| | | |
|---|---|---|
| Sierra de Guara instituto de educación secundaria | **PROGRAMACIÓN DIDÁCTICA**<br>**DEPARTAMENTO DE INFORMÁTICA** | **Curso:**<br>**2020/2021**<br>**Revisión:**<br>**1** |
| **Módulo: Seguridad Informática**<br>**Ciclo: Sistemas Microinformáticos y Redes** | | |

**ÍNDICE:**



| **Realizado por:** | **Revisado por:** | **Aprobado por:** |
|---|---|---|
| Unai Urrestarazu Esporrín | Equipo docente | Departamento de informática |
| Fecha: 9 / 12/ 2020 | Fecha: | Fecha:<br>*(La del acta de aprobación en el Dpto.)* |

## 1. CRITERIOS DE EVALUACIÓN

| 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.**<br>**b) Se han descrito las diferencias entre seguridad física y lógica.**<br>**c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores.**<br>**d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.**<br>**e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.**<br>**f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.**<br>g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.<br>**h) Se ha valorado la importancia de establecer una política de contraseñas.**<br>**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.<br>**b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad, accesibilidad, entre otros).**<br>**c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en red.**<br>d) Se han descrito las tecnologías de almacenamiento redundante y distribuido.<br>**e) Se han seleccionado estrategias para la realización de copias de seguridad.**<br>f) Se ha tenido en cuenta la frecuencia y el esquema de rotación.<br>**g) Se han realizado copias de seguridad con distintas estrategias.**<br>**h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles.**<br>**i) Se han utilizado medios de almacenamiento remotos y extraíbles.**<br>j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento. |

| | |
|---|---|
| 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.**<br>**b) Se han clasificado los principales tipos de software malicioso.**<br>**c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.**<br>**d) Se ha verificado el origen y la autenticidad de las aplicaciones que se instalan en los sistemas.**<br>**e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.**<br>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.**<br>**b) Se ha contrastado la incidencia de las técnicas de ingeniería social en los fraudes informáticos y robos de información.**<br>c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.<br>d) Se han aplicado medidas para evitar la monitorización de redes cableadas.<br>**e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.**<br>**f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.**<br>**g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.**<br>**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.**<br>**b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.**<br>**c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.**<br>**d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen.**<br>e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.<br>f) Se han contrastado las normas sobre gestión de seguridad de la información. |

## 2. CRITERIOS DE CALIFICACIÓN

| 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% |

## 3. RESULTADOS DE APRENDIZAJE MÍNIMOS EXIGIBLES PARA OBTENER LA EVALUACIÓN POSITIVA DEL MÓDULO

Los resultados de aprendizaje mínimos están indicados en negrita en los criterios de evaluación.

| 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.**<br>**b) Se han descrito las diferencias entre seguridad física y lógica.**<br>**c) Se han definido las características de la ubicación física y condiciones ambientales de los equipos y servidores.**<br>**d) Se ha identificado la necesidad de proteger físicamente los sistemas informáticos.**<br>**e) Se ha verificado el funcionamiento de los sistemas de alimentación ininterrumpida.**<br>**f) Se han seleccionado los puntos de aplicación de los sistemas de alimentación ininterrumpida.**<br>g) Se han esquematizado las características de una política de seguridad basada en listas de control de acceso.<br>**h) Se ha valorado la importancia de establecer una política de contraseñas.**<br>**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.<br>**b) Se han tenido en cuenta factores inherentes al almacenamiento de la información (rendimiento, disponibilidad,**<br>**accesibilidad, entre otros).**<br>**c) Se han clasificado y enumerado los principales métodos de almacenamiento incluidos los sistemas de almacenamiento en**<br>**red.**<br>d) Se han descrito las tecnologías de almacenamiento redundante y distribuido.<br>**e) Se han seleccionado estrategias para la realización de copias**<br>**de seguridad.**<br>f) Se ha tenido en cuenta la frecuencia y el esquema de rotación.<br>**g) Se han realizado copias de seguridad con distintas estrategias.**<br>**h) Se han identificado las características de los medios de almacenamiento remotos y extraíbles.**<br>**i) Se han utilizado medios de almacenamiento remotos y extraíbles.**<br>j) Se han creado y restaurado imágenes de respaldo de sistemas en funcionamiento. |
| 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**<br>**de seguridad.**<br>**b) Se han clasificado los principales tipos de software malicioso.**<br>**c) Se han realizado actualizaciones periódicas de los sistemas para corregir posibles vulnerabilidades.**<br>**d) Se ha verificado el origen y la autenticidad de las aplicaciones**<br>**que se instalan en los sistemas.**<br>**e) Se han instalado, probado y actualizado aplicaciones específicas para la detección y eliminación de software malicioso.**<br>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.**<br>**b) Se ha contrastado la incidencia de las técnicas de ingeniería**<br>**social en los fraudes informáticos y robos de información.**<br>c) Se ha deducido la importancia de minimizar el volumen de tráfico generado por la publicidad y el correo no deseado.<br>d) Se han aplicado medidas para evitar la monitorización de redes cableadas.<br>**e) Se han clasificado y valorado las propiedades de seguridad de los protocolos usados en redes inalámbricas.**<br>**f) Se han descrito sistemas de identificación como la firma electrónica, certificado digital, entre otros.**<br>**g) Se han utilizado sistemas de identificación como la firma electrónica, certificado digital, entre otros.**<br>**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.**<br>**b) Se ha determinado la necesidad de controlar el acceso a la información personal almacenada.**<br>**c) Se han identificado las figuras legales que intervienen en el tratamiento y mantenimiento de los ficheros de datos.**<br>**d) Se ha contrastado la obligación de poner a disposición de las personas los datos personales que les conciernen.**<br>e) Se ha descrito la legislación actual sobre los servicios de la sociedad de la información y comercio electrónico.<br>f) Se han contrastado las normas sobre gestión de seguridad de la información. |

## 4. PLAN DE REFUERZO DE LOS CONTENIDOS QUE NO PUDIERON IMPARTIRSE EL CURSO PASADO

Se van a realizar trabajos y prácticas que complementen los conocimientos del año pasado, siempre en la medida de lo posible dada la situación de presencialidad en semanas alternas. Para ello se hará uso del ordenador, programas informáticos y búsqueda de información que fomenten el aprendizaje por indagación.