



| Guía docente          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    |                      |           |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------------|-----------|
| Datos Identificativos |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    |                      | 2021/22   |
| Asignatura (*)        | Fortificación de Sistemas Operativos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                    | Código               | 614530007 |
| Titulación            | Máster Universitario en Ciberseguridade                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                    |                      |           |
| Descriptor            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    |                      |           |
| Ciclo                 | Periodo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Curso              | Tipo                 | Créditos  |
| Máster Oficial        | 2º cuatrimestre                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Primero            | Obligatoria          | 5         |
| Idioma                | CastellanoGallegoInglés                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                    |                      |           |
| Modalidad docente     | Presencial                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                    |                      |           |
| Prerrequisitos        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    |                      |           |
| Departamento          | Ciencias da Computación e Tecnoloxías da InformaciónComputación                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    |                      |           |
| Coordinador/a         | Yañez Izquierdo, Antonio Fermin                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Correo electrónico | antonio.yanez@udc.es |           |
| Profesorado           | Yañez Izquierdo, Antonio Fermin                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Correo electrónico | antonio.yanez@udc.es |           |
| Web                   | faitic.uvigo.es                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    |                      |           |
| Descripción general   | <p>Un sistema operativo recién instalado es inherentemente inseguro. Presenta ciertas vulnerabilidades dependiendo de factores tales como la edad del S.O., la existencia de puertas traseras sin parchear, los servicios que proporciona y el uso de políticas por defecto que no tienen como primer objetivo la seguridad.</p> <p>Por fortificación de un S.O nos referimos al acto de configurar dicho S.O con la intención de hacerlo tan seguro como sea posible, intentando minimizar el riesgo de que quede comprometido a ser explotada alguna de sus vulnerabilidades. Esto suele implicar la aplicación de parches de seguridad, el cambio de ciertas políticas por defecto del S.O. y la eliminación (o deshabilitación) de aplicaciones y servicios no esenciales.</p> <p>En este curso trataremos de identificar vulnerabilidades comunes y ver como el S.O. se puede defender de ellas. Se considerarán sistemas tipo Windows y tipo linux</p>                                         |                    |                      |           |
| Plan de contingencia  | <p>1. Modificaciones en los contenidos.</p> <p>ninguna</p> <p>2. Metodologías</p> <p>* Metodologías docentes que cambian</p> <p>- Sesión magistral: videoconferencia</p> <p>- Prácticas: supervisadas a través de las TIC,</p> <p>- Prueba objetiva y prueba práctica: a través de Teams, Faitic, Moodle u otras herramientas de UVigo y / o UDC.</p> <p>3. Mecanismos de atención personalizada a los alumnos.</p> <p>- Moodle: todos los recursos docentes se proporcionarán a través de Faitic.</p> <p>- Teams u otras herramientas de videoconferencia. Se pueden convocar sesiones de equipo para tutoría</p> <p>- Correo electrónico: para cualquier consulta</p> <p>4. Modificaciones en la evaluación.</p> <p>ninguna</p> <p>* Observaciones de evaluación:</p> <p>En el caso de no poder ser presencial tanto la prueba objetiva como la prueba práctica se realizarán utilizando Teams, campus remoto o faitic</p> <p>5. Modificaciones a la bibliografía o webografía.</p> <p>ninguna</p> |                    |                      |           |

| Competencias del título |                                                                                                                                                                                                                |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Código                  | Competencias del título                                                                                                                                                                                        |
| A3                      | CE3 - Conocer la normativa técnica y legal de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información |



|     |                                                                                                                                                                                                                                                 |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A4  | CE4 - Conocer la normativa técnica y legal de aplicación en materia de ciberseguridad, sus implicaciones en el diseño de sistemas, en el uso de herramientas de seguridad y en la protección de la información                                  |
| A5  | CE5 - Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información                             |
| A8  | CE8 - Tener capacidad para concebir, diseñar, poner en práctica y mantener sistemas de ciberseguridad                                                                                                                                           |
| A9  | CE9 - Tener capacidad para elaborar de planes y proyectos de trabajo en el ámbito de la ciberseguridad, claros, concisos y razonados                                                                                                            |
| A11 | CE11 - Reunir e interpretar datos relevantes dentro del área de la seguridad informática y de las comunicaciones                                                                                                                                |
| A13 | CE13 - Tener capacidad de análisis, detección y eliminación de vulnerabilidades, y del malware susceptible de utilizarlas, en sistemas y redes                                                                                                  |
| B2  | CB2 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio   |
| B5  | CB5 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo                                                                        |
| B6  | CG1 - Tener capacidad de análisis y síntesis. Tener capacidad para proyectar, modelar, calcular y diseñar soluciones de seguridad de la información, las redes y/o los sistemas de comunicaciones en todos los ámbitos de aplicación            |
| B7  | CG2 - Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones                          |
| B8  | CG3 - Capacidad para el razonamiento crítico y la evaluación crítica de cualquier sistema de protección de la información, cualquier sistema de seguridad de la información, de la seguridad de las redes y/o los sistemas 14 de comunicaciones |
| B10 | CG5 - Tener capacidad para aplicar los conocimientos teóricos en la práctica, en el marco de infraestructuras, equipamientos y aplicaciones concretos, y sujetos a requisitos de funcionamiento específicos                                     |
| C3  | CT3 - Incorporar en el ejercicio profesional criterios de sostenibilidad y compromiso ambiental. Incorporar a los proyectos el uso equitativo, responsable y eficiente de los recursos                                                          |
| C4  | CT4 - Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad                                                                                                                                       |

| Resultados de aprendizaje                                                                                             |  |                                                 |                                               |
|-----------------------------------------------------------------------------------------------------------------------|--|-------------------------------------------------|-----------------------------------------------|
| Resultados de aprendizaje                                                                                             |  | Competencias del título                         |                                               |
| Identificar las diferentes vulnerabilidades de un S.O.                                                                |  | BP2<br>BP5<br>BP6<br>BP7<br>BP10                |                                               |
| Entender como funcionan las vulnerabilidades y como el S.O. puede protegerse de ellas                                 |  | AP8<br>BP2<br>BP5<br>BP6<br>BP7<br>BP10         |                                               |
| Configurar un S.O. de manera que limitemos su exposición a amenazas, minimizando el riesgo de que se vea comprometido |  | AP3<br>AP4<br>AP5<br>AP8<br>AP9<br>AP11<br>AP13 | BP2<br>BP5<br>BP6<br>BP7<br>BP8<br>CP3<br>CP4 |

| Contenidos            |                                                                                                                               |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Tema                  | Subtema                                                                                                                       |
| Introducción a F.S.O. | Concepto de fortificación de un S.O. Vulnerabilidades. Fortificación durante la instalación, post instalación y mantenimiento |



|                                          |                                                                                                                                                                                              |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fortificación del proceso de arranque    | Seguridad física del sistema. Fortificación del firmware (BIOS, UEFI). Fortificación del cargador                                                                                            |
| Fortificación de las cuentas de usuarios | Identificar y eliminar cuentas no suadas. Limitar privilegios de los usuarios. políticas de grupo. Fortificar autenticación. Forzar políticas de contraseñas                                 |
| Fortificación de sistemas de ficheros    | Permisos y protecciones de sistemas de ficheros. Cuotas. Bloqueo de directorios del sistema. Encriptación. Limitar acceso a dispositivos                                                     |
| Fortificación de aplicaciones            | Identificando y eliminando aplicaciones no usadas. Identificando conexiones y aplicaciones que proporcionan conexiones no deseadas. Ejecución en entornos seguros (tipo contenedor), SELinux |
| Fortificación de la red                  | Identificar y eliminar conexiones no deseadas. Filtrado de paquetes                                                                                                                          |
| Monitorización y mantenimiento           | Monitorización del sistema. Logs. Parches                                                                                                                                                    |

| Planificación                                                                                                                     |                                                 |                    |                                          |               |
|-----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|--------------------|------------------------------------------|---------------|
| Metodologías / pruebas                                                                                                            | Competencias                                    | Horas presenciales | Horas no presenciales / trabajo autónomo | Horas totales |
| Actividades iniciales                                                                                                             | A8 A11 A13 B6                                   | 1                  | 2                                        | 3             |
| Sesión magistral                                                                                                                  | A3 A4 A11 A13 B5 B6 B8 B10 C3                   | 16                 | 32                                       | 48            |
| Solución de problemas                                                                                                             | A3 A4 A5 B2 B5 B7 B8 B10 C3                     | 5                  | 15                                       | 20            |
| Prácticas de laboratorio                                                                                                          | A4 A5 A8 A9 A11 A13 B2 B5 B6 B7 B8 B10 C3       | 16                 | 16                                       | 32            |
| Prueba objetiva                                                                                                                   | A3 A4 A5 A8 A9 A11 A13 B2 B5 B6 B7 B8 B10 C3 C4 | 2                  | 20                                       | 22            |
| Atención personalizada                                                                                                            |                                                 | 0                  |                                          | 0             |
| (*)Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos |                                                 |                    |                                          |               |

| Metodologías             |                                                                                                                                                                                                                                                  |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Metodologías             | Descripción                                                                                                                                                                                                                                      |
| Actividades iniciales    | Actividades iniciales para familiarizar al alumno con el S.O., sus vulnerabilidades y las defensas frente a ellas                                                                                                                                |
| Sesión magistral         | El estudiante asistirá las sesiones magistrales impartidas por el profesor sobre como minimizar la posibilidad de que las distintas vulnerabilidades (arranque, usuarios, conexiones de red..) puedan ser aprovechadas para comprometer el S.O.. |
| Solución de problemas    | Problemas y pequeñas cuestiones practicas para consolidar los contenidos presentados en las sesiones magistrales                                                                                                                                 |
| Prácticas de laboratorio | Practicas de laboratorio sobre la fortificación de sistemas operativos reales. Se considerarán tanto sistemas Windows como Linux                                                                                                                 |
| Prueba objetiva          | Test ssobre los contenidos fundamentales de la asignatura.                                                                                                                                                                                       |

| Atención personalizada   |                                                                                                                                                                                                                                                                  |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Metodologías             | Descripción                                                                                                                                                                                                                                                      |
| Sesión magistral         | Aunque las prácticas de laboratorio y la solución de problemas se realizará en su mayor parte en el horario de clases, el profesor estará disponible para ayudar de manera individual con cualquier duda o cuestion que surga de la realización de estas tareas. |
| Solución de problemas    |                                                                                                                                                                                                                                                                  |
| Prácticas de laboratorio |                                                                                                                                                                                                                                                                  |
|                          | El profesor estará asimismo disponible para ayudar con los conceptos expuestos durante las sesiones magistrales.                                                                                                                                                 |



| Evaluación               |                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |              |
|--------------------------|-------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| Metodologías             | Competencias                                          | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Calificación |
| Prueba objetiva          | A3 A4 A5 A8 A9 A11<br>A13 B2 B5 B6 B7 B8<br>B10 C3 C4 | <p>Questiones relacionadas con el conocimiento adquirido</p> <p>Questiones que impliquen razonar sobre el conocimiento adquirido</p> <p>Questiones que involucren resolución de problemas en Sistemas Operativos reales</p> <p>Para superar la asignatura es necesario superar ambas partes por separado: prueba objetiva y prácticas de laboratorio</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 50           |
| Prácticas de laboratorio | A4 A5 A8 A9 A11 A13<br>B2 B5 B6 B7 B8 B10<br>C3       | <p>Control de las prácticas realizadas y evaluación de los resultados obtenidos:</p> <p>Las prácticas realizadas durante las sesiones de prácticas se evaluarán con hasta un 40-60% de la puntuación de prácticas (20-30% del total de la asignatura)</p> <p>Además habrá una prueba práctica donde el alumno realizará algunos ejercicios similares a los realizados en las clases prácticas, sobre un equipo físico (máquina real o virtualizada), sin la ayuda de material adicional.</p> <p>Dicha prueba se realizará en las últimas sesiones de prácticas o después de cada parte de las prácticas (linux y windows). En caso de no ser posible se hará el día de la prueba objetiva, después de ésta.</p> <p>La prueba práctica representa el 60-40% de la puntuación de prácticas (30-20% del total de la asignatura)</p> <p>Para superar la asignatura es necesario superar ambas partes por separado: prueba objetiva y prácticas de laboratorio</p> <p>La convocatoria de Julio solo consta de la prueba objetiva. Si algún alumno quisiera repetir la prueba práctica, deberá solicitarlo por escrito ANTES de una semana de la fecha de la prueba objetiva</p> | 50           |

| Observaciones evaluación                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Para superar la asignatura es necesario superar ambas partes por separado: prueba objetiva y prácticas de laboratorio (es decir, 2.5 en cada parte)</p> <p><b>PRIMERA OPORTUNIDAD</b></p> <p>Los estudiantes que no participan alguna de las partes de la evaluación en la primera oportunidad tendrán 0 en cada parte no participada. En caso de ser la prueba objetiva la calificación final será de No Presentado</p> <p><b>SEGUNDA OPORTUNIDAD</b></p> <p>Solo se repite la prueba objetiva. Si algún alumno quisiera repetir la prueba práctica, deberá solicitarlo por escrito ANTES de una semana de la fecha de la prueba objetiva</p> <p><b>PLAGIO:</b> En el caso de detectar plagio en cualquier prueba o material entregado, la calificación final será de SUSPENSO (0) y el hecho será comunicado a la dirección del Centro para los efectos oportunos.</p> |

| Fuentes de información |
|------------------------|
|------------------------|



|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Básica         | <ul style="list-style-type: none"><li>- Donald A. Tevault (2018). Mastering Linux Security and Hardening. Packt Publishing</li><li>- James Turnbull (2008). Hardening Linux . Apress</li><li>- Carlos Álvarez Martín y Pablo González Pérez 0xWord (2016). Hardening de servidores GNU / Linux (3a Edición). 0xWord</li><li>- Tajinder Kalsi (2018). Practical Linux Security Cookbook: Secure your Linux environment from modern-day attacks with practical recipes, 2nd Edition. Packt Publishing</li><li>- Gris, Myriam (2017). Windows 10. ENI</li><li>- Aprea, Jean-François (2017). Windows Server 2016 : Arquitectura y Administración de los servicios de dominio Active Directory. ENI</li><li>- Bonnet, Nicolas (2017). Windows Server 2016 : las bases imprescindibles para administrar y configurar su servidor. ENI</li><li>- De los Santos, Sergio (). Máxima Seguridad en Windows: Secretos Técnico. 0xWord</li><li>- Núñez, Ángel (). Windows Server 2016: Administración, seguridad y operaciones. 0xWord</li><li>- Yuri Diogenes, Erdal Ozkaya (2018). Cybersecurity - Attack and Defense Strategies. Packt Publishing</li><li>- Salvy, Pierre (2017). Windows 10 : despliegue y gestión a través de los servicios de empresa. ENI</li><li>- Deman, Thierry (2018). Windows Server 2016 : Administración avanzada. ENI</li><li>- García, Carlos. González, Pablo (). Hacking Windows: Ataques a sistemas y redes Microsoft. 0xWord</li></ul> |
| Complementaria |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

| Recomendaciones                                         |
|---------------------------------------------------------|
| Asignaturas que se recomienda haber cursado previamente |
|                                                         |
| Asignaturas que se recomienda cursar simultáneamente    |
|                                                         |
| Asignaturas que continúan el temario                    |
|                                                         |
| Otros comentarios                                       |
|                                                         |

(\*) La Guía Docente es el documento donde se visualiza la propuesta académica de la UDC. Este documento es público y no se puede modificar, salvo cosas excepcionales bajo la revisión del órgano competente de acuerdo a la normativa vigente que establece el proceso de elaboración de guías