de seguridad y del sistema**. El análisis y gestión de riesgos permite mantener un entorno controlado. Los responsables de la información y del servicio son los propietarios de los riesgos sobre la información y los servicios, siendo responsables de su seguimiento y control.

1.4. Prevención, Reacción y Recuperación

- **Prevención**: Medidas para **eliminar o reducir** las amenazas. Estas medidas incluyen la **disuasión** y la **reducción de la exposición** a los riesgos. Las acciones preventivas están diseñadas para anticiparse a los problemas antes de que ocurran.
- **Detección**: Medidas para **identificar incidentes** de seguridad y acompañarlas de **medidas de reacción**. Los sistemas de detección de intrusiones y las auditorías de seguridad son componentes clave.
- **Recuperación**: Medidas para **restaurar la información y los servicios** de forma que se pueda hacer frente a incidentes que inhabiliten los medios habituales. Esto incluye la creación de copias de seguridad y planes de recuperación ante desastres.

1.5. Conservación y Disponibilidad

El sistema debe garantizar la **conservación de los datos en soporte electrónico** y mantener disponibles los **servicios** durante todo el ciclo vital de la **información digital**. Esto asegura la **preservación del patrimonio digital**. Además, la **disponibilidad** implica que los datos y sistemas estén accesibles cuando se necesiten, lo que es crucial para la continuidad del negocio y la respuesta efectiva ante incidentes.

1.6. Líneas de Defensa

Las estrategias de protección deben incluir **múltiples capas de seguridad** para **minimizar el impacto** de los incidentes y **reducir la probabilidad** de que el sistema sea comprometido en su totalidad. Estas capas permiten **ganar tiempo para una reacción adecuada** y **minimizar el impacto final**. Las líneas de defensa se componen de medidas organizativas (como políticas y procedimientos), físicas (como control de acceso y vigilancia) y lógicas (como cortafuegos y sistemas de encriptación).

1.7. Reevaluación Periódica

Las **medidas de seguridad** se deben **reevaluar periódicamente** para adaptarse a la evolución de los **riesgos** y los **sistemas de protección**. Esto puede llevar incluso a un **replanteamiento de la seguridad** si fuese necesario. La reevaluación regular asegura que las estrategias de seguridad siguen siendo efectivas y que las nuevas amenazas se abordan de manera adecuada.

1.8. Seguridad como Función Diferenciada

Diferenciar las responsabilidades entre el **responsable de la información**, del **servicio** y de la **seguridad** es fundamental para una **gestión eficiente y segura** de los sistemas de información. La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos. Esta separación de funciones garantiza que cada aspecto de la seguridad sea gestionado por el personal más competente y que se eviten conflictos de intereses.

1.9. Conceptos Básicos de Seguridad

- **Activo**: Componente o funcionalidad de un sistema de información susceptible de ser **atacado deliberada o accidentalmente**. Incluye información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, físicos y humanos.
- **Análisis de Riesgos**: Utilización sistemática de la información disponible para **identificar peligros y estimar riesgos**. Los responsables de la información y del servicio son los

propietarios de los riesgos y deben contar con la participación y asesoramiento del responsable de seguridad y del sistema.

- **Auditoría de la Seguridad**: **Revisión independiente** de los registros y actividades del sistema para verificar la **idoneidad de los controles** y asegurar el cumplimiento de la política de seguridad. Detecta infracciones de seguridad y recomienda modificaciones apropiadas.
- **Autenticidad**: Propiedad por la cual una entidad es quien dice ser o garantiza la fuente de los datos.
- **Categoría de un Sistema**: Nivel dentro de la escala Básica-Media-Alta para seleccionar las **medidas de seguridad necesarias**.
- **Confidencialidad**: Propiedad que asegura que la información no está disponible ni es revelada a individuos, entidades o procesos no autorizados.
- **Disponibilidad**: Propiedad de los activos que asegura que las entidades o procesos autorizados tienen **acceso a los mismos** cuando lo requieren.
- **Gestión de Incidentes**: Procedimientos para **detectar, analizar, limitar y responder** ante incidentes de seguridad. Incluye un plan de acción para atender a los incidentes y medidas de desempeño para evaluar la calidad del sistema de protección.
- **Gestión de Riesgos**: Actividades coordinadas para dirigir y controlar una organización respecto a los riesgos.
- **Incidente de Seguridad**: Suceso inesperado o no deseado con consecuencias negativas para la seguridad del sistema.
- **Medidas de Seguridad**: Conjunto de disposiciones para protegerse de los riesgos posibles sobre el sistema de información. Pueden ser medidas de prevención, disuasión, protección, detección y reacción o de recuperación.
- **Política de Seguridad**: Conjunto de directrices plasmadas en documento escrito que rigen cómo una organización gestiona y protege la información y los servicios críticos.

2. La Protección de Datos: Principios, Derechos de los Ciudadanos y Ficheros de Titularidad Pública

2.1. Principios de Protección de Datos

- **Exactitud de los Datos**: Los datos deben ser **exactos y actualizados**. El responsable del tratamiento debe tomar todas las medidas razonables para suprimir o rectificar sin dilación la inexactitud de los datos personales.
- **Deber de Confidencialidad**: Responsables y encargados del tratamiento deben mantener la **confidencialidad de los datos**. Este deber complementa las obligaciones de secreto profesional.
- **Tratamiento Basado en el Consentimiento del Afectado**: Requiere una **manifestación de voluntad libre, específica, informada e inequívoca**. El consentimiento debe ser explícito para todas las finalidades del tratamiento.
- **Consentimiento de Menores**: Solo es válido a partir de los **14 años**, salvo en casos donde se requiera la asistencia de los titulares de la patria potestad o tutela.
- **Tratamiento de Datos por Obligación Legal**: Fundado en una **norma de Derecho de la UE** o de los Estados miembros que imponga condiciones específicas al tratamiento.
- **Categorías Especiales de Datos**: Requieren **medidas adicionales de seguridad** debido a su naturaleza sensible (por ejemplo, ideología, afiliación sindical, religión, orientación sexual).

2.2. Derechos de los Ciudadanos

Los derechos de los ciudadanos incluyen:

- **Derecho de Acceso**: Derecho a obtener **confirmación** sobre el tratamiento de sus datos personales y a acceder a ellos, junto con información adicional sobre los fines del tratamiento, los destinatarios de los datos y los plazos de conservación.
- **Derecho de Rectificación**: Derecho a **corregir datos inexactos** o incompletos. El afectado debe indicar a qué datos se refiere y proporcionar la documentación justificativa.
- **Derecho de Supresión**: Derecho a la **eliminación de datos personales** cuando ya no son necesarios para los fines para los que fueron recogidos, cuando el interesado retira su consentimiento, o cuando los datos se han tratado de manera ilícita.
- **Derecho a la Limitación del Tratamiento**: Derecho a **restringir el uso** de sus datos en determinadas circunstancias, como cuando se impugna la exactitud de los datos.
- **Derecho a la Portabilidad**: Derecho a **recibir y transmitir** sus datos a otro responsable en un formato estructurado, de uso común y lectura mecánica.

- **Derecho de Oposición**: Derecho a **oponerse** al tratamiento de sus datos por motivos personales, especialmente cuando se utilizan para mercadotecnia directa.

2.3. Derechos Digitales

El **Título X** de la LOPDP regula la garantía de los **derechos digitales**, destacando:

- **Derecho a la Neutralidad de Internet**: Servicios ofrecidos sin **discriminación** técnica o económica, garantizando una oferta transparente de servicios.
- **Derecho de Acceso Universal a Internet**: Garantía de acceso para **todos**, independientemente de su condición personal, social, económica o geográfica. Se asegura un acceso universal asequible, de calidad y no discriminatorio.
- **Derecho a la Seguridad Digital**: **Protección** de las comunicaciones en Internet, asegurando que los proveedores informen a los usuarios sobre sus derechos.
- **Derecho a la Educación Digital**: Formación para un **uso seguro y respetuoso** de los medios digitales, integrando competencias digitales en el sistema educativo y garantizando la inclusión de todos los estudiantes, especialmente aquellos con necesidades educativas especiales.
- **Derecho a la Intimidad en el Ámbito Laboral**: **Protección de la privacidad** en el uso de dispositivos digitales en el trabajo, estableciendo criterios claros para su utilización y garantizando la intimidad de los trabajadores.
- **Derecho a la Desconexión Digital**: Garantía de respeto al **tiempo de descanso** fuera del horario laboral, promoviendo la conciliación entre la vida laboral y personal y evitando la fatiga informática.
- **Protección de los Menores en Internet**: Asegurar que los menores hagan un uso equilibrado y responsable de los dispositivos digitales y servicios de la sociedad de la información.
- **Derecho al Olvido**: Derecho a que los motores de búsqueda eliminen de las listas de resultados los enlaces que contengan información inadecuada, inexacta, no pertinente, no actualizada o excesiva sobre una persona.