



## **Bastionado de Redes y Sistemas**

### **Tarea 2**

**ESTHER CARRILLO GÁLVEZ**

## Índice

1. Apartado 1 .....	3
1.2. Detección de puntos clave y propuesta de soluciones .....	3
1.2. Propuesta de soluciones .....	4
2. Bibliografía .....	6

# 1. Apartado 1

## 1.2. Detección de puntos clave y propuesta de soluciones

Este caso práctico es un claro ejemplo de mala praxis en cuanto se refiere a ciberseguridad. La empresa Venus SA ha decidido llevar a cabo un proyecto de grandes dimensiones tomando unas decisiones y acciones poco firmes y que comprometen los sistemas de la organización. Para una mejora en las decisiones, se han detectado los siguientes puntos clave:

**La falta de análisis previo.** Al prescindir de una fase de análisis, la empresa podría condenar el proyecto desde los inicios, esto lleva a una asignación de recursos inadecuada y a la implementación de controles de seguridad posiblemente ineficaces. Este desconocimiento podría ser determinante en la seguridad de los activos de la organización, ya que, ante un ataque real, no estarían disponibles los recursos necesarios para identificarlo y mitigarlo.

**Uno de los requisitos principales para la organización es la reducción de costes.** Punto clave para hacer tambalear su infraestructura. Las soluciones de seguridad gratuitas pueden parecer atractivas, pero lo cierto es que el atacante podría usar los puntos débiles para explotarlos. Asimismo, contratar a personal no cualificado podría suponer un riesgo a la hora de responder ante incidentes.

**El uso de gestor de contenidos (CMS) de código abierto** no es del todo menos seguro, pero requiere una gestión y configuración más activa. Esto es, muchos CMS llevan configuraciones por defecto, por lo que es necesario cambiar los nombres de usuarios y las contraseñas que viene de fábrica. Del mismo modo, el CMS de código abierto requiere de una constante política de actualizaciones porque las vulnerabilidades que se hagan públicas pueden comprometer el sistema.

**El servidor se ubicará en el cuarto de la limpieza.** En cualquier caso, un servidor debe de estar aislado y con unas condiciones óptimas para el correcto funcionamiento y que su integridad no se vea comprometida por las condiciones de ubicación.

**La ausencia de Zero Trust** es un error en la empresa Venus SA. La decisión de no adoptar medidas como la autenticación multifactor (MFA) o doble factor (2FA), pone en riesgo los sistemas críticos. De igual modo que la falta del mínimo privilegio es esencial para que ninguna persona disfrute de más permisos de los que realmente necesita.

**Evaluación de la puesta en marcha.** Este paso es primordial para el correcto funcionamiento de los sistemas antes de llevarlo a la práctica real. Una evaluación

inadecuada puede tener consecuencias muy graves para la disponibilidad, la integridad y la confidencialidad de los datos.

## 1.2. Propuesta de soluciones

Una vez analizados los puntos clave para una buena praxis en ciberseguridad, se desglosarán las soluciones propuestas ante tales problemas:

1. Se debe iniciar con un análisis de riesgos, activos y servicios. Para ello, se deben identificar los activos involucrados en el nuevo proyecto, ya sea el hardware, software o datos.
2. Reducción de costes o mayor seguridad. Se debe contratar a personal cualificado, de modo que cumpla con lo necesario para garantizar seguridad y se minimice el riesgo de errores costosos por el factor humano.
3. Implementar una política de *hardening* para que el CMS de código abierto. Se debe renombrar los usuarios administradores y fortalecer las contraseñas que vienen por defecto. Asimismo, establecer una política de actualizaciones para asegurar una óptima gestión de parches.
4. Cambio de ubicación del servidor. Es de máxima urgencia reubicar el servidor a una sala aislada y con control de acceso con una temperatura y humedad adecuadas y así evitar fallos en el sistema.
5. Implementar arquitectura Zero Trust mediante la autenticación multifactor para acceder a todos los sistemas, ya sean servidores, bases de datos, VPN, etc. Además, se deberá garantizar el principio del mínimo privilegio para no exponer los activos de la empresa a riesgos evitables.
6. Establecimiento de puesta en marcha post-implementación. Esta fase es esencial para asegurar que los sistemas son funcionales y seguros antes de ponerlos en marcha en la vida real.
7. Realización periódica de auditorías de seguridad para identificar vulnerabilidades. Se llevarán a cabo auditorías de 3 tipos al menos 1 vez al año cada una: auditoría de compliance, auditorías técnicas y auditoría de seguridad física.

8. Plan de respuesta a incidentes. Es necesaria la redacción de este plan para recoger el *modus operandi* de la organización ante posibles eventos que puedan suponer la modificación o eliminación de los datos.

En conclusión, el caso de Venus SA es un compendio de mala praxis en ciberseguridad, motivado por una escasez de conocimientos e ignorancia a la gravedad del asunto. La prosperidad y el éxito de la organización dependerá de lo que se consoliden estas medidas de seguridad y prevención y lo que se quiera invertir a largo plazo para mantenerlas en el tiempo.

## 2. Bibliografía

National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments* (NIST Special Publication 800-30 Revision 1). U.S. Department of Commerce.

<https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf>

Instituto Nacional de Ciberseguridad (INCIBE). (s.f.). *Fortalecer la ciberseguridad en tu pyme: cómo pasar de la preocupación a la acción*. Recuperado el 25 de noviembre de 2025, de <https://www.incibe.es/empresas/blog/fortalecer-la-ciberseguridad-en-tu-pyme-como-pasar-de-la-preocupacion-la-accion>

Instituto Nacional de Ciberseguridad (INCIBE). (2024). *Guía de gestión de crisis de ciberseguridad en empresas*. INCIBE. <https://www.incibe.es/empresas/blog/guia-de-gestion-de-crisis-de-ciberseguridad-en-empresas>

OWASP Foundation. (s.f.). *Prácticas de Codificación Segura - Guía de Referencia Rápida*. Recuperado el 25 de noviembre de 2025, de <https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-es/01-introduction/05-introduction>