LEET SECURITY
CyberSecurity Rating Agency

ZIUR
INDUSTRIAL CYBER SECURITY CENTER-GIPUZKOA

Autoevaluación LEET Security
Guía de uso

ÍNDICE

1. INTRODUCCIÓN

E-Qualify es una herramienta de auto-evaluación online que incorpora todo el conocimiento y la experiencia de **LEET Security** en la realización de calificaciones de ciberseguridad y que permite, mediante la respuesta a una serie de preguntas tabuladas, obtener un entendimiento del nivel y capacidades en ciberseguridad del alcance elegido.

La evaluación se realiza utilizando la metodología de calificación de **LEET Security** completa, es decir, incluye el conjunto completo de controles sobre las medidas de seguridad técnicas y organizativas, agrupados en los 14 dominios sobre los que se apoya:

- Gestión de Seguridad de la Información
- Operación de Sistemas
- Seguridad del Personal
- Seguridad de las Instalaciones
- Procesamiento por terceros
- Resiliencia
- Cumplimiento normativo
- Protección frente a malware
- Controles de red
- Monitorización
- Control de acceso
- Desarrollo de seguro
- Gestión de incidentes
- Criptografía

La herramienta **E-Qualify** ha sido desarrollada para simplificar el proceso de evaluación, de forma que pueda ser realizado con una dedicación de tiempo razonable, considerando el alto volumen de información a evaluar.

Cada auto-evaluación realizada estará referida a un servicio o alcance específico, si bien la misma también propone cuestiones más generales que pueden afectar a varios, o incluso a procedimientos generales de la compañía.

Cuando para la prestación del servicio evaluado sean empleados múltiples componentes o esté a su vez compuesto por diferentes servicios que son agregados en el mismo, las respuestas proporcionadas deben referirse a la totalidad de estos, tomando siempre el componente más débil. Es decir, el incumplimiento de un control determinado en uno cualquiera de los componentes, causa el incumplimiento en el servicio global.

2. ACCESO AL SISTEMA

La aplicación se encuentra ubicada en https://diagnostikoa.ziur.eus/.

Esta guía está referida a la versión PREMIUM, cuya dirección de acceso es:

https://diagnostikoa.ziur.eus/login?ReturnUrl=%2fhome%2fes

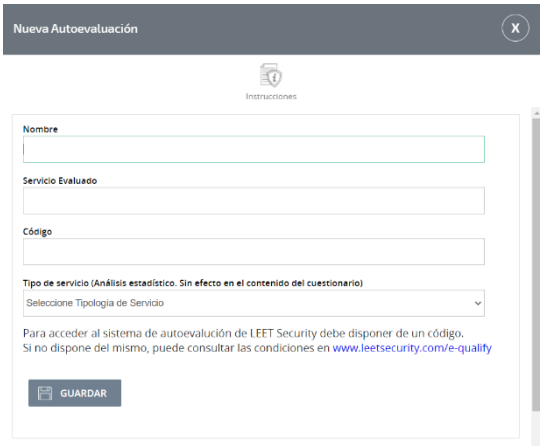
El acceso al sistema requiere el registro con su cuenta de correo electrónico, a la que se hará llegar un correo de confirmación para su activación como usuario de E-Qualify.

El usuario de acceso al sistema es su cuenta de correo. La pantalla de entrada a E-Qualify muestra las autoevaluaciones asociadas:

Para generar una autoevaluación, pulsar en botón **+ Nueva Autoevaluación**, abriéndose a la derecha de la pantalla una ventana en la que identificarla.

En esta ventana debe indicar el nombre que desee asignar a la autoevaluación, una referencia al servicio o alcance sobre el cual se realizará, introducir un código válido y seleccionar la tipología del servicio evaluado.

Si no se dispone de un código, deberán seguirse las indicaciones para acceder a uno.



Una vez generada la autoevaluación, pulsar el icono lápiz para proceder

Con ello se da acceso a la pantalla de instrucciones para su cumplimentación

En esta pantalla de inicio pueden leerse las instrucciones básicas, que se explican en detalle en esta guía de uso.

3. CUESTIONES DE APLICABILIDAD

Para proceder con la cumplimentación, en primer lugar se plantean una serie de **cuestiones para determinar la aplicabilidad** de determinados controles, siendo la primera de ellas el **nivel objetivo** sobre el que realizar la autoevaluación, ya que cuanto más elevado es el mismo, es mayor el número de controles a evaluar. De esta forma, si se desea optar, por ejemplo, a un nivel BBB, podrán descartarse aquellas preguntas que afectan únicamente a los niveles A y A+, manteniendo las correspondientes a B, así como a los inferiores.

A título de ejemplo, se indica a continuación el número de preguntas contenidas en E-Qualify para cada uno de los niveles objetivo:

Nivel	D	C	B	A	A+	Total controles
Preguntas	80	227	328	379	399	**1.327**

Es decir, para un nivel A+, las respuestas dadas a las 399 cuestiones planteadas en E-Qualify, cumplimentarían el estado de implantación de los 1.327 controles que conforman el esquema en su totalidad. Al seleccionar niveles objetivos más bajos, se reduce el número de preguntas presentadas, puesto que los controles que únicamente afectan a los niveles superiores son considerados como NO aplicables.

A continuación, se plantean el resto de cuestiones de Aplicabilidad, sobre el tipo de servicio y los componentes del mismo. En función de las respuestas proporcionadas se podrá reducir el número de preguntas presentadas. Estas cuestiones de aplicabilidad son las siguientes:

2. El servicio se presta en alguna de las siguientes modalidades (indique únicamente la más semejante o ninguna)
    a. Personal, en las instalaciones y con equipamiento proporcionado por el cliente
    b. Acceso remoto mediante escritorio virtual proporcionado por los clientes
    c. Acceso remoto a los sistemas del cliente desde instalaciones del proveedor
    d. Asesorías (o similares) con información del cliente y equipamiento propio
3. Servicio de tipo "Cloud" (IaaS/PaaS/SaaS)? (incluye nube pública y nube privada)
4. Servicio de desarrollo o basado en aplicaciones de desarrollo propio (o externalizado)
5. Se utilizan terceras partes/proveedores externos
6. Se gestiona alguna PKI propia (infraestructura de clave pública)
7. Se procesan, tratan o transmiten datos de carácter personal
8. El CPD es propio o los sistemas se alojan en un CPD de terceros
9. Opciones permitidas o no en la prestación de los servicios:
    - Acceso con dispositivos móviles
    - Conexiones con dispositivos propios (BYOD)
    - Servidores VoIP
10. Sistemas de autenticación NO empleados (deben marcarse los que NO son utilizados)

Las respuestas dadas a estas cuestiones descartan automáticamente como NO aplicables aquellos controles que quedarían excluidos, generando la selección de los controles que son de aplicación al servicio evaluado.

Se incluye una pregunta adicional en este grupo:

11. Para este servicio, ¿existe un proceso para registrar la actividad de uso del sistema / eventos de auditoría? (generación y gestión de logs)

En caso de respuesta negativa excluye todas las preguntas que se plantean en torno al mantenimiento y monitorización de los registros de actividad en el sistema, marcando como NO implantados los controles correspondientes en el capítulo de Monitorización.

Al final, pulsar el botón 

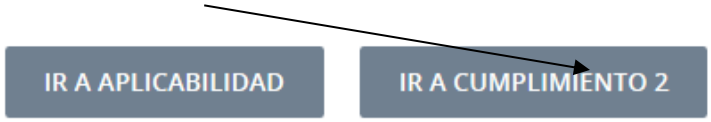
4. CUESTIONES DE CUMPLIMIENTO 1

Finalizado este grupo de preguntas, se plantea un segundo grupo, denominado **cuestiones de Cumplimiento 1**, para tratar otras posibles certificaciones o auditorías sobre el alcance evaluado. Los referenciales que considera la herramienta actualmente son los siguientes:

- Certificaciones ISO: 27001, 20000 y/o 22301
- PCI-DSS
- Esquema Nacional de Seguridad, ENS, en sus diferentes niveles
- Certificación STAR sobre Cloud Control Matrix
- Modelo de Construcción de Capacidades en Ciberseguridad para la Cadena de Valor (C4V), del Esquema Nacional de Seguridad Industrial

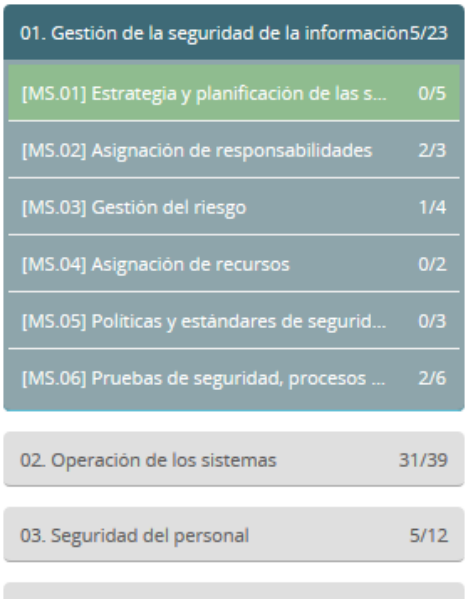
La herramienta da por cumplimentados automáticamente los controles que son verificados para otorgas las correspondientes certificaciones.

A la finalización, **pulsar el botón** (o si se desea, puede volver a la sección anterior)



5. CUESTIONES DE CUMPLIMIENTO 2

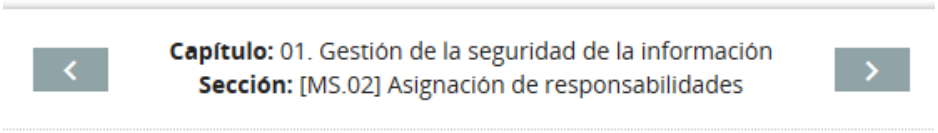
Finalizado a su vez este grupo de cuestiones, se inicia el proceso propiamente dicho, con las preguntas denominadas de **Cumplimiento 2**, en las que se plantean todas las cuestiones con varias posibilidades de respuesta, en función de las cuales se marcan como implantados o no implantados todos los controles que han quedado seleccionados como aplicables tras las preguntas de Aplicabilidad.



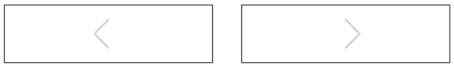
Estas preguntas se presentan agrupadas por cada una de las secciones en que están divididos los 14 capítulos del esquema.

A la izquierda de la pantalla se presenta un índice de capítulos y secciones, en el que se detalla el número total de preguntas a responder, así como las ya respondidas en cada sección, destacando la sección que se está respondiendo en cada momento.

Al principio de cada pantalla de secciones se indica el nombre del dominio y la sección correspondientes, pudiendo navegar hacia la anterior o posterior:



La navegación hacia las secciones anterior y posterior también se posibilita mediante las flechas al final de cada pantalla:



Sin embargo, no se requiere finalizar una sección para pasar a la siguiente, sino que es posible navegar libremente entre capítulos y secciones, desde el panel de la izquierda, para cumplimentar el modelo en el orden de preferencia.

Por otra parte, también al final de cada pantalla del grupo de cuestiones de cumplimiento 2 nos encontramos con los botones siguientes:

6. PANTALLA DE RESULTADO

El primero de los botones vuelve a las cuestiones del grupo anterior, mientras que cada vez que se pulsa el segundo se realiza un cálculo basado en las respuestas que se hayan dado hasta el momento (aunque el proceso no se haya finalizado):

En esta pantalla se muestra el nivel objetivo así como el obtenido (hasta el momento), mostrando el porcentaje de secciones en cada uno de los niveles, así como los resultados parciales de cada uno de los 14 dominios del esquema.

Lógicamente, si quedan cuestiones sin responder, la aplicación considera que los controles correspondientes no están implementados, por lo que será muy frecuente el resultado F ("Failed").

En esta pantalla de Resultado se muestran también los botones de vuelta y de finalizar:

El primero nos devuelve al inicio de las cuestiones de cumplimiento 2, mientras que el segundo no resulta operativo hasta que no se hayan respondido la totalidad de preguntas, dando por cumplimentado en cuestionario.

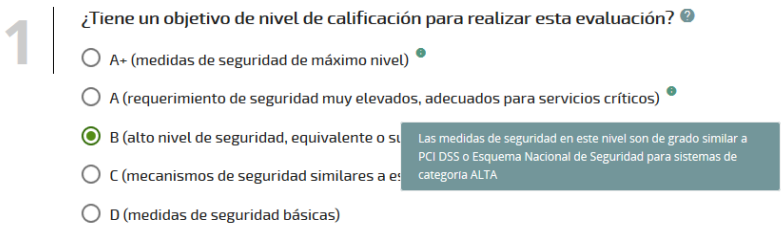
7. ASPECTOS GENERALES SOBRE TODAS LAS PREGUNTAS

Para todos los casos, las respuestas a cada pregunta pueden ser únicas o múltiples. En caso de respuestas únicas, solo se podrá seleccionar una de las opciones de respuesta presentadas. Las respuestas múltiples permiten la selección de cualesquiera de las respuestas posibles.

Las respuestas de tipo único se identifican con un botón de tipo circular. La selección de una respuesta desactiva la anterior que pudiese haberse dado. En las de tipo múltiple, el botón es cuadrado, y se podrán seleccionar todas ellas de forma simultánea, salvo cuando la última es "Ninguna de las anteriores", que las desactiva.

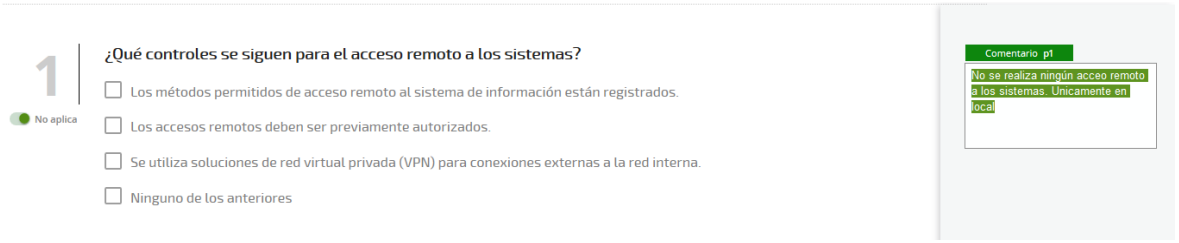
> En caso de respuesta múltiple, siempre **deben seleccionarse TODAS las posibles respuestas que sean cumplidas o excedidas** por los controles implementados en el servicio, ya que en muchos casos estas respuestas no se acumulan automáticamente.

Tanto el enunciado de las preguntas como las posibles respuestas pueden estar marcadas con un botón de interrogación o información:



Pasando el ratón por encima del mismo, aparece un cuadro emergente con información adicional, que puede ser aclarativa o complementaria a la presentada y necesaria para su cumplimentación.

Además de lo anterior, para las cuestiones de cumplimiento 2 se dispone de un botón interruptor de "No aplica", y de un cuadro de comentarios:



Cuando el contenido de una pregunta no resulta de aplicación al servicio evaluado, se marcará dicha pregunta como "No aplica", y todos los controles que están sujetos a las respuestas presentadas en la misma, son marcados como No aplicables al servicio (no utilizar esta opción si la pregunta aplica pero no se cumplen las respuestas presentadas).

> En caso de que la cuestión si resulte pertinente, pero una o varias de las respuestas resulten no aplicables (p.e. si la respuesta solamente se refiere a redes inalámbricas, y éstas no están permitidas como acceso o no existen en el servicio), dichas respuestas deben ser chequeadas de igual forma que si su contenido estuviese cumplimentado.

En el cuadro de comentarios puede darse cualquier indicación que se considere relacionada con la pregunta o controles asociados, quedando ligada a todos ellos, para cualquier uso posterior que pueda resultar pertinente.

8. FINALIZACIÓN

Todas las respuestas que se han dado en la autoevaluación pueden ser modificadas pudiendo presentarse nuevas o excluirse preguntas en el grupo cumplimiento 2, en caso de cambiarse las de Aplicabilidad o Cumplimiento 1. En todo caso, una vez respondida la totalidad de preguntas presentadas en el ejercicio, se podrá dar por finalizado **pulsando el botón finalizar** en la pantalla de Resultado, produciendo así el informe correspondiente, que podrá descargarse pulsando el botón que aparece bajo el sello que muestra el resultado global:

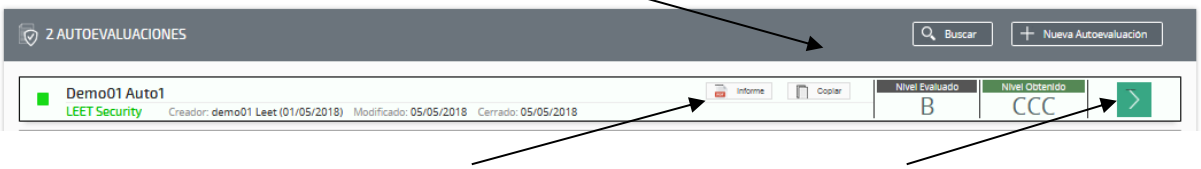
También podrá descargarse en cualquier momento desde el icono correspondiente que se presenta en la pantalla de acceso a la herramienta en la que se muestras las autoevaluaciones asociadas al usuario.

Una vez finalizado el proceso para una autoevaluación, ya no se podrá modificar ninguna de las respuestas facilitadas, pero sí revisar todas ellas.

El informe de resultado muestra el contexto del servicio evaluado, con las respuestas proporcionadas a las cuestiones de Aplicabilidad y Cumplimiento

1, así como la calificación global y gráfico con la distribución de secciones en cada nivel, así como el detalle de los resultados individuales en cada una de las 73 secciones en que se estructura la calificación, y un listado de los controles que sería necesario cumplir para acceder a los niveles superiores al obtenido, hasta el nivel indicado como objetivo, proporcionando así una valiosa información sobre las fortalezas y áreas de mejora en la seguridad. Siempre acorde a las respuestas facilitadas.

En caso de realizarse nuevas autoevaluaciones, si se trata de servicios de características similares o que comparten una parte de los procedimientos o medidas de seguridad aplicadas, se podrá iniciar una nueva autoevaluación copiando los datos facilitados en otra, pulsando en el botón copiar en la pantalla de entrada:



Botón de descarga del informe Botón de revisión de respuestas

Esta operación puede hacerse tanto a partir de una autoevaluación finalizada y cerrada, como a partir de otra que esté en curso, siempre y cuando el origen sea una autoevaluación en la versión actual. La nueva copiada a partir de la anterior permitirá la modificación de cualquiera de las respuestas dadas en la original, permitiendo así comparar los diferentes resultados obtenidos en ambas. La copia de una autoevaluación también requiere la aplicación de un código válido.