LOGO

Resultado de la auto-evaluación del nivel de calificación

Este informe es válido para uso exclusivo de <<Cliente referencia>>, quedando su uso expresamente prohibido para otros propósitos.

Fecha de emisión: DD de MMM de YYYY

Entidad prestadora del Servicio	Identificación del Servicio
CLIENT NAME	**SERVICE NAME**

Descripción

Este documento recoge el resultado del proceso de auto-evaluación llevado a cabo por la entidad mencionada en el encabezado mediante una herramienta online E-Qualify Premium (https://e-qualify.leetsecurity.com) desarrollada y gestionada por LEET Security, para obtener una orientación del nivel de calificación para el Servicio objeto de auto-evaluación.

Este nivel de calificación se obtiene, exclusivamente, sobre la base de las respuestas indicadas por la propia entidad proveedora del servicio en cuanto a la aplicabilidad y, en su caso, existencia de los controles incluidos en la metodología de calificación en su versión 3, sin que se haya realizado ningún tipo de verificación sobre ls mismas.

LEET Security no se hace responsable de la veracidad de las respuestas proporcionadas y, por tanto, el resultado de esta auto-evaluación no puede entenderse como sustitutiva, en ningún caso, de una calificación formal emitida por LEET Security.

Datos facilitados

El contexto de controles se ha establecido en base a la información que ha sido declarada en su inicio, en relación a la modalidad del servicio evaluado, limitando así el alcance, y de la posesión de otras certificaciones relacionadas, con las que se consideran cumplimentados los controles que se corresponden con las mismas.

Nivel máximo evaluado (objetivo)	A+ / A / B / C / D
Servicio de personal, en instalaciones y con equipos del cliente	Si/No
Conexión a sistemas del cliente mediante escritorio virtual	Si/No
Conexión remota a sistemas del cliente	Si/No
Asesoria y proceso de información de cliente en sistemas propios	Si/No
Servicio de tipo "Cloud" (IaaS/PaaS/SaaS)	Si/No
Se realizan desarrollos o basado en desarrollos propios	Si/No
Utilización de terceras partes / proveedores externos	Si/No
Se gestiona alguna PKI propia	Si/No
Existe tratamiento o transmisión de información personal	Si/No
Los servidores se alojan en un CPD propio	Si/No
Se conservan y analizan los registros de actividad	Si/No
Certificación ISO 27001	Si/No
Certificación ISO 20000	Si/No
Certificación ISO 22301	Si/No
Certificación ENS	No/Básica/Media/Alta
Certificación PCI-DSS	Si/No
Certificación CCM	Si/No
Calificación C4V	Si/No

QUALIFY by LEET Security

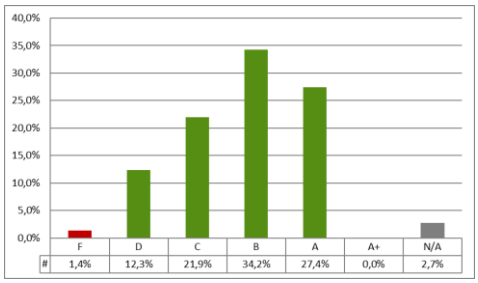
LOGO

Resultado de la auto-evaluación del nivel de calificación

Este informe es válido para uso exclusivo de <<Cliente referencia>>, quedando su uso expresamente prohibido para otros propósitos.

Resultado de la auto-evaluación

El nivel de calificación global y calificación cuantitativa, así como el resumen de evaluación base de cada una de las secciones según el nivel de calificación individual, resultantes de las respuestas a la autoevaluación, son los siguientes:



Los criterios para asignar la calificación global requieren la implantación, para cada dimensión, de:

- El 100% de las medidas generales y para la dimensión correspondiente, de prioridad '1'.
- Al menos, el 85% de las medidas generales y para la dimensión correspondiente, de prioridad '2'.
- Al menos, el 50% de las medidas generales y para la dimensión correspondiente, de prioridad '3'.

A continuación, se muestra la calificación obtenida en cada una de las secciones.
El resultado Base se obtiene aplicando un requisito del 100%; es decir, para que una sección muestre un nivel, deben estar implementados la totalidad los controles aplicables -sea cual sea su prioridad- asociados a dicho nivel.
El resultado Ponderado requiere la existencia del 100% de los controles de prioridad 1 (con un máximo de 2 fallos en controles no prioritarios).
El resultada para cada dominio es inferior de los resultados de las secciones que lo componen.
Se indican también el número de controles totales para el nivel objetivo, los que resultan de aplicación y los implantados para cada sección, en base a las respuestas aportadas.

	Nº Controles			Resultado	
Sección	**Tot**	**Apl**	**Imp**	**Base**	**Ponderado**
01. Gestión de la seguridad de la información				**D**	**C-**
[MS.01] Estrategia y planificación de la seguridad	9	9	9	**A**	**A**
[MS.02] Asignación de responsabilidades	10	10	10	**A**	**A**
[MS.03] Gestión del riesgo	13	12	11	**B**	**A-**
[MS.04] Asignación de recursos	12	4	4	**A**	**A**
[MS.05] Políticas y estándares de seguridad	7	7	6	**B**	**A-**
[MS.06] Pruebas de seguridad, procesos y desempeño	21	21	15	**D**	**C-**
02. Operación de los sistemas				**F**	**B-**
[SO.01] Gestión de cambios	11	9	8	**B**	**B**
[SO.02] Identificación y gestión de activos	12	11	10	**D**	**A-**
[SO.03] Gestión de la información y el conocimiento	29	22	18	**D**	**B-**
[SO.04] Seguridad de la información de los sistemas	6	6	5	**C**	**A-**
[SO.05] Requerimientos de seguridad para los sistemas de información	28	22	20	**D**	**A-**
[SO.06] Control del software operacional	11	7	6	**A**	**A**
[SO.07] Teletrabajo	23	22	19	**F**	**A-**
[SO.08] Soporte de software y sistemas	3	2	2	**A**	**A**
[SO.09] Procesamiento seguro	15	7	6	**C**	**A-**

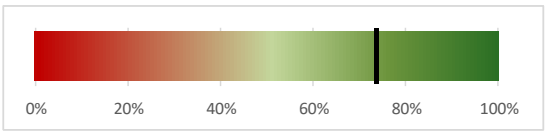
[SO.10] Control de vulnerabilidades	26	24	22	C	A-
03. Seguridad del personal				**B**	**B**
[PS.01] Responsabilidades de los usuarios	8	8	8	A	A
[PS.02] Formación y concienciación	17	16	13	B	B
[PS.03] Seguridad de las personas	7	7	7	A	A
04. Seguridad de las instalaciones				**B**	**B**
[FS.01] Perímetro físico	29	26	23	B	B
[FS.02] Controles de entrada	23	23	19	B	B
[FS.03] Disposición y protección de los equipos	33	33	33	A	A
[FS.04] Seguridad de los equipos en el exterior	6	6	6	A	A
[FS.05] Protección de los medios de información durante el transporte	12	2	2	A	A
[FS.06] Seguridad en la eliminación de equipos	3	3	1	B	A-
[FS.07] Gestión de medios removibles	6	5	5	A	A
[FS.08] Eliminación de medios	6	4	4	A	A
[FS.09] Políticas de escritorio y pantalla limpios	4	4	3	B	B
05. Aseguramiento de la cadena de suministro				**D**	**B**
[TP.01] Procesamiento compartido	15	5	5	A	A
[TP.02] Portabilidad de la información y los servicios	8	0	0	N/A	N/A
[TP.03] Garantías en la finalización de servicios	6	5	4	D	A-
[TP.04] Gestión de terceras/cuartas partes	18	18	13	B	B
06. Resiliencia				**D**	**B**
[RE.01] Cifrado de los medios de respaldo	4	4	4	A	A
[RE.02] Protección frente amenazas externas y ambientales	15	15	12	B	B
[RE.03] Gestión de la capacidad	12	11	8	B	B
[RE.04] Recuperación de la información	23	21	18	B	B
[RE.06] Aspectos de seguridad en la continuidad de negocio	39	39	35	B	B
[RE.07] Mantenimiento de los sistemas	14	14	11	D	A-
[RE.08] Resiliencia operacional	5	5	4	B	B
07. Cumplimiento				**C**	**B-**
[CO.01] Con los requerimientos legales	39	31	27	C	B-
[CO.02] Con las políticas y estándares técnicos y de seguridad	8	6	6	A	A
[CO.03] Auditorías de cumplimiento	3	3	3	A	A
08. Protección contra código malicioso				**C**	**B-**
[MP.01] Protección contra malware	19	19	16	C	B-
09. Controles de red				**C**	**B-**
[NC.01] Gestión de red	16	14	14	A	A
[NC.02] Controles de enrutamiento	19	19	17	C	A-
[NC.03] Segregación de redes	19	18	16	B	B
[NC.04] Autenticación de usuarios desde conexiones externas	17	16	14	B	B
[NC.05] Mantenimiento de la confidencialidad sobre redes públicas	8	8	7	C	B-
[NC.06] Mantenimiento de la integridad sobre redes públicas	5	5	4	C	B-

[NC.07] Disponibilidad de los servicios de red	7	6	6	A	A
10. Supervisión				**D**	**C**
[MO.01] Registros de auditoría	11	11	8	D	B-
[MO.02] Monitorización del uso de los sistemas	18	17	13	C	C
[MO.03] Protección de los registros	12	12	10	B	B
[MO.04] Fugas de información	6	5	3	B	B
[MO.05] Ciberinteligencia y compartición de información	9	9	6	C	B-
11. Control de acceso				**D**	**C-**
[AC.01] Niveles de garantía	10	8	8	A	A
[AC.02] Identificación de los usuarios	11	7	5	D	C-
[AC.03] Gestión de la identificación de los usuarios	10	8	6	B	A-
[AC.04] Uso de las herramientas del sistema	7	7	6	C	A-
[AC.05] Requisitos para autenticadores	78	64	57	D	C-
[AC.06] Gestión de autenticadores	33	30	26	B	B
[AC.07] Restricciones de acceso a la información	16	12	11	B	B
[AC.08] Gestión de los privilegios	10	8	6	C	C
12. Desarrollo seguro				**C**	**B-**
[SD.01] Control de acceso a código fuente	7	7	7	A	A
[SD.02] Procedimientos de control de cambios	11	11	10	B	A-
[SD.03] Seguridad por defecto (desarrollo seguro de sistemas y aplicaciones)	20	15	11	C	B-
[SD.04] Externalización de desarrollo de software	9	7	7	A	A
[SD.05] Informes de vulnerabilidades	3	3	2	B	A-
[SD.06] Segregación de entornos	6	6	5	B	A-
[SD.07] Protección de los datos del sistema	5	5	4	A	A
13. Gestión de incidentes				**B**	**A-**
[IH.01] Informes de incidentes y debilidades	11	11	10	A	A
[IH.02] Gestión de incidentes y mejora	20	20	18	B	A-
14. Cifrado				**N/A**	**N/A**
[CR.01] Gestión de claves	58	0	0	N/A	N/A

Privacidad

Este apartado únicamente es relevante en caso de procesar datos de carácter personal. Se han evaluado los controles que deberían estar implantados para la ejecución de estos tratamientos, con las medidas de seguridad técnicas y organizativas apropiadas al nivel indicado como objetivo. El grado de implantación resultante para las mismas es el indicado a continuación:

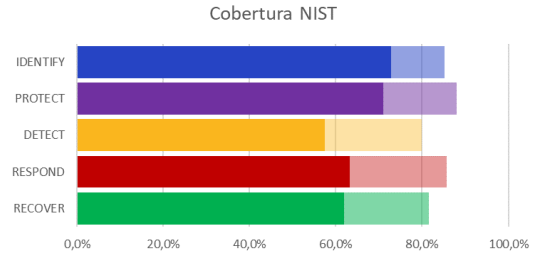
CALIFICADOR DE PRIVACIDAD NIVEL "A"	Aplican	112
	Cumple	82
		73%



Implantación del marco de ciberseguridad del NIST

Este informe es válido para uso exclusivo de <<Cliente referencia>>, quedando su uso expresamente prohibido para otros propósitos.

El siguiente gráfico muestra el porcentaje de implementación de los controles aplicables en el servicio, para el nivel objetivo evaluado (marca decolorada) como respecto al nivel máximo (marca de color intenso), por cada una de las cinco etapas del marco de ciberseguridad.



Oportunidades de mejora

El nivel de calificación global responde a la aplicación de la regla de otorgar el mínimo nivel alcanzado en los controles asignados a cada dimensión.

------ Opción 1: No se ha alcanzado el nivel objetivo

Según las respuestas proporcionadas, los controles de prioridad '1' que estarían actuando como factores limitantes para alcanzar niveles superiores serían los indicados a continuación.

Controles a implantar para alcanzar un nivel C:

Referencia	Dimensión	Sección	Control
[FS.03]08.01-A2	Disponibilidad	[FS.03] Disposición y protección de los equipos	La organización emplea dispositivos/servicios de detección y extinción de incendios para el sistema de información conectados a un sistema de alimentación independiente.
[RE.02]03.01-A2	Disponibilidad	[RE.02] Protección frente amenazas externas y ambientales	El sitio de procesamiento alterno ofrece garantías de seguridad de la información equivalentes a las del sitio principal.
[NC.07]01.01-A2	Disponibilidad	[NC.07] Disponibilidad de los servicios de red	Se han identificado los procesos críticos del negocio que dependen de conexiones externas.

Controles a implantar para alcanzar un nivel B:

Referencia	Dimensión	Sección	Control
[SO.03]05.03-C3	Confidencialidad	[SO.03] Gestión de la información y el conocimiento	Al enviarse, debe mantenerse bajo control de personas autorizadas, no dejarse desatendida y, si telemáticamente, cifrada.
[FS.03]06.05-A3	Disponibilidad	[FS.03] Disposición y protección de los equipos	La capacidad de combustible del generador es de 24 horas.
[FS.03]08.01-A2	Disponibilidad	[FS.03] Disposición y protección de los equipos	La organización emplea dispositivos/servicios de detección y extinción de incendios para el sistema de información conectados a un sistema de alimentación independiente.
[FS.05]01.03-C3	Confidencialidad	[FS.05] Protección de los medios de información durante el transporte	Los medios se cifran o protegen con protección equivalente.

[RE.01]02.01-C3	Confidencialidad	[RE.01] Cifrado de los medios de respaldo	Los dispositivos extraíbles de respaldo están protegidos mediante cifrado.
[RE.02]03.01-A2	Disponibilidad	[RE.02] Protección frente amenazas externas y ambientales	El sitio de procesamiento alterno ofrece garantías de seguridad de la información equivalentes a las del sitio principal.
[RE.03]03.02-A3	Disponibilidad	[RE.03] Gestión de la capacidad	El proveedor de servicios ofrece garantías sobre los recursos máximos disponibles dentro de un período mínimo (> 25%).
[RE.04]01.04-A3	Disponibilidad	[RE.04] Recuperación de la información	Las copias de respaldo cubren toda la información del sistema, las aplicaciones y los datos necesarios para recuperar el sistema completo en caso de un desastre (incluidos los dispositivos móviles).
[AC.07]03.03-C3	Confidencialidad	[AC.07] Restricciones de acceso a la información	El sistema permite implementar separación de funciones.

Controles a implantar para alcanzar un nivel A:

Referencia	Dimensión	Sección	Control
[MS.01]01.04-G4	General	[MS.01] Estrategia y planificación de la seguridad	Orientación y soporte claro a las iniciativas de seguridad de la información.
[MS.06]03.02-G4	General	[MS.06] Pruebas de seguridad, procesos y desempeño	La ejecución del plan está supervisado por un Comité de Auditoría.
[SO.01]03.04-G4	General	[SO.01] Gestión de cambios	La organización revisa y reevalúa los privilegios de los desarrolladores de sistemas, al menos, trimestralmente.
[FS.01]10.02-G4	General	[FS.01] Perímetro físico	Evaluación de los riesgos del perímetro físico y evaluación de los perímetros al menos dos veces al año.
[FS.02]01.05-G4	General	[FS.02] Controles de entrada	Todas las salas tienen controles de acceso con registro mediante biometría.
[FS.09]02.02-C4	Confidencialidad	[FS.09] Políticas de escritorio y pantalla limpios	Las pantallas de ordenadores y terminales están protegidas con filtros de privacidad cuando están visibles para el público o usuarios no autorizados.
[RE.03]03.04-A4	Disponibilidad	[RE.03] Gestión de la capacidad	El proveedor de servicios ofrece garantías sobre los recursos máximos disponibles dentro de un período mínimo (> 50%).
[RE.03]03.05-A4	Disponibilidad	[RE.03] Gestión de la capacidad	El proveedor de servicios ofrece garantías sobre la disponibilidad de recursos suplementarios dentro de un período mínimo (> 40%).
[RE.04]02.04-A4	Disponibilidad	[RE.04] Recuperación de la información	Los procedimientos de respaldo se prueban, al menos, una vez al año.

[RE.04]02.05-A4	Disponibilidad	[RE.04] Recuperación de la información	La recuperación de datos de respaldo se prueba, al menos, todos los meses.
[RE.06]01.06-A4	Disponibilidad	[RE.06] Aspectos de seguridad en la continuidad de negocio	Gestión, actualización y verificación de los Análisis de Impacto sobre el Negocio, los RTO y los RPO.
[RE.06]02.03-A4	Disponibilidad	[RE.06] Aspectos de seguridad en la continuidad de negocio	La organización evalúa el plan de contingencia en el sitio de procesamiento alterno, incluyendo una prueba de la copia de seguridad de la información en la restauración. Se corrigen los problemas encontrados durante las pruebas.
[RE.06]04.06-A4	Disponibilidad	[RE.06] Aspectos de seguridad en la continuidad de negocio	RPO – 12 horas
[RE.06]04.07-A4	Disponibilidad	[RE.06] Aspectos de seguridad en la continuidad de negocio	RTO – 4 horas
[RE.06]06.04-A4	Disponibilidad	[RE.06] Aspectos de seguridad en la continuidad de negocio	Se garantiza a los clientes una disponibilidad del 99,99% (0,8 horas de interrupción al año).
[RE.08]01.04-A4	Disponibilidad	[RE.08] Resiliencia operacional	Los requisitos de ciber-resiliencia están documentados y actualizados, y son gestionados y verificados
[CO.01]02.08-G3	General	[CO.01] Con los requerimientos legales	Los datos, objetos, aplicaciones, infraestructura y hardware tienen asignado un dominio y jurisdicción legislativa para facilitar el cumplimiento normativo.
[NC.03]02.09-G4	General	[NC.03] Segregación de redes	Uso de mecanismos de seguridad de puertos para limitar el número de direcciones MAC permitidas (o similares, IEEE 802.1x y EAP, etc.). El sistema de autenticación debe estar vinculado a los datos del inventario de activos de hardware para garantizar que solo los dispositivos autorizados puedan conectarse a la red.
[NC.04]03.02-G4	General	[NC.04] Autenticación de usuarios desde conexiones externas	Se monitorizan las cuentas utilizadas por los proveedores para acceso remoto cuando estas se usan

[NC.05]01.04-C3	Confidencialidad	[NC.05] Mantenimiento de la confidencialidad sobre redes públicas	La tunelización dividida está deshabilitada en los dispositivos clientes de VPN.
[NC.06]01.04-I3	Integridad	[NC.06] Mantenimiento de la integridad sobre redes públicas	La tunelización dividida está deshabilitada en los dispositivos clientes de VPN.
[MO.01]01.04-G4	General	[MO.01] Registros de auditoría	Los registros de auditoría también incluyen: · Uso de las utilidades y aplicaciones del sistema. · Archivos a los que se accede y tipo de acceso. · Registro de cada acceso.
[MO.02]01.03-G4	General	[MO.02] Monitorización del uso de los sistemas	Los registros de auditoría de todos los componentes del sistema también permiten reconstruir los siguientes incidentes: · Intentos de acceso no autorizado. · Inserción/extracción de dispositivos de entrada/salida. · Alertas o mensajes de la consola. · Excepciones de registros de los sistemas. · Alarmas de gestión de redes. · Cambios o intentos de cambio de las configuraciones de seguridad del sistema. · (Si aplica) Si se ha modificado Información sensible o Personal (agregada, modificada o eliminada) como resultado de un evento y por quién. · (Si procede) Intentos de restauración de datos personales. En SCI, un fallo potencial de dichos mecanismos no debe afectar a las funciones esenciales y, en caso de que el fabricante no proporcionen dichos registros, se permitirán mecanismos alternativos con el objetivo de permitir la trazabilidad de las acciones (p.ej. registros alternativos o incluso manuales).
[MO.02]07.01-G4	General	[MO.02] Monitorización del uso de los sistemas	Se emplean mecanismos de detección de cambios (por ejemplo, herramientas de monitorización de la

			integridad de archivos) para alertar al personal de la modificación no autorizada de los archivos críticos del sistema, los archivos de configuración o los archivos de contenido; y se configura el software para que realice comparaciones de archivos críticos al menos semanalmente. En SCI, estos sistemas podrán ser de tipo pasivo.
[MO.03]01.04-G4	General	[MO.03] Protección de los registros	Los registros se almacenan durante, al menos, 5 años.
[MO.03]05.03-G4	General	[MO.03] Protección de los registros	Los administradores de sistemas no tienen permiso para borrar o desactivar el registro de su propia actividad.
[AC.05]02.03-G4	General	[AC.05] Requisitos para autenticadores	Limitar a 3 el número permitido de intentos fallidos de inicio de sesión.
[AC.05]07.05-G4	General	[AC.05] Requisitos para autenticadores	Imponer cambios de contraseñas cada 60 días.
[AC.05]12.03-G3	General	[AC.05] Requisitos para autenticadores	Antes de que el usuario cambie los secretos memorizados, el valor propuesto se compara con una lista que contiene valores que se sabe que son de uso común, esperados o comprometidos (por ejemplo, contraseñas obtenidas de violaciones anteriores, palabras de diccionario, caracteres repetitivos o secuenciales, o relación con el contexto, como el nombre del servicio, el nombre de usuario y derivados del mismo).
[AC.07]03.03-C3	Confidencialidad	[AC.07] Restricciones de acceso a la información	El sistema permite implementar separación de funciones.
[AC.07]04.02-C4	Confidencialidad	[AC.07] Restricciones de acceso a la información	Se dispone de un control para impedir el acceso a la información por el proveedor sin el consentimiento del cliente.
[AC.08]02.02-I4	Integridad	[AC.08] Gestión de los privilegios	Los derechos de acceso de usuario se revisan cada 6 meses y aquellos con privilegios especiales cada 3 meses

------ Opción 2: Sí se ha alcanzado el nivel objetivo

Según las respuestas proporcionadas se ha alcanzado el nivel objetivo establecido, por lo que no se dan factores limitantes a consignar en este apartado.

LOGO

Resultado de la auto-evaluación del nivel de calificación

Este informe es válido para uso exclusivo de <<Cliente referencia>>, quedando su uso expresamente prohibido para otros propósitos.

El referencial de controles utilizados en la auto-evaluación es el íntegro correspondiente a la versión 3.1, que está disponible para su descarga, junto a la metodología de calificación, en el siguiente enlace:
https://leetsecurity.com/dl/whitepaper/request/?wpslug=security-rating-guide

LEET Security, S.L.
Calle López de Hoyos, 125
28002 Madrid
Tel: +34 915 798 187
info@leetsecurity.com

Estado del documento

Versión	Elaborado	Revisado	Aprobado
1.0	Nombre: Antonio Ramos Fecha: 3/8/17	Nombre: Antonio Ramos Fecha: 3/8/17	Nombre: Antonio Ramos Fecha: 3/8/17
1.1	Nombre: Alfonso Pastor Fecha: 24/8/17		
2.0	Nombre: Alfonso Pastor Fecha: 2/2/2018		
3.0	Nombre: Alfonso Pastor Fecha: 01/11/2021		

Control de versiones

Versión	Fecha	Descripción – Motivos del cambio	Página(s) modificada(s)
1.0	3/8/17	Elaboración inicial	Todas
1.1	24/8/17	Cambios redacción	1
2.2	2/3/2018	Ampliación contenidos: Contexto y secciones completas	todas
3.0	1/11/2021	Ampliación de información y adecuación a metodología v3.1	Todas