WordCamp Valencia 2026

Tu (posible) cliente te ha mandado un cuestionario de seguridad

Guía de supervivencia

Por Néstor Angulo de Ugarte

¿Vuestra organización tiene una política de seguridad de la información aprobada?

Sí

No

JULIO DE 2022 · ESTADOS UNIDOS

9 millones $

Aerojet Rocketdyne, contratista de defensa, paga para cerrar una demanda: **haber declarado un cumplimiento de ciberseguridad que no tenía.**

- Destapada por ex-empleado del propio área de ciberseguridad.
- Acuerdo al 2º día del juicio.

Acuerdo sin determinación de responsabilidad: la empresa no admitió culpa.
Fuente: Departamento de Justicia de EE. UU., 8 de julio de 2022.



No sois Aerojet.
Pero vuestro Excel es igual.

14	¿Se utiliza autenticación multifactor en todos los accesos a sistemas con datos del cliente?	**Sí**

No sois Aerojet.
Pero vuestro Excel es igual.

14	¿Se utiliza autenticación multifactor en todos los accesos a sistemas con datos del cliente?	**Sí**

Esto no es un trámite. Es una declaración.

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	ID	CCM Control Specification	CCM Co
A&A-01.1	Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained?			1	Establish, document, approve, communicate, apply, evaluate, and maintain audit and assurance policies and procedures and standards. Review and update the policies and procedures at least annually, or upon significant changes.	Audit and A and Pr
A&A-01.2	Are audit and assurance policies, procedures, and standards reviewed and updated at least annually, or upon significant changes?					
A&A-02.1	Are independent audit and assurance assessments conducted according to relevant standards at least annually?			2	Conduct independent audit and assurance assessments according to relevant standards at least annually.	Independen
A&A-03.1	Are independent audit and assurance assessments performed according to risk-based plans and policies, and in response to significant changes or emerging risks?			3	Perform independent audit and assurance assessments according to risk-based plans and policies, and in response to significant changes or emerging risks.	Risk Bas Asse
A&A-04.1	Is compliance verified regarding all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit?			4	Verify compliance with all relevant standards, regulations, legal/contractual, and statutory requirements applicable to the audit.	Requiremen
A&A-05.1	Is an audit management process defined and implemented to support audit planning, risk analysis, security control assessments, conclusions, remediation schedules, report generation, and reviews of past reports and supporting evidence and aligned with relevant auditing standards?			5	Define and implement an Audit Management process aligned with relevant auditing standards to support audit planning, risk analysis, security control assessment, conclusion, remediation schedules, report generation, and review of past reports and supporting evidence.	Audit Manag
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?			6	Establish, document, approve, communicate, apply, evaluate, and maintain a risk-based corrective action plan to remediate audit findings, regularly review and report remediation status to relevant stakeholders.	Rem
A&A-06.2	Is the remediation status of audit findings regularly reviewed and reported to relevant stakeholders?					
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained?				Establish, document, approve, communicate, apply, evaluate, and maintain policies and procedures for application security. Review and update the policies and procedures at least annually, or upon significant changes.	

Lo he visto desde los dos lados

Como proveedor

Rellenando cuestionarios de clientes, con la tentación de contestar que sí a todo.

Montando el programa

Construyendo después la parte que permite contestarlos con evidencia, no con fe.



Durante años os lo hemos pedido con cariño.

- MFA
- Copias que se restauran
- Actualizaciones
- Menos Administradores

Durante años os lo hemos pedido con cariño.

Ahora os lo pide vuestro cliente.
En un Excel. Antes de firmar.

ANTES

- Lo comprobaba un **atacante** a posteriori
- Saltártelo era un **riesgo** que *quizá nunca llegaba.*

AHORA

- Lo pregunta tu **cliente**, antes de firmar.
- Saltártelo te **cuesta** el proyecto.

PREGUNTA

¿Por qué me lo mandan a mí?



Porque la obligación baja por la cadena

Su auditor o regulador
ISO 27001, SOC 2, NIS2, DORA

→

Tu (posible) cliente
tiene que demostrar que controla a sus proveedores

→

Tú
agencia, freelance, mantenimiento WordPress

→

Tus proveedores
hosting, plugins con servicio externo, correo, herramientas de IA

Si tocas datos de tu cliente, para el RGPD eres su encargado del tratamiento (art. 28).
Su obligación de controlar proveedores baja por contrato… y tú se la bajas a los tuyos.

Te puede llegar de tres formas

120

preguntas en un Excel antes de firmar

1

"Mándanos tu política de seguridad de la información"

?

"¿Estáis certificados en algo?"

Antes de firmar, la misma pregunta:
¿puedo fiarme de ti con mis datos?

Las dos reacciones que salen caras

"Sí" a todo

- Ganas el proyecto.
- Firmas promesas que no cumples.
- Si pasa algo, el Excel es **la prueba contra ti.**

Bloquearse

- No contestas, o contestas tarde y a medias.
- El proyecto se va a otro que sí contestó.

La tercera vía: **honesta y suficiente.**

Cómo leer cada pregunta

1. **Qué pregunta**
   La letra literal de la fila.

2. **Qué riesgo intenta cubrir**
   Lo que le preocupa de verdad a tu cliente.

3. **Qué respuesta es honesta y suficiente**
   La que puedes defender si un día la releen.

Votación a mano alzada: A, B o C.



14	¿Se utiliza autenticación multifactor en todos los accesos a sistemas con datos del cliente?

A Sí.

B No.

C Sí en WordPress, hosting y correo. Pendiente en el acceso SFTP: lo cerramos antes del [fecha].

El riesgo que cubre

Que una contraseña robada abra la puerta. Y que la puerta siga abierta cuando alguien se va del equipo.

La que te hunde

A, si hay un solo acceso sin MFA. Basta uno para que el "Sí" sea falso.

La honesta y suficiente

C. Dice qué está cubierto, qué falta y cuándo se cierra. Es verificable y defendible.

La de al lado en el Excel:
"¿Retiráis los accesos cuando alguien deja el proyecto?"

Revisa quién es Administrador en cada WordPress, hosting y SFTP/SSH (proceso de offboarding).

27	¿Se realizan copias de seguridad periódicas y se verifica su restauración?

A Sí, diarias.

B Sí, tenemos un plugin de copias en WordPress.

C Sí. Copias diarias fuera del servidor; restauramos la web en un staging una vez al trimestre.

El riesgo que cubre

Que un ataque, un error o un ransomware te deje sin web y sin datos del cliente, sin forma de volver.

La que te hunde

A y B. Contestan solo la mitad de la pregunta. Y si la copia vive en el mismo servidor, cae con él.

La honesta y suficiente

C. Dónde está la copia, cada cuánto y cuándo se restauró en un staging. Si nunca lo has hecho, dilo, y pon fecha.

Una copia que nunca has restaurado no es una copia: **es una hipótesis.**

41	En caso de incidente de seguridad que afecte a datos del cliente, ¿se compromete a notificarlo en un máximo de 24 horas?

A Sí.

B No.

C Sí, 24 horas desde que lo detectemos. Contacto de incidentes: [nombre, teléfono]. Procedimiento de una página adjunto.

El riesgo que cubre

Que tu cliente se entere tarde de un problema con sus datos. Él tiene sus propios plazos legales que cumplir.

La que te hunde

A, si no sabes quién llama a quién un sábado. B te saca de la lista: dar un plazo es razonable.

La honesta y suficiente

C. Plazo desde la detección, una persona de contacto y un procedimiento escrito, aunque sea de una página.

Fíjate en desde cuándo corre el reloj. Esa frase **se negocia** en el contrato, no en el Excel.

Y otras tres que van a salir seguro

Proveedores

"¿Qué terceros tienen acceso a nuestros datos?"

Subencargados e IA

"¿Usáis/entrenáis herramientas de IA con nuestros datos?"

Borrado

"¿Qué pasa con nuestros datos al terminar el contrato?"

Y otras tres que van a salir seguro

Proveedores

"¿Qué terceros tienen acceso a nuestros datos?"

Ten la lista: hosting, correo y los plugins que sacan datos fuera de WordPress (formularios, analítica, CRM).

Subencargados e IA

"¿Usáis/entrenáis herramientas de IA con nuestros datos?"

- La pregunta nueva.
- Di cuáles, con qué datos y con qué condiciones.
- "No sé" no es respuesta.

Borrado

"¿Qué pasa con nuestros datos al terminar el contrato?"

Qué borras (pedidos de WooCommerce, envíos de formularios), en qué plazo, y qué pasa con las copias, que también los guardan.

Tres clásicas si trabajas con WordPress

Mantenimiento

"¿Cómo y cada cuánto actualizáis el núcleo, los plugins y los temas?"

Hosting

"¿Dónde están alojados nuestros datos y quién tiene acceso al servidor?"

SEO y marketing

"¿Cómo accedéis a nuestras cuentas: Search Console, Analytics, DNS?"



Tres clásicas si trabajas con WordPress

Mantenimiento

"¿Cómo y cada cuánto actualizáis el núcleo, los plugins y los temas?"

- Cada **cuánto**, **quién** lo hace y si **se prueba** antes en un staging.
- El inventario: qué plugins hay en cada web y cuáles llevan años sin actualizarse.

Hosting

"¿Dónde están alojados nuestros datos y quién tiene acceso al servidor?"

- País del hosting y de sus copias, servidor compartido o aislado, y quién entra.
- Si revendes hosting, contestas tú por tu proveedor.

SEO y marketing

"¿Cómo accedéis a nuestras cuentas: Search Console, Analytics, DNS?"

- Con usuario propio, invitado desde su cuenta.
- Nunca con su contraseña.
- Al terminar el contrato, ellos te retiran el acceso.

Lo que se arregla en una tarde y lo que no

Una tarde

- MFA en wp-admin, hosting y correo
- Gestor de contraseñas compartido
- Revisar Administradores y plugins de cada WordPress
- Lista de proveedores y plugins que sacan datos
- Restaurar una copia en un staging, una vez
- Política de una página que describa lo que ya haces
- Contacto y pasos ante un incidente

Un proyecto

- Pruebas de intrusión periódicas
- Plan de continuidad probado
- Monitorización continua
- Certificación ISO 27001 o SOC 2

Esto no se finge en un Excel.

Cómo decir "no" sin caerte de la lista

No, pero…	*"No tenemos monitorización 24/7. Revisamos los accesos cada semana y recibimos alertas de inicio de sesión."*
No todavía	*"MFA en todos los accesos antes del 31 de enero."*
No aplica	*"No guardamos datos de tarjetas: el pago lo procesa la pasarela."*
Mejor así	*"Notificación en 24 horas desde la detección, no desde el incidente."*

Un "no" con contexto vale más que un "sí" que no aguanta una pregunta.

Contesta una vez. Reutiliza siempre.

1 **Banco de respuestas**

Guarda cada respuesta con su evidencia: la captura, el documento, la fecha.

2 **Fecha de revisión**

Una respuesta de hace dos años puede haber dejado de ser verdad.

3 **Pregunta por un estándar**

Existen cuestionarios estándar, como el CAIQ (gratuito) de la Cloud Security Alliance. Pregunta si aceptan uno en lugar de su Excel.

El segundo cuestionario cuesta la mitad. El décimo, una tarde.



14	¿Se utiliza autenticación multifactor en todos los accesos a sistemas con datos del cliente?	**Sí**

Lo que firmas es lo que haces.

Y si todavía no lo haces, dilo, y pon fecha.



El lunes, tres cosas

1	Revisa quién es Administrador en tus WordPress, y activa MFA donde falte.
2	Restaura una copia en un staging. Una. Apunta cuánto tardas.
3	Escribe tu política de una página: lo que ya haces, no lo que te gustaría hacer.



Hoja de una página

Hoja de una página: cada bloque que hemos visto, qué riesgo cubre y la respuesta mínima honesta.


Everybody needs a hacker

Gràcies

¿Preguntas?



Néstor Angulo de Ugarte

CISSP · Head of Technology, ISC2 Spain Chapter

WordCamp Valencia 2026

#WCVLC26