Sierra de Guara instituto de educación secundaria	**PROGRAMACIÓN DIDÁCTICA** **DEPARTAMENTO DE INFORMÁTICA**	**Curso:** **2022/23** **Revisión:** **1**
Módulo: Seguridad Informática **Ciclo: Sistemas Microinformáticos y Redes**		

Contenido

0. IDENTIFICACIÓN DEL MÓDULO 2

2. ORGANIZACIÓN, SECUENCIACIÓN Y TEMPORALIZACIÓN DE SUS CONTENIDOS EN UNIDADES DIDÁCTICAS 4

4.1 CRITERIOS DE EVALUACIÓN Y CALIFICACIÓN DEL MÓDULO 5

4.2. PRUEBA INICIAL 5

5. RESULTADOS DE APRENDIZAJE Y CRITERIOS MÍNIMOS EXIGIBLES CON SU PORCENTAJE EN PESO PARA OBTENER LA EVALUACIÓN POSITIVA DEL MÓDULO 6

6. PROCEDIMIENTOS E INSTRUMENTOS DE EVALUACIÓN 8

10. PLAN DE CONTINGENCIA 8

Realizado por:	**Revisado por:**	**Aprobado por:**
Javier Sorinas Buil	Equipo docente	Departamento de informática
Fecha: 02 / 10/ 2022	Fecha:	Fecha: *(La del acta de aprobación en el Dpto.)*

Este documento debe ser utilizado en soporte informático.
Las copias impresas no están controladas y pueden quedar obsoletas; por tanto antes de usarlas debe verificarse su vigencia

0. IDENTIFICACIÓN DEL MÓDULO

Real Decreto 774/2015, de 28 de agosto, por el que se establecen seis Títulos de Formación Profesional Básica del catálogo de Títulos de las enseñanzas de Formación Profesional. (BOE 29/08/2015).

Real Decreto 127/2014, de 28 de febrero, por el que se regulan aspectos específicos de la Formación Profesional Básica de las enseñanzas de formación profesional del sistema educativo, se aprueban catorce títulos profesionales básicos, se fijan sus currículos básicos y se modifica el Real Decreto 1850/2009, de 4 de diciembre, sobre expedición de títulos académicos y profesionales correspondientes a las enseñanzas establecidas en la Ley Orgánica 2/2006, de 3 de mayo, de Educación.

Ley Orgánica 8/2013, de 9 de diciembre, para la mejora de la calidad educativa.

Real Decreto 1147/2011, de 29 de julio, por el que se establece la ordenación general de la formación profesional del sistema educativo.

Ley Orgánica 4/2011, de 11 de marzo, complementaria de la ley de economía sostenible, por la que se modifican las leyes orgánicas 5/2002, de 19 de junio, de las cualificaciones y de la formación profesional, 2/2006, de 3 de mayo, de educación, y 6/1985, de 1 de julio, del poder judicial.

Ley 2/2011, de 4 de marzo, de economía sostenible.

Real Decreto 395/2007 de 23 de marzo, por el que se regula el subsistema de formación profesional para el empleo.

Ley Orgánica 2/2006, de 3 mayo, de Educación.

Real Decreto 1558/2005 de 23 de diciembre, por el que se regulan los requisitos básicos de los Centros Integrados de Formación Profesional.

LEY 56/2003, de 16 de diciembre, de Empleo.

Ley Orgánica 5/2002 de 19 de junio, de las Cualificaciones y de la Formación Profesional.

Real Decreto 1629/2009, de 30 de octubre, por el que se establece el título de Técnico Superior en Administración de Sistemas Informáticos en Red y se fijan sus enseñanzas mínimas.

ORDEN de 29 de mayo de 2008, de la Consejera de Educación, Cultura y Deporte, por la que se establece la estructura básica de los currículos de los ciclos formativos de formación profesional y su aplicación en la Comunidad Autónoma de Aragón.

ORDEN de 26 de octubre de 2009, de la Consejera de Educación, Cultura y Deporte, que regula la matriculación, evaluación y acreditación académica del alumnado de Formación Profesional en los centros docentes de la Comunidad Autónoma de Aragón.

ORDEN de 26 de junio de 2009, de la Consejera de Educación, Cultura y Deporte, por la que se establece el currículo del título de Técnico en Sistemas Microinformáticos y Redes para la Comunidad Autónoma de Aragón.

ORDEN de 26 de julio de 2011, de la Consejera de Educación, Universidad, Cultura y Deporte, por la que se modifica diversos currículos de Ciclos Formativos de Formación Profesional.

Este documento debe ser utilizado en soporte informático.
Las copias impresas no están controladas y pueden quedar obsoletas; por tanto antes de usarlas debe verificarse su vigencia

- **Código del módulo:** 0226
- **Denominación:** Seguridad Informatica
- **Horas totales: 105**
- **Horas semanales:** 5
- **Pérdida de la evaluación continua en situación de normalidad, en horas: 16**

Este documento debe ser utilizado en soporte informático.
Las copias impresas no están controladas y pueden quedar obsoletas; por tanto antes de usarlas debe verificarse su vigencia

2. ORGANIZACIÓN, SECUENCIACIÓN Y TEMPORALIZACIÓN DE SUS CONTENIDOS EN UNIDADES DIDÁCTICAS

Unidad didáctica	Contenidos	Horas	Evaluación
UT1 – Introducción a la seguridad informática	- Introducción-Definición - Objetivos y principios de la seguridad informática - Políticas de seguridad - Análisis de riesgos	5	1
UT2 – Seguridad Pasiva y Física. CPD y SAI	- Centros de procesamiento de datos - Ubicación y protección física de los equipos y servidores. - Sistemas de control de acceso y detección - Sistemas de alimentación ininterrumpida.	10	1
UT3 – Seguridad Pasiva y Lógica. Backups y Raids	- Gestión y políticas de almacenamiento - Dispositivos de almacenamiento - Almacenamiento redundante y distribuido - Almacenamiento remoto y extraíble. - Copias de seguridad - Gestión de imágenes del sistema - Recuperación de datos eliminados	18	1
UT4 – Seguridad Activa. Criptografía	- Introducción a la criptografía - Cifrado de clave simétrica - Cifrado de clave asimétrica - Algoritmo de cifrado hash - Sistemas híbridos - Aplicaciones prácticas de la criptografía: -Autenticación: - Firma digital - Certificados digitales -Cifrado - SSL - Cifrado de la información	18	1
UT5 – Seguridad Activa en el Sistema	- Amenazas: virus y malware - Auditorías - Vulnerabilidades - Listas de control de acceso, permisos - Monitorización del sistema - Herramientas de seguridad	20	2
UT6 – Seguridad Activa en Redes	- Vulnerabilidades - Ataques -MITM -DdoS - Aplicaciones monitorización redes - SSH - HTTPS - VLAN - VPN	28	2

Este documento debe ser utilizado en soporte informático.
Las copias impresas no están controladas y pueden quedar obsoletas; por tanto antes de usarlas debe verificarse su vigencia

	- Proxy - Firewall - DMZ - UTM		
UT7 – Normativa sobre seguridad y protección de datos	- Legislación sobre protección de datos. - Legislación sobre los servicios de la sociedad de la información y correo electrónico	6	2
	Horas totales del módulo	105	

4.1 CRITERIOS DE EVALUACIÓN Y CALIFICACIÓN DEL MÓDULO

RESULTADOS DE APRENDIZAJE	CALIFICACIÓN
1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.	20%
2. Gestiona dispositivos de almacenamiento describiendo los procedimientos efectuados y aplicando técnicas para asegurar la integridad de la información.	20%
3. Aplica mecanismos de seguridad activa describiendo sus características y relacionándolas con las necesidades de uso del sistema informático.	20%
4. Asegura la privacidad de la información transmitida en redes informáticas describiendo vulnerabilidades e instalando software especifico	20%
5. Reconoce la legislación y normativa sobre seguridad y protección de datos analizando las repercusiones de su incumplimiento.	20%

4.2. PRUEBA INICIAL

Se ha realizado una prueba inicial de conocimientos con los criterios mínimos imprescindibles para superar la asignatura

El motivo de la realización de la prueba es el de conocer el nivel de conocimientos de los alumnos, puesto que se trata de un grado cuyos conocimientos no se imparten previamente y así poder adaptar la enseñanza al nivel del alumnado. Si bien se espera que gran parte del alumnado no tenga conocimientos previos.

Esta prueba se ha realizado puesto que es conveniente conocer el nivel de los alumnos y así a lo largo del curso ir viendo si se van cumpliendo los objetivos, se adquieren los criterios mínimos y los no mínimos y ver que tipos de instrumentos de evaluación pueden ser los mejores para evaluar los criterios y poder cerciorarse de que se ha realizado un correcto aprendizaje significativo.

El instrumento elegido ha sido una prueba tipo test a través de formulario de google

Este documento debe ser utilizado en soporte informático.
Las copias impresas no están controladas y pueden quedar obsoletas; por tanto antes de usarlas debe verificarse su vigencia

Gracias a la prueba inicial se puede ver si hay que partir desde cero o hay cosas que pueden ser repasadas con mayor velocidad para centrarse en otras y si fuera necesario adaptar la programación a las necesidades de uno o varios alumnos.

5. RESULTADOS DE APRENDIZAJE Y CRITERIOS MÍNIMOS EXIGIBLES CON SU PORCENTAJE EN PESO PARA OBTENER LA EVALUACIÓN POSITIVA DEL MÓDULO

Para aprobar la asignatura el alumno deberá tener aprobados todos los criterios considerados como mínimos imprescindibles, los cuales están en negrita para identificarlos con mayor facilidad.

RESULTADOS DE APRENDIZAJE.	CRITERIOS DE EVALUACIÓN.
RA1. Aplica medidas de seguridad pasiva en sistemas informáticos describiendo características de entornos y relacionándolas con sus necesidades.	a) Se ha valorado la importancia de mantener la información segura. **b) Se han descrito las diferencias entre seguridad física y lógica.** c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores. d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos. **e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.** f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida. **g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.** h) Se ha valorado la importancia de establecer una política de contraseñas. i) Se han valorado las ventajas que supone la utilización de sistemas biométricos
2. Instala sistemas operativos, relacionando sus características con el hardware del equipo y el software de aplicación.	a) Se ha interpretado la documentación técnica relativa a la política de almacenamiento. b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros). c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red. d) Se han descrito las tecnologías de almacenamiento redundante y distribuido. **e) Se han seleccionado estrategias para la realización de copias de seguridad.** f) Se ha tenido en cuenta la frecuencia y el esquema de rotación. **g) Se han realizado copias de seguridad con distintas estrategias.** h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles. i) Se han utilizado medios de almacenamiento remotos y extraíbles. **j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento.**

Este documento debe ser utilizado en soporte informático.
Las copias impresas no están controladas y pueden quedar obsoletas; por tanto antes de usarlas debe verificarse su vigencia

3. Realiza tareas básicas de configuración de sistemas operativos, interpretando requerimientos y describiendo los procedimientos seguidos.	a) Se han seguido planes de contingencia para actuar ante fallos de seguridad. **b) Se han clasificado los principales tipos de software malicioso.** c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades. d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas. e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso. **f) Se han aplicado técnicas de recuperación de datos.**
4. Realiza operaciones básicas de administración de sistemas operativos, interpretando requerimientos y optimizando el sistema para su uso.	a) Se ha identificado la necesidad de inventariar y controlar los servicios de red. **b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.** c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado. d) Se han aplicado medidas para evitar la monitorización de redes cableadas. e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas. f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros. g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros. **h) Se ha instalado y configurado un cortafuegos en un equipo o servidor.**
5. Crea máquinas virtuales identificando su campo de aplicación e instalando software específico.	**a) Se ha descrito la legislación sobre protección de datos de carácter personal.** b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada. c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos. d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen. e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico. **f) Se han contrastado las normas sobre gestión de seguridad de la información.**

Este documento debe ser utilizado en soporte informático.
Las copias impresas no están controladas y pueden quedar obsoletas; por tanto antes de usarlas debe verificarse su vigencia

6. PROCEDIMIENTOS E INSTRUMENTOS DE EVALUACIÓN

En el procedimiento de evaluación se tendrá en cuenta tanto el grado de conocimientos adquiridos sobre los contenidos, como el grado de consecución de las actividades propuestas, valorando en todo momento el esfuerzo realizado por el alumno/a así como los razonamientos empleados.

Todas las actividades propuestas deberán ser entregadas en la fecha que se indique de forma obligatoria.

Cuando un profesor tenga evidencias claras de que un alumno ha realizado de forma fraudulenta una actividad, calificará la citada actividad con un 0. Adicionalmente se podrán interponer las sanciones disciplinarias que se estimen oportunas.

Si aun no existiendo evidencias, el profesor tuviera sospechas por cualquier tipo de motivo de que un alumno ha realizado cualquier actividad con métodos fraudulentos, podrá realizar -previa consulta con el departamento- una nueva prueba de contraste al efecto de comprobar que el alumno realmente es competente para realizar esa tarea. Dicha prueba de competencia podrá realizarse por cualquier medio, incluyendo la entrevista oral. En los casos en que no quede registro del resultado de la prueba, se requerirá la presencia de otro profesor habilitado para la impartición del módulo. Si se comprueba que el alumno no es competente para realizar la tarea, la evaluación de la misma será un 0.

Evaluación inicial

La realización de la evaluación inicial tiene como objetivo, detectar los conocimientos previos de los que parte el alumno respecto a los contenidos que se van a abordar en el modulo, a fin de detectar aquellos a los que sus conocimientos previos les hagan no partir de cero.

Las cuestiones y preguntas formuladas en dicha evaluación corresponden a contenidos de cada una de las unidades del módulo, así como a contenidos base vistos en módulos relacionados de primer curso.

Para cada **evaluación**:

La nota de por evaluación se calculara a través de la **prueba** de evaluación (PE) correspondiente y las **practicas** o actividades correspondientes de cada evaluación (PA). PA es la media aritmética de la nota de todas las prácticas de la evaluación. Las PA se presentaran en su fecha correspondiente. Todas las PA tienen que estar todas un valor superior a 5 para aprobar. Si NE no llega al 5 la evaluación estará suspendida.

$$NE = (0{,}90*PE + 0{,}1*PA)$$

Para cada evaluación se realizara una **recuperación** en caso de que NE no llegue al 5. No se tendrán en cuenta las prácticas. En caso de superarla la nota de la evaluación será de 5.

Si se han superado las 2 evaluaciones la nota final es la media aritmética de las dos evaluaciones.

La nota Final del modulo (C)= Nota 1ª Evaluación + Nota 2ª Evaluación / 2

En el caso de no tener aprobada todas las evaluaciones será necesario superar la prueba **ordinaria** de Marzo, donde entraran todos los contenidos del modulo. En el caso de no superar esta prueba se realizara una prueba **extraordinaria** en Junio en la cual también entraran todos los contenidos del modulo. Para aprobar la asignatura será necesario sacar 5 o más en estas pruebas. La nota será la que salga de las pruebas.

10. PLAN DE CONTINGENCIA

Este documento debe ser utilizado en soporte informático.
Las copias impresas no están controladas y pueden quedar obsoletas; por tanto antes de usarlas debe verificarse su vigencia

En el caso de que el profesor falte durante un periodo de tiempo, se prepararán una serie de actividades para que los alumnos las puedan realizar en las horas que el profesor no pueda acudir al centro. Dichas actividades se entregaran al profesor de guardia correspondiente.

Se intentará en la media de lo posible adecuar el horario para que los profesores de guardia sean aquellos que dispongan de un mayor conocimiento de la materia.

Si un alumno falta un número importante de clases por motivos justificados. Se determinará en la medida de lo posible un plan de trabajo, acordado por profesor y alumno, para que este pueda realizar las actividades de clase fuera de horario y, además, pueda disponer de una atención por parte del profesor respecto a las dudas que le vayan surgiendo en el desarrollo de dichas actividades.

En el caso de faltar más del 15% de horas del modulo injustificadas perderá el derecho de evolución continua.

Este documento debe ser utilizado en soporte informático.
Las copias impresas no están controladas y pueden quedar obsoletas; por tanto antes de usarlas debe verificarse su vigencia