Auditoría de seguridad basada en un análisis cuantitativo de riesgos

**Grupo 5**

Diego Villa García – UO277188@uniovi.es

Saúl Tuñón Fernández - UO277490@uniovi.es

Hugo Roberto Pulido Pensado - UO282823@uniovi.es

Carlos Sánchez Rodríguez - UO282621@uniovi.es

Miguel Olamendi Alonso - UO285032@uniovi.es

# Contenido

[Contenido 1](#_Toc155543356)

[Presentación del informe 2](#_Toc155543357)

[Objetivos y alcance de la auditoría 3](#_Toc155543358)

[Temas considerados 3](#_Toc155543359)

[Cuerpo expositivo 3](#_Toc155543360)

[Dominios de seguridad 3](#_Toc155543361)

[Aulas de teoría 3](#_Toc155543362)

[Aulas de laboratorio 4](#_Toc155543363)

[Sala de libre acceso 4](#_Toc155543364)

[Infraestructura de comunicaciones 5](#_Toc155543365)

[Sala de servidores 6](#_Toc155543366)

[Sala de robótica 6](#_Toc155543367)

[Conserjería 7](#_Toc155543368)

[Secretaría 7](#_Toc155543369)

[Observaciones generales 8](#_Toc155543370)

[Servicios 9](#_Toc155543371)

[Resultado 9](#_Toc155543372)

[Plan de trabajo 9](#_Toc155543373)

[Bibliografía 10](#_Toc155543374)

[Anexo I: Checklists 11](#_Toc155543375)

[Anexo II: Entrevista con trabajador del centro 13](#_Toc155543376)

[Anexo III: Pilar 14](#_Toc155543377)

[Anexo IV: Servicios 15](#_Toc155543378)

[Anexo V: Estructura de la escuela 16](#_Toc155543379)

# Presentación del informe

|  |  |  |
| --- | --- | --- |
| **Información de la entidad auditada** | | |
| Nombre de la entidad auditada | Escuela de Ingeniería Informática |
| Dirección | Edificio Valdés Salas Campus de los Catalanes, s/n 33007 Oviedo (Asturias) - España |
| Página web | https://ingenieriainformatica.uniovi.es/inicio |
| Email | [eii@uniovi.es](mailto:eii@uniovi.es) |
| Teléfono | +34 985 10 27 96 |

|  |
| --- |
| **Información de la auditoría** |

|  |  |
| --- | --- |
| Fecha de comienzo de la auditoría | 13 de noviembre de 2023 |
| Fecha de redacción del informe | 27 de diciembre de 2023 |
| Equipo auditor | |  | | --- | | Diego Villa García (jefe de auditoría) | | Saúl Tuñón Fernández | | Hugo Roberto Pulido Pensado | | Miguel Olamendi Alonso | | Carlos Sánchez Rodríguez | |
| Normas auditadas | ISO 27001 |
|  |  |

# Objetivos y alcance de la auditoría

El objetivo de esta auditoría es un análisis cuantitativo de riesgos de la Escuela de Ingeniería Informática mediante la aplicación de la Metodología de Análisis y Gestión de Riesgos en TI (MAGERIT), basada en el estándar ISO 27001.

Para ello se han identificado diferentes activos de la organización y las amenazas a las que pueden estar sometidos, y se ha comprobado si se implantan salvaguardas para mitigar los riesgos y los daños.

Se han excluido de esta auditoría la organización interna del personal de la Escuela y aquellos sistemas que utiliza, pero no dependen específicamente de ella, sino de otras organizaciones (como la Universidad de Oviedo).

# Temas considerados

Los temas tratados por parte de los auditores han sido:

* Equipos de escritorio en las distintas aulas de la Escuela.
* Infraestructura de comunicaciones de la Escuela.
* Servidores situados dentro de la Escuela.
* Servicios prestados por estos servidores.

# Cuerpo expositivo

Para llevar a cabo la auditoría se han hecho observaciones de los activos que maneja la organización, además de preguntas concretas a personal que está relacionado con la gestión de éstos.

## Dominios de seguridad

Para la realización de la auditoría, en primer lugar, se ha llevado a cabo la identificación de dominios de seguridad.

Hemos clasificado los activos en 8 dominios de seguridad:

### Aulas de teoría

Las aulas de teoría están distribuidas por todas las plantas de la escuela excepto la segunda, y todas contienen un único ordenador y un proyector.

El ordenador tiene un alto valor en cuanto disponibilidad e integridad, ya que de su buen funcionamiento depende la normal realización de las clases expositivas. También tiene un alto valor de autenticidad y trazabilidad ya que puede contener información confidencial del profesor y solo debería ser accesible por él.

Los factores agravantes que afectan a este dominio son que el personal interno puede acceder, una persona podría tener intención destructiva, económica o de provocar pérdidas. El atenuante es que es un objetivo poco atractivo porque solamente hay un ordenador.

#### No conformidad menor

Las aulas de teoría del sótano pueden ser accedidas a través de las ventanas, ya que están a la altura de la calle, facilitando el robo del ordenador.

**Acción preventiva**: instalar rejillas metálicas en las ventanas de las aulas del sótano.

Acción para realizar por parte del subdirector de infraestructuras en un plazo de un año.

#### No conformidad menor

Los ordenadores de las aulas de teoría tienen cuentas locales que pueden ser utilizadas por cualquier persona, incluidas personas externas a la organización, ya que las credenciales están en una hoja encima de la mesa donde está el ordenador.

**Acción preventiva**: limitar el acceso a las credenciales, por ejemplo, teniendo que pedirlas en la secretaría para llevar un control de quién las solicita.

Acción para realizar por parte del personal de secretaría en un plazo de un año.

### Aulas de laboratorio

Hay varias aulas de laboratorio repartidas por toda la escuela. En cada una de ellas está equipada con una elevada cantidad de equipos (con sus respectivos periféricos), así como con un proyector. Está aulas son usadas diariamente por una gran cantidad de alumnos y profesores.

Tanto los equipos como el proyector tienen un alto valor, ya que ambos deben estar en buenas condiciones y disponibles para permitir a los alumnos y a los docentes realizar sus actividades con normalidad. Los equipos también tienen un alto valor en cuanto a autenticidad y trazabilidad, ya que en cada equipo hay información que pertenece a diferentes docentes y alumnos.

Como factores agravantes están el uso de estas clases por muchas personas durante el día, por lo que algún alumno o profesor no sería difícil hacer acciones maliciosas.

#### No conformidad menor

Aunque las puertas de las aulas de laboratorio tienen cerradura, muchas veces no se usan y se dejan las aulas abiertas y sin vigilancia, lo que facilita el acceso a ellas para gente de fuera de la organización.

**Acción preventiva:** Asegurarse de que las aulas se cierran correctamente a la finalización de cada clase.

Esta acción la deben realizar los docentes y demás trabajadores de la escuela, pues deberían ser los únicos con acceso a las llaves.

#### No conformidad menor

Las aulas de laboratorio del sótano pueden ser accedidas a través de las ventanas, ya que están a la altura de la calle, facilitando el robo de los equipos.

**Acción preventiva**: instalar rejillas metálicas en las ventanas de las aulas del sótano.

Acción para realizar por parte del subdirector de infraestructuras en un plazo de un año.

### Sala de libre acceso

La escuela cuenta con dos salas de libre acceso. Ambas cuentan en su interior con un gran número de equipos informáticos, así como de periféricos y cables de red.

Las dos salas están abiertas en su horario correspondiente (una de 11:00 a 14:00 y la otra en el horario de apertura del centro). Estando, principalmente la segunda, buena parte de su horario sin supervisión por parte de algún responsable.

El valor de los activos de esta sala es bajo ya que solo suele usarse por los alumnos en su tiempo libre y no suelen contener ninguna información confidencial. Por esto tendrían un bajo valor en todos los aspectos.

Como factor agravante está el uso de estas salas por una gran cantidad de personas a lo largo del día sin control alguno sobre sus actuaciones.

#### No conformidad menor

Las salas constan con periodos de tiempo sin supervisión alguna, facilitando así cualquier actuación malintencionada, tanto a nivel físico como lógico, por parte de un usuario.

**Acción preventiva:** Instalar cámaras de videovigilancia o contar con una persona supervisora en dichas salas.

Acción a realizar por parte del director de la organización en un plazo de 2 años.

#### No conformidad menor

El acceso y uso de las salas es libre y sin ningún tipo de identificación. Favoreciendo así que cualquier usuario, ya sea miembro o no de la organización, entre sin dejar constancia de ello.

**Acción preventiva:** Activar un registro, donde para usar las salas debas dejar constancia de que lo has hecho.

Acción para realizar por parte del director de la organización en un plazo de 1 año.

#### No conformidad menor

En una de las salas, se encuentran varios puestos, de becarios informáticos de la organización, sin supervisión alguna en determinados momentos. Favoreciendo el acceso de personas no autorizadas, a sus equipos y objetos personales, donde podrían tener material confidencial como credenciales o información sobre las configuraciones de la red del centro.

**Acción preventiva:** Habilitar una sala para uso exclusivo de los becarios y técnicos informáticos.

Acción para realizar por parte del director de la organización en un plazo de 1 año.

### Infraestructura de comunicaciones

En cada piso hay un rack de comunicaciones que permite el acceso a internet de todos los equipos del piso. Es fundamental para el correcto funcionamiento de la organización.

El rack tiene un altísimo valor de integridad y disponibilidad ya que dé él depende el buen funcionamiento de una gran cantidad de ordenadores.

Los factores agravantes que afectan a este dominio son que están accesibles al público general (ya que están en los pasillos) además del personal interno, pueden ser objetivos interesantes por su importancia, conectan un amplio número de equipos y redes y una persona podría tener intención destructiva o de provocar pérdidas.

#### No conformidad mayor

Los racks de comunicaciones ubicados en el sótano y el primer piso de la Escuela de Ingeniería Informática cuentan con una cerradura para evitar el acceso a estos, cosa inútil ya que se puede acceder a él por uno de los laterales simplemente quitando un tornillo (se puede hacer incluso con una moneda). El acceso indebido a dicha infraestructura puede provocar todo tipo de acciones como dejar a toda la planta sin conexión o incluso la inclusión de algún dispositivo para almacenar toda la información que circula entre los diferentes equipos (ataque *Man-in-the-Middle*).

**Acción preventiva:** impedir el acceso por completo al rack, ya sea creando una sala de comunicaciones con una cerradura y acceso restringido a una serie de personas o incorporando algún tipo de cerradura para estos laterales del rack.

Acción para realizar por parte del subdirector de infraestructuras en un plazo de un mes.

### Sala de servidores

La Escuela de Ingeniería Informática dispone de infraestructura de virtualización que se utiliza, entre otras actividades, para proporcionar servidores de uso exclusivo a cada estudiante del Máster, y que pueden utilizarse como estaciones de trabajo en remoto.

La infraestructura se divide en 2 Clusters que funcionan bajo un sistema de virtualización basado en el hipervisor XEN.

Estos servidores se encuentran en dos salas: una en la planta baja y otra en el primer piso.

Entre los principales servidores virtualizados en dicha infraestructura se encuentran:

* Un servidor de bases de datos Oracle Linux 6 que da servicio a todos los estudiantes de las asignaturas relacionadas con los sistemas de gestión de bases de datos y repositorios de información.
* Un servidor para el sistema de helpdesk que permite gestionar las incidencias de infraestructuras de la Escuela.
* Un servidor de imágenes de disco para el despliegue de laboratorios de prácticas.
* Un servidor para la gobernanza electrónica de la Escuela.

### Sala de robótica

La sala de robótica es un aula que tiene varias utilidades, una de ellas es realizar ejercicios relacionados con la asignatura de Software de Robots por lo que en esta aula hay distintos robots (robots móviles, actuadores lineales...), diferentes tipos de Arduino, componentes electrónicos (cables, leds, zumbadores, pulsadores, diferentes sensores, resistencias...) y un par de ordenadores de sobremesa.

Para poder utilizar dicha sala debes reservarla contactando con el profesor de dicha asignatura y este te asigna un horario concreto por lo que se tiene un control de las personas que entran a dicha sala y se hacen responsables de todo el material allí presente.

#### No conformidad menor

Para el acceso al aula solo hay que contactar con el profesor que tendrá constancia de que alumnos entran en dicha sala, pero solo uno de ellos es el encargado de dejar el DNI para poder identificarlo si ocurre algo (teniendo solo constancia el profesor de que otros alumnos han podido estar en la sala en base a los grupos que conforman en la asignatura).

**Acción preventiva:** una forma de asegurarse de que alumnos estuvieron presentes para poder identificarlos más fácilmente seria que toda aquella persona que vaya a trabajar en dicha aula dejase su DNI y firmase un papel afirmando que estuvo en allí en ese periodo de tiempo.

Acción para realizar por parte del profesor correspondiente y los alumnos que soliciten el aula en un plazo de un mes.

#### No conformidad menor

El profesor no tiene un inventario muy específico del material de robótica que contiene el aula (sí que lo tiene del equipo más importante o de más valor, pero no de la mayoría de pequeños componentes electrónicos).

**Acción preventiva:** tener un inventario con todo el equipo que se deja en el aula para que los alumnos trabajen y una vez estos terminen su tarea, comprobar que sigue presente todos los componentes.

Acción para realizar por parte del profesor correspondiente en un plazo de un mes.

### Conserjería

La conserjería es una pequeña sala situada en la entrada principal de la escuela. En esta sala se encuentran ordenadores, documentación acerca de la organización y llaves de las aulas.

Las llaves tienen un alto valor en lo referente a la autenticidad y confidencialidad ya que si alguien accede a ellas tendría acceso a toda la escuela. Los documentos, aunque puede que no contengan información sensible también tienen un valor moderado en cuanto a confidencialidad y trazabilidad ya que pueden contener información privada.

Un factor agravante es que la conserjería al estar cerca de la entrada es más vulnerable a personan como malas intenciones que se puedan colar en la escuela.

#### No conformidad menor

A veces la ventanilla del mostrador se deja abierta sin haber nadie en su interior, lo que facilitaría el acceso a la sala a gente no autorizada.

**Acción preventiva:** Asegurarse de cerrar correctamente todas las posibles entradas a la sala cuando no haya nadie para evitar el acceso por parte de personas no autorizadas. Esto incluye cerrar la puerta, el mostrado y la ventana, de forma que no se pueda abrir desde fuera.

Acción para realizar por parte los por todos los trabajadores que accedan a la sala.

### Secretaría

La escuela cuenta con una sala de secretaría en la planta baja, donde se llevan a cabo operaciones administrativas relacionadas con toda la organización.

Como factor agravante se encuentra la disponibilidad de documentos confidenciales de alto valor, como pueden ser datos personales de todos los miembros de la organización, ya sean trabajadores, profesores o alumnos. Información relativa a distintas operaciones administrativas como pagos y gestiones tanto internas como externas.

Debido a todo ello, tiene un alto valor de confidencialidad, trazabilidad y autenticidad.

#### No conformidad menor

Las ventanas de secretaría se encuentran a la altura de la calle sin ninguna protección extra más allá de la propia cerradura, facilitando así la intrusión en dicha sala mediante la rotura del cristal, por parte de un usuario malintencionados.

**Acción preventiva**: instalar rejillas metálicas en las ventanas.

Acción para realizar por parte del subdirector de infraestructuras en un plazo de un año.

## Observaciones generales

Aquí se recogen las inconformidades comunes de activos de distintos dominios como las de los ordenadores de las diferentes aulas.

#### No conformidad menor

Un candado protege las cajas de los equipos, pero el material de fabricación de la parte trasera de la caja es acero dulce, lo que facilita abrirla, forzando la cerradura con la mano o cortando la caja con tijeras o similares.

**Acción preventiva:** Cambiar las cajas por otras cuyos materiales de fabricación sean más resistentes.

Acción a realizar por parte del director de la organización en un plazo de 3 años.

#### No conformidad menor

Los ordenadores no están fijados de ninguna manera o están fijados únicamente con una brida o algo similar a las mesas por lo que alguien podría robar todo el ordenador en su conjunto.

**Acción preventiva:** Anclar los ordenadores a las mesas o fijarlos con una cuerda o algo similar al propio suelo del aula.

Acción a realizar por parte del director de la organización en un plazo de 1 año.

#### No conformidad menor

Los periféricos de los ordenadores no están fijados correctamente a estos por lo que alguien podría desconectarlos y robarlos.

**Acción preventiva:** Anclar los periféricos a los ordenadores.

Acción a realizar por parte del director de la organización en un plazo de 1 año.

#### No conformidad menor

En algunos equipos parte del software instalado es innecesario, ya que no es usado durante ninguna clase, lo que hace que dichos programas solo ocupen espacio y sean fuentes de posibles vulnerabilidades.

**Acción preventiva:** Hacer imágenes personalizadas para cada aula de manera que en cada equipo se instalen solo los programas que se van a utilizar en las clases que impartan en esa aula.

Acción a realizar por parte del personal técnico de la organización en el plazo de un año.

## Servicios

La página está bien protegida de herramientas como shodan ya que no es detectada por estas.

#### No conformidad menor

Faltan cabeceras http que podrían aumentar la seguridad, como puede ser el caso de X-Frame-Options y X-content-Type-Options para prevenir ataques de clickjacking y la confusión de tipos MIME respetivamente.

**Acción preventiva:** Añadir las cabeceras para aumentar la seguridad.

Acción a realizar por parte de los desarrolladores en el plazo de 6 meses.

#### No conformidad menor

No se utiliza httponly para el manejo de las cookies, el uso de httponly podría evitar que se cambiara el valor de las cookies con scripts del lado del cliente.

**Acción preventiva:** Añadir el uso de httponly para el manejo de cookies.

Acción a realizar por parte de los desarrolladores en el plazo de 6 meses.

La política de bloqueos de ip parece correcta ya que no permite escanear correctamente la página con muchas herramientas.

# Resultado

Se encontraron 17 no conformidades menores y una mayor. Se concluye que la auditoría es **desfavorable**.

# Plan de trabajo

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Auditores | TAreaS realizadas | | | | | |
| Aulas teoría | Aulas lab | Comunicaciones | Libre acceso | Servidores | Robótica | Secretaría | Conserjería | Entrevistas |
| Diego Villa García | X |  | X |  |  |  |  |  |  |
| Saúl Tuñón Fernández |  |  |  |  |  | X | X |  |  |
| Hugo Roberto Pulido Pensado |  | X |  |  |  |  |  | X |  |
| Miguel Olamendi Alonso |  |  |  |  | X |  |  |  | X |
| Carlos Sánchez Rodríguez |  |  |  | X |  |  | X |  |  |

# Bibliografía

Escuela de Ingeniería Informática. (14 de 12 de 2023). *Instalaciones*. Obtenido de https://ingenieriainformatica.uniovi.es/elcentro/instalaciones

Escuela de Ingeniería Informática. (14 de 12 de 2023). *Personal*. Obtenido de https://ingenieriainformatica.uniovi.es/personal

Universidad de Oviedo. (5 de 1 de 2024). *Sistema de Información Geográfica*. Obtenido de https://gis.uniovi.es/GISUniovi/GeoLoc.do?codEspacio=01.01.01.00.P3

# Anexo I: Checklists

|  |  |  |  |
| --- | --- | --- | --- |
| **Aulas de teoría** | | | |
|  | ***Sí*** | ***No*** | |
| ¿Se cierran las aulas cuando no hay nadie en ellas? |  | X |
| ¿Los ordenadores se pueden abrir? | X |  |
| ¿Se lleva un control de para qué se está usando cada aula? | X |  |
| ¿Los ordenadores pueden ser utilizados solamente por personal autorizado? |  | X |
| ¿El software instalado en los equipos está actualizado? | X |  |
| ¿Solamente los usuarios administradores pueden modificar configuraciones o instalar programas? | X |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Aulas de laboratorio** | | | |
|  | ***Sí*** | ***No*** | |
| ¿Se cierran las aulas cuando no hay nadie en ellas? |  | X |
| ¿Los ordenadores se pueden abrir? | X |  |
| ¿Se lleva un control de para qué se está usando cada aula? | X |  |
| ¿Los ordenadores pueden ser utilizados solamente por personal autorizado? | X |  |
| ¿El software instalado en los equipos está actualizado? | X |  |
| ¿Solamente los usuarios administradores pueden modificar configuraciones o instalar programas? | X |  |
| ¿Todo el software instalado en los equipos tiene licencia? | X |  |
| ¿Los ordenadores están anclados al aula? |  | X |
| ¿Están los periféricos fijados de alguna manera a los ordenadores? |  | X |
| ¿El acceso a la BIOS está protegido? | X |  | |

|  |  |  |
| --- | --- | --- |
| **Salas de libre acceso** | | |
|  | ***Sí*** | ***No*** |
| ¿Puede entrar cualquier persona a las salas, aun no perteneciendo a la organización? | X |  |
| ¿Los ordenadores se pueden abrir fácilmente? | X |  |
| ¿Los ordenadores pueden ser utilizados únicamente por personal autorizado? |  | X |
| ¿El software instalado en los equipos está actualizado? | X |  |
| ¿Solamente los usuarios administradores pueden modificar configuraciones o instalar programas? | X |  |
| ¿Está protegido el acceso a la BIOS de los equipos? | X |  |
| ¿Todo el software instalado en los equipos tiene licencia? | X |  |
| ¿Los ordenadores están anclados al aula? |  | X |
| ¿Están los periféricos fijados de alguna manera efectiva a los ordenadores? |  | X |
| ¿Existe un registro de quien ha utilizado cada ordenador? |  | X |
| ¿Existe algún impedimento para conectar equipos propios a través de los cables de red? |  | X |
| ¿Hay información delicada o confidencial en alguna de las salas? | X |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Infraestructura de comunicaciones** | | | |
|  | ***Sí*** | ***No*** | |
| ¿Los racks de comunicaciones están situados en lugares protegidos (salas con cerradura)? |  | X |
| ¿Los racks de comunicaciones están protegidos mediante cerradura? | X |  |
| ¿Puede un individuo ajeno a la organización manipular el contenido de los racks? | X |  |
| ¿La conexión WiFi que ofrece la Escuela requiere autenticación? | X |  |
| ¿Configurar el punto de acceso WiFi requiere ser administrador? | X |  |

|  |  |  |
| --- | --- | --- |
| **Salas de servidores** | | |
|  | ***Sí*** | ***No*** |
| ¿Permanecen cerradas siempre? | X |  |
| ¿El acceso físico está limitado? | X |  |
| ¿Dispone de alguna autenticación biométrica? |  | X |
| ¿Se registran las acciones llevadas a cabo por cada usuario? | X |  |
| ¿Estos registros son enviados a un servidor externo? | X |  |

|  |  |  |
| --- | --- | --- |
| **Aula de robótica** | | |
|  | ***Sí*** | ***No*** |
| ¿Se utiliza dicha aula para otra actividad? | X |  |
| ¿Tienen cerradura la puerta de esta aula? | X |  |
| ¿Se cierran las aulas cuando no hay nadie en ellas? | X |  |
| ¿Los ordenadores se pueden abrir? |  | X |
| ¿Se pueden desconectar los periféricos del ordenador para posteriormente irse con ellos? |  | X |
| ¿Se lleva un control de para qué se está usando cada aula en cada momento? | X |  |
| ¿Se lleva un control de que personas están utilizando dicha aula en cada momento? | X |  |
| En caso afirmativo, ¿se anota datos de todas las personas presentes? |  | X |
| ¿El software instalado en los equipos está actualizado? |  | X |
| ¿Solamente los usuarios administradores pueden modificar configuraciones o instalar programas? | X |  |
| ¿Todo el software instalado en los equipos tiene licencia? | X |  |
| ¿Se tiene un control del material que hay presente en la sala para cada sesión? |  | X |
| ¿Hay alguna persona con mayor grado de autoridad (profesor, conserje...) presente en el aula mientras los alumnos están en ella? |  | X |

|  |  |  |
| --- | --- | --- |
| **Secretaría** | | |
|  | ***Sí*** | ***No*** |
| ¿La puerta de acceso tiene cerradura? | X |  |
| ¿Se cierran correctamente todas las posibles entradas a la sala? | X |  |
| ¿Se almacenan datos comprometidos en dicha sala? | X |  |
| ¿Existe alguna medida para evitar que los datos discutidos en la sala sean visualizados desde fuera de la misma? | X |  |
| ¿Permanece la sala cerrada cuando no hay ningún trabajador dentro? | X |  |

# Anexo II: Entrevista con trabajador del centro

¿Todos los ordenadores tienen la misma imagen?

* No, algunos ordenadores con una GPU más potente y mayor capacidad de procesamiento contienen programas para la asignatura de Realidad Aumentada.

¿Cuándo se crean estas imágenes?

* Las imágenes se crean anualmente en un servidor de la escuela.

¿Como se deciden los programas a instalar en las imágenes?

* Los profesores comunican que programas van a necesitar para llevar a cabo las clases y las imágenes se crean con los programas solicitados por los distintos profesores.

# Anexo III: Pilar

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

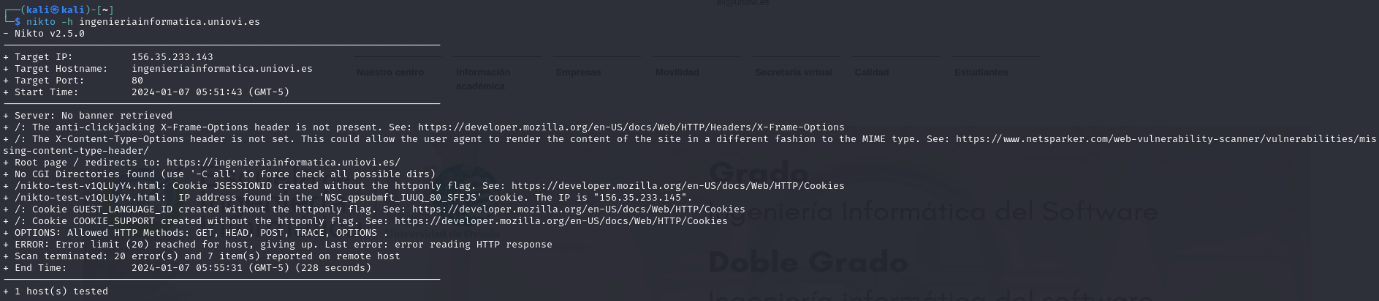
Ilustración 1 Dominios de seguridad

Tabla

Descripción generada automáticamente

Ilustración 2 Valoraciones de los activos esenciales y dominios

# Anexo IV: Servicios



# Anexo V: Estructura de la escuela

