INFORME DE PREPARACIÓN PARA CYBER ESSENTIALS

Example GmbH

PERIODO	DOMINIOS	HOSTS	CREADO EL
23/6/2026 – 21/9/2026	1	8	14/10/2026

Este informe asigna los hallazgos de Example GmbH visibles desde el exterior a los cinco controles técnicos de Cyber Essentials, el esquema de certificación del NCSC británico (requisitos v3.3, cuestionario «Danzell», vigente desde el 27 de abril de 2026). Muestra dónde ya se ve desde fuera que hay que actuar y qué debe acreditar todavía internamente. veyrisk no certifica.

1. Resumen

4 hallazgos abiertos harían probablemente que no se superase la evaluación. Corríjalos antes de presentar la autoevaluación.

CONTROL	ESTADO	HALLAZGOS ABIERTOS	PROBABLE SUSPENSO
Cortafuegos	HALLAZGOS ABIERTOS	3	2
Configuración segura	HALLAZGOS ABIERTOS	5	0
Gestión de actualizaciones de seguridad	HALLAZGOS ABIERTOS	1	1
Control de acceso de usuarios	HALLAZGOS ABIERTOS	1	1
Protección contra malware	NO EVALUABLE DESDE FUERA	0	0

2. Cortafuegos

HALLAZGOS ABIERTOS

Qué comprueba veyrisk desde fuera

Desde internet solo deben ser accesibles los servicios necesarios. veyrisk comprueba puertos abiertos (solo con prueba de titularidad), interfaces de administración accesibles públicamente y sistemas de desarrollo y pruebas.

GRAVEDAD	HALLAZGO	ABIERTO DESDE (DÍAS)	NOTA

ALTO	vpn.example.com RDP accesible desde internet (puerto 3389)	38	ALTO O CRÍTICO Y ABIERTO MÁS DE 14 DÍAS
ALTO	shop.example.com Interfaz de administración accesible públicamente (phpMyAdmin)	61	ALTO O CRÍTICO Y ABIERTO MÁS DE 14 DÍAS
MEDIO	dev.example.com Sistema de desarrollo o de pruebas accesible públicamente	61	

A acreditar internamente

- Un cortafuegos en cada frontera con internet, con la contraseña predeterminada cambiada
- Cada regla de entrada documentada y justificada; las que ya no se necesitan, eliminadas
- Un cortafuegos de software en los equipos que se usan en redes ajenas, como wifi públicas

3. Configuración segura

HALLAZGOS ABIERTOS

Qué comprueba veyrisk desde fuera

Equipos y servicios están bastionados: sin software innecesario, sin cuentas predeterminadas y con ajustes seguros. veyrisk comprueba certificados, TLS, HTTPS, cabeceras de seguridad y la divulgación de versiones, además de hallazgos de configuración de las revisiones de aplicaciones web y nube.

GRAVEDAD	HALLAZGO	ABIERTO DESDE (DÍAS)	NOTA
MEDIO	mail.example.com El certificado TLS caduca en 9 días	3	
MEDIO	shop.example.com Falta la cabecera Strict-Transport-Security	90	
BAJO	www.example.com Versión de software visible en la cabecera Server (Apache/2.4.49)	45	
BAJO	www.example.com Falta la cabecera Content-Security-Policy	90	
BAJO	portal.example.com Falta la cabecera X-Content-Type-Options	90	

A acreditar internamente

- Software, servicios y cuentas de usuario innecesarios eliminados o desactivados
- Contraseñas predeterminadas cambiadas y ejecución automática desactivada
- Bloqueo de pantalla con PIN, contraseña o biometría en todos los equipos

4. Gestión de actualizaciones de seguridad

HALLAZGOS ABIERTOS

Qué comprueba veyrisk desde fuera

Todo el software tiene licencia y sigue contando con soporte del fabricante. Las actualizaciones críticas y de alto riesgo deben instalarse en un plazo de 14 días desde su publicación. veyrisk utiliza para ello los hallazgos de Advanced Vulnerability Detection y los hallazgos de aplicaciones web con CVE.

GRAVEDAD	HALLAZGO	ABIERTO DESDE (DÍAS)	NOTA
ALTO	vpn.example.com OpenSSH 'regreSSHion' Remote Code Execution Vulnerability (22/tcp)	26	ALTO O CRÍTICO Y ABIERTO MÁS DE 14 DÍAS

A acreditar internamente

- Inventario de todos los equipos del alcance con sistema operativo y versión
- Solo sistemas operativos y aplicaciones con soporte; los que ya no lo tienen, eliminados o aislados
- Actualizaciones automáticas activadas cuando sea posible; si no, prueba de la instalación en 14 días

5. Control de acceso de usuarios

HALLAZGOS ABIERTOS

Qué comprueba veyrisk desde fuera

Las cuentas solo se crean cuando hacen falta y los derechos de administrador se usan con cuentas separadas. La MFA es obligatoria en todos los servicios en la nube que la ofrecen; sin ella, la evaluación no se supera automáticamente. Las passkeys cuentan como inicio de sesión sin contraseña. veyrisk solo lo ve en las cuentas en la nube y de Microsoft 365 conectadas.

GRAVEDAD	HALLAZGO	ABIERTO DESDE (DÍAS)	NOTA
ALTO	Microsoft 365 (example.com) Ensure multifactor authentication is enabled for all users	9	FALTA MFA: SUSPENSO AUTOMÁTICO

A acreditar internamente

- MFA para todos los usuarios en cada servicio en la nube que la ofrezca
- Cuentas de administrador separadas que no se usan para correo ni navegación
- Un proceso definido para crear y eliminar cuentas, con revisión periódica de los permisos
- Reglas de contraseñas o inicio de sesión sin contraseña con passkeys, protección contra ataques de fuerza bruta

6. Protección contra malware

NO EVALUABLE DESDE FUERA

Qué comprueba veyrisk desde fuera

En todos los equipos del alcance funciona una protección contra malware. Esto no se puede comprobar desde fuera.

La protección contra malware no se puede comprobar desde fuera.

A acreditar internamente

- Antivirus con firmas actualizadas en todos los equipos o lista de aplicaciones permitidas
- Análisis de archivos al acceder a ellos y protección contra sitios web maliciosos

7. Notas y limitaciones

Este informe es una comprobación de preparación desde fuera y no una certificación. veyrisk no certifica. Cyber Essentials y Cyber Essentials Plus solo los conceden organismos de certificación con licencia de IASME; Cyber Essentials Plus añade pruebas técnicas. El certificado es válido durante 12 meses.

El alcance comprende todos los equipos conectados a internet y todos los servicios en la nube. veyrisk solo ve los sistemas accesibles públicamente de sus dominios y las cuentas en la nube conectadas. La protección contra malware y la mayor parte del control de acceso no se pueden comprobar desde fuera.

La asignación de los hallazgos a los controles es una valoración de veyrisk. Los hallazgos sobre autenticación del correo (SPF, DMARC, MTA-STS) no pertenecen a ninguno de los cinco controles y no aparecen aquí. Lo determinante son los requisitos del NCSC y la valoración de su organismo de certificación.

VEYRISK · NEONOTU GMBH

Edelsbergstraße 8, 80686 München · +49 89 2000 7975 0 · contact@veyrisk.com