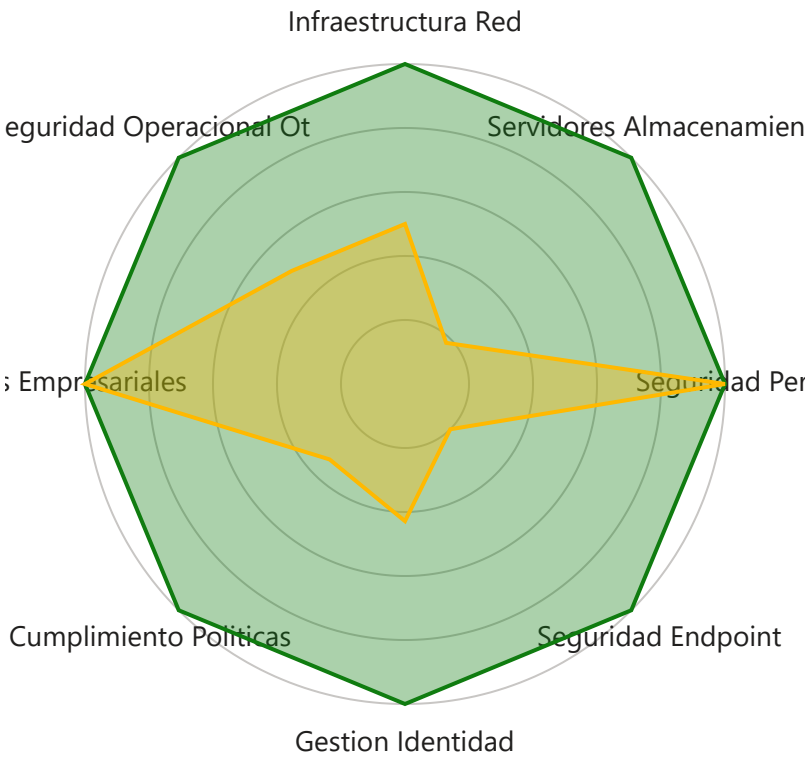
Informe de Evaluación de Madurez de Infraestructura y Seguridad TI

Cliente: z
Fecha: 19 de agosto de 2025
Perfil de Cliente Detectado: PYME

🧠 Resumen Ejecutivo y Nivel de Madurez

Basado en sus respuestas, su organización se alinea con el perfil de **PYME**: Pequeñas y Medianas Empresas (PYMEs) que buscan optimizar sus recursos y mejorar su seguridad con soluciones escalables y rentables.

Su nivel de madurez general es del **45%**. Esto indica que existen áreas críticas que requieren atención inmediata para mitigar riesgos y mejorar la eficiencia.



- Nivel de madurez general: **45%**
- Área más débil: **Seguridad Endpoint**
- Área más fuerte: **Seguridad Perimetral**

💡 Cuadro Resumen de Licenciamiento

A continuación se muestra una comparación directa entre su licenciamiento actual y el recomendado, destacando las funcionalidades clave que ganaría con la optimización.

Funcionalidad	Microsoft 365 E3	
Actual		✓
Recomendado		✓

Funcionalidad	Microsoft 365 E5	
Actual		✗
Recomendado		✓

Funcionalidad	Copilot para Microsoft 365	
Actual		✗
Recomendado		✓

🔍 Filtros del Informe

Mostrar Todo | General | Infraestructura red | Servidores almacenamiento | Seguridad endpoint | Gestion identidad | Cumplimiento politicas | Seguridad operacional ot

Diagnóstico Detallado

El análisis de sus respuestas indica las siguientes observaciones clave y áreas donde se requiere atención para mejorar la madurez de su infraestructura y seguridad TI.

Área de Enfoque	Infraestructura de Red
Observación Específica	Su infraestructura de red se basa en un modelo tradicional On-Premise, lo que puede limitar la flexibilidad y escalabilidad.
Impacto de Negocio	Una infraestructura rígida dificulta la adaptación a nuevas demandas del negocio, puede incrementar los costes de mantenimiento y ralentizar la innovación.

Área de Enfoque	Infraestructura de Red
Observación Específica	La falta de segmentación de red expone a los sistemas críticos a mayores riesgos. Si un dispositivo se ve comprometido, un atacante podría moverse lateralmente por la red sin restricciones.
Impacto de Negocio	Un incidente de seguridad en un área de bajo riesgo (como la red de invitados) podría escalar y afectar a sistemas críticos de producción o administración,

causando interrupciones operativas y pérdida de datos.

Área de Enfoque	**Servidores y Almacenamiento**
Observación Específica	**La baja o nula adopción de virtualización de servidores resulta en un uso ineficiente del hardware, mayores costes de energía y refrigeración, y una gestión más compleja.**
Impacto de Negocio	**El provisionamiento de nuevos servidores es lento y costoso. La falta de flexibilidad dificulta la recuperación ante desastres y la optimización de recursos.**

Área de Enfoque	**Servidores y Almacenamiento**
Observación Específica	**El uso de hardware de servidores obsoleto o la falta de un plan de renovación aumenta el riesgo de fallos de hardware, bajo rendimiento y vulnerabilidades de seguridad no parcheables.**
Impacto de Negocio	**Un fallo de hardware puede causar interrupciones no planificadas y pérdida de datos. El bajo rendimiento afecta la productividad y la experiencia del usuario. Las vulnerabilidades pueden ser explotadas por atacantes.**

Área de Enfoque	**Servidores y Almacenamiento**

Observación Específica	**La estrategia de copias de seguridad es inexistente, manual o no se prueba. No se garantiza la recuperabilidad de los datos en caso de un incidente.**
Impacto de Negocio	**Un ataque de ransomware, un fallo de hardware o un error humano podrían resultar en una pérdida de datos permanente y catastrófica para el negocio.**

Área de Enfoque	**Servidores y Almacenamiento**
Observación Específica	**La ausencia de un Plan de Recuperación de Desastres (DRP) documentado y probado deja a la organización sin una guía clara sobre cómo actuar ante un incidente grave.**
Impacto de Negocio	**En caso de un desastre (incendio, inundación, ciberataque masivo), la falta de un plan resultará en tiempos de inactividad prolongados, toma de decisiones caótica y un impacto financiero y reputacional severo.**

Área de Enfoque	**Seguridad del Endpoint**
Observación Específica	**El uso de un antivirus tradicional o la falta de protección en los endpoints (ordenadores, portátiles) es insuficiente para detectar y responder a las amenazas actuales como el ransomware.**
Impacto de Negocio	**Los endpoints son uno de los principales vectores de ataque. Sin una protección avanzada, la probabilidad de una**

	infección por malware que se propague por la red es muy alta.

Área de Enfoque	**Gestión de Identidad y Acceso**
Observación Específica	La ausencia de Autenticación Multifactor (MFA) para todos los usuarios, especialmente para accesos a sistemas críticos, es una brecha de seguridad grave.
Impacto de Negocio	Las contraseñas son susceptibles de ser robadas o adivinadas. Sin MFA, un atacante con una contraseña válida tiene acceso directo a los sistemas y datos de la empresa.

Área de Enfoque	**Gestión de Identidad y Acceso**
Observación Específica	El acceso a sistemas críticos depende únicamente de usuario y contraseña, lo que representa un riesgo de seguridad muy alto.
Impacto de Negocio	El compromiso de una sola credencial podría dar a un atacante acceso a la información más sensible de la empresa, como datos financieros, de clientes o de propiedad intelectual.

Área de Enfoque	**Políticas y Cumplimiento**
Observación Específica	La falta de políticas de seguridad claras y comunicadas genera inconsistencia en las prácticas de seguridad y dificulta la exigencia de responsabilidades.

Impacto de Negocio	**Sin políticas formales, los empleados pueden no ser conscientes de sus responsabilidades en materia de seguridad, lo que aumenta el riesgo de errores humanos y dificulta el cumplimiento de normativas.**

Área de Enfoque	**Políticas y Cumplimiento**
Observación Específica	**La falta de un programa de concienciación en ciberseguridad para los empleados es una de las mayores debilidades en la defensa de una organización.**
Impacto de Negocio	**Los empleados no capacitados son el eslabón más débil y el objetivo principal de los ataques de phishing y ingeniería social, que pueden conducir al robo de credenciales y a infecciones por ransomware.**

Área de Enfoque	**Políticas y Cumplimiento**
Observación Específica	**La gestión de parches es reactiva o inexistente, lo que deja a los sistemas expuestos a vulnerabilidades conocidas que los atacantes pueden explotar fácilmente.**
Impacto de Negocio	**La mayoría de los ciberataques exitosos explotan vulnerabilidades para las que ya existe un parche. No aplicar actualizaciones de seguridad es una de las principales causas de brechas de seguridad.**

Área de Enfoque	**Seguridad Operacional (OT)**
Observación Específica	**La conexión de sistemas de control industrial (OT) a la red corporativa sin el aislamiento adecuado representa un riesgo de seguridad crítico.**
Impacto de Negocio	**Un ataque de malware en la red de TI podría propagarse a la red de OT, causando la interrupción de la producción, daños a la maquinaria, riesgos para la seguridad de los empleados y un impacto financiero masivo.**

Plan de Acción y Recomendaciones

Evaluar la Adopción de un Modelo Híbrido o Cloud-Native: Recomendamos explorar una estrategia de nube híbrida o migrar cargas de trabajo a la nube para ganar agilidad, optimizar costes y mejorar la continuidad del negocio.

Implementar una Segmentación de Red Robusta (VLANs): Es prioritario crear redes virtuales (VLANs) para aislar el tráfico de sistemas críticos (OT/Producción), servidores (IT), estaciones de trabajo administrativas y la red de invitados. Esto contiene las amenazas y reduce la superficie de ataque.

Acelerar la Adopción de la Virtualización: Recomendamos implementar o expandir el uso de tecnologías de virtualización (como VMware vSphere o Microsoft Hyper-V) para consolidar servidores, mejorar la utilización de recursos, agilizar la recuperación ante desastres y reducir costes operativos.

Establecer un Ciclo de Vida y Plan de Renovación de Hardware: Es fundamental definir un ciclo de vida para el hardware de servidores (típicamente 3-5 años) y crear un plan de renovación proactivo. Priorizar la migración de servicios críticos a hardware moderno y bajo garantía.

Implementar una Estrategia de Backup Robusta (Regla 3-2-1): Recomendamos implementar urgentemente una solución de backup automatizada que siga la regla 3-2-1: 3 copias de los datos, en 2 tipos de medios diferentes, con al menos 1 copia off-site (fuera de la oficina, por ejemplo, en la nube). Las restauraciones deben probarse periódicamente.

Desarrollar y Probar un Plan de Recuperación de Desastres (DRP): Es crítico desarrollar un DRP que detalle los roles, responsabilidades y procedimientos para restaurar los servicios de TI. El plan debe estar accesible fuera de la infraestructura principal y debe ser probado al menos una vez al año mediante simulacros.

Desplegar una Solución de EDR (Endpoint Detection and Response): Sugerimos reemplazar el antivirus tradicional por una solución EDR. El EDR no solo bloquea amenazas conocidas, sino que también monitoriza el comportamiento de los sistemas para detectar y responder a ataques desconocidos o en curso.

Implementar Autenticación Multifactor (MFA) de Forma Universal: Es prioritario habilitar MFA para todos los usuarios y en todas las aplicaciones críticas (correo electrónico, VPN, ERP, etc.). Esto añade una capa de seguridad esencial que protege contra el robo de credenciales.

Proteger el Acceso a Sistemas Críticos con MFA: Se debe implementar de forma inmediata la Autenticación de Dos Factores (2FA/MFA) en todos los sistemas críticos. Confiar únicamente en contraseñas, incluso si son complejas y se cambian con frecuencia, ya no es una práctica segura.

Definir y Comunicar un Conjunto de Políticas de Seguridad: Recomendamos desarrollar un conjunto de políticas de seguridad de la información que cubran áreas como el uso aceptable de los activos, la gestión de contraseñas, el acceso remoto y la respuesta a incidentes. Estas políticas deben ser comunicadas a todo el personal.

Establecer un Programa de Concienciación y Capacitación en Ciberseguridad: Es fundamental implementar un programa de capacitación anual obligatoria para todo el personal sobre cómo identificar amenazas de ciberseguridad. Esto debe complementarse con simulaciones de phishing periódicas para medir la eficacia de la formación.

Implementar un Proceso Formal de Gestión de Parches: Recomendamos establecer un proceso proactivo para la gestión de parches que incluya la identificación de activos, el monitoreo de vulnerabilidades, la prueba de parches en un entorno de no producción y su despliegue controlado en toda la organización.

Aislar y Proteger las Redes de Tecnología Operacional (OT): Es imperativo segmentar la red de OT de la red de TI mediante firewalls y zonas desmilitarizadas (DMZ). El acceso a los sistemas de OT debe ser estrictamente controlado y monitorizado. La seguridad de la tecnología operacional es una prioridad absoluta.

Estimación de Ahorro y Valor Generado

Concepto	Evaluar la Adopción de un Modelo Híbrido o Cloud-Native
Situación Actual	N/A
Acción Propuesta	Recomendamos explorar una estrategia de nube híbrida o migrar cargas de trabajo a la nube para ganar agilidad, optimizar costes y mejorar la continuidad del negocio.
Valor / Ahorro	**Reducción de costes de capital (CapEx)** al disminuir la inversión en hardware. **Optimización de costes operativos (OpEx)** mediante el pago por uso. **Mejora de la agilidad** para responder a las demandas del mercado.

Concepto	Implementar una Segmentación de Red Robusta (VLANs)
Situación Actual	N/A
Acción Propuesta	Es prioritario crear redes virtuales (VLANs) para aislar el tráfico de sistemas críticos (OT/Producción), servidores (IT), estaciones de trabajo administrativas y la red de invitados. Esto contiene las amenazas y reduce la superficie de ataque.
Valor / Ahorro	**Reducción del riesgo de brechas de seguridad**, evitando multas y costes de remediación. **Protección de la propiedad intelectual** y los datos críticos del negocio.

Concepto	Acelerar la Adopción de la Virtualización
Situación Actual	N/A
Acción Propuesta	Recomendamos implementar o expandir el uso de tecnologías de virtualización (como VMware vSphere o Microsoft Hyper-V) para consolidar servidores, mejorar la utilización de recursos, agilizar la recuperación ante desastres y reducir costes operativos.
Valor / Ahorro	**Reducción de costes de hardware** (consolidación de servidores). **Ahorro en energía y refrigeración**. **Disminución del tiempo de inactividad** no planificado.

Concepto	Establecer un Ciclo de Vida y Plan de Renovación de Hardware
Situación Actual	N/A
Acción Propuesta	Es fundamental definir un ciclo de vida para el hardware de servidores (típicamente 3-5 años) y crear un plan de renovación proactivo. Priorizar la migración de servicios críticos a hardware moderno y bajo garantía.
Valor / Ahorro	**Reducción de costes de mantenimiento** de hardware obsoleto. **Mejora del rendimiento y la productividad** de los empleados. **Mitigación de riesgos** de seguridad.

Concepto	Implementar una Estrategia de Backup Robusta (Regla 3-2-1)

Situación Actual	N/A
Acción Propuesta	Recomendamos implementar urgentemente una solución de backup automatizada que siga la regla 3-2-1: 3 copias de los datos, en 2 tipos de medios diferentes, con al menos 1 copia off-site (fuera de la oficina, por ejemplo, en la nube). Las restauraciones deben probarse periódicamente.
Valor / Ahorro	**Garantiza la continuidad del negocio** ante un desastre. **Evita la pérdida de datos críticos** y los costes asociados a su recuperación (si es posible).

Concepto	Desarrollar y Probar un Plan de Recuperación de Desastres (DRP)
Situación Actual	N/A
Acción Propuesta	Es crítico desarrollar un DRP que detalle los roles, responsabilidades y procedimientos para restaurar los servicios de TI. El plan debe estar accesible fuera de la infraestructura principal y debe ser probado al menos una vez al año mediante simulacros.
Valor / Ahorro	**Minimiza el impacto financiero** de un desastre. **Reduce el tiempo de inactividad** y acelera la recuperación. **Cumplimiento de requisitos** normativos y de clientes.

Concepto	Desplegar una Solución de EDR (Endpoint Detection and Response)

Situación Actual	N/A
Acción Propuesta	Sugerimos reemplazar el antivirus tradicional por una solución EDR. El EDR no solo bloquea amenazas conocidas, sino que también monitoriza el comportamiento de los sistemas para detectar y responder a ataques desconocidos o en curso.
Valor / Ahorro	**Detección y respuesta proactiva** a amenazas avanzadas. **Reducción del tiempo de permanencia de los atacantes** en la red. **Protección contra ransomware** y otros ataques destructivos.

Concepto	Implementar Autenticación Multifactor (MFA) de Forma Universal
Situación Actual	N/A
Acción Propuesta	Es prioritario habilitar MFA para todos los usuarios y en todas las aplicaciones críticas (correo electrónico, VPN, ERP, etc.). Esto añade una capa de seguridad esencial que protege contra el robo de credenciales.
Valor / Ahorro	**Reducción drástica del riesgo** de compromiso de credenciales, el vector de ataque más común. **Protección del acceso** a datos sensibles y sistemas críticos.

Concepto	Proteger el Acceso a Sistemas Críticos con MFA
Situación Actual	N/A

Acción Propuesta	Se debe implementar de forma inmediata la Autenticación de Dos Factores (2FA/MFA) en todos los sistemas críticos. Confiar únicamente en contraseñas, incluso si son complejas y se cambian con frecuencia, ya no es una práctica segura.
Valor / Ahorro	**Salvaguarda de los activos más importantes** de la empresa (datos financieros, propiedad intelectual). **Cumplimiento de normativas** que exigen controles de acceso estrictos.

Concepto	Definir y Comunicar un Conjunto de Políticas de Seguridad
Situación Actual	N/A
Acción Propuesta	Recomendamos desarrollar un conjunto de políticas de seguridad de la información que cubran áreas como el uso aceptable de los activos, la gestión de contraseñas, el acceso remoto y la respuesta a incidentes. Estas políticas deben ser comunicadas a todo el personal.
Valor / Ahorro	**Creación de una cultura de seguridad** en la organización. **Reducción del riesgo de errores humanos**. **Demostración de la debida diligencia** en seguridad a clientes y reguladores.

Concepto	Establecer un Programa de Concienciación y Capacitación en Ciberseguridad
Situación Actual	N/A

Acción Propuesta	Es fundamental implementar un programa de capacitación anual obligatoria para todo el personal sobre cómo identificar amenazas de ciberseguridad. Esto debe complementarse con simulaciones de phishing periódicas para medir la eficacia de la formación.
Valor / Ahorro	**Fortalecimiento del eslabón más débil** de la cadena de seguridad. **Reducción de la probabilidad de éxito** de los ataques de phishing y ingeniería social.

Concepto	Implementar un Proceso Formal de Gestión de Parches
Situación Actual	N/A
Acción Propuesta	Recomendamos establecer un proceso proactivo para la gestión de parches que incluya la identificación de activos, el monitoreo de vulnerabilidades, la prueba de parches en un entorno de no producción y su despliegue controlado en toda la organización.
Valor / Ahorro	**Cierre de las puertas de entrada** más comunes para los atacantes. **Reducción de la superficie de ataque** de la organización. **Evita multas** por incumplimiento de normativas.

Concepto	Aislar y Proteger las Redes de Tecnología Operacional (OT)
Situación Actual	N/A

Acción Propuesta	Es imperativo segmentar la red de OT de la red de TI mediante firewalls y zonas desmilitarizadas (DMZ). El acceso a los sistemas de OT debe ser estrictamente controlado y monitorizado. La seguridad de la tecnología operacional es una prioridad absoluta.
Valor / Ahorro	**Protección de la infraestructura crítica** de producción. **Evita paradas de producción** y pérdidas económicas masivas. **Garantiza la seguridad** de los empleados.

📋 Resumen de sus Respuestas

Pregunta	Nombre de la empresa:
Respuesta	z
Valoración	**0 / 0**

Pregunta	Sector de actividad:
Respuesta	agro
Valoración	**0 / 0**

Pregunta	Número de empleados:
Respuesta	25

Valoración	**0 / 0**

Pregunta	¿Cómo gestiona el soporte de TI de su empresa?
Respuesta	Externo
Valoración	**1 / 2**

Pregunta	¿Qué tipo de infraestructura de red utiliza principalmente?
Respuesta	On-Premise
Valoración	**0 / 2**

Pregunta	¿Cómo se gestiona su red?
Respuesta	Proveedor de servicios gestionados (MSP)
Valoración	**2 / 2**

Pregunta	¿Monitoriza el rendimiento y la disponibilidad de su red?
Respuesta	Sí, de forma reactiva (cuando hay problemas)
Valoración	**1 / 2**

Pregunta	¿Cómo está segmentada la red de la empresa para mejorar la seguridad?
Respuesta	Existen redes separadas para invitados y para la empresa, pero los equipos de producción y administrativos comparten la misma red.
Valoración	**1 / 2**

Pregunta	¿Utiliza tecnologías de virtualización para sus servidores?
Respuesta	Sí, parcialmente
Valoración	**1 / 2**

Pregunta	¿Tiene una solución de backup y recuperación de desastres (DR)?
Respuesta	Sí, pero no se prueba
Valoración	**1 / 2**

Pregunta	¿Utiliza almacenamiento en la nube (ej. Azure Files, AWS S3)?
Respuesta	No
Valoración	**0 / 1**

Pregunta	En cuanto al hardware de servidores de la empresa, ¿cuál de las siguientes situaciones representa un mayor nivel de madurez?
Respuesta	La mayoría de los servidores son físicos y tienen más de 7 años de antigüedad.
Valoración	**0 / 2**

Pregunta	¿Cuál es la práctica de la empresa con respecto a las copias de seguridad (backups) de los datos críticos?
Respuesta	Se realiza una copia de seguridad semanal en un disco duro externo que se guarda en la misma oficina.
Valoración	**0 / 2**

Pregunta	¿Existe un plan de recuperación de desastres (DRP) documentado y probado?
Respuesta	No existe un plan formal. Se improvisaría en caso de un desastre.
Valoración	**0 / 2**

Pregunta	¿Cuenta con un firewall de nueva generación (NGFW)?
Respuesta	Sí

Valoración	**2 / 2**

Pregunta	¿Cómo gestiona el acceso remoto a la red corporativa?
Respuesta	Zero Trust Network Access (ZTNA)
Valoración	**2 / 2**

Pregunta	¿Tiene protección contra ataques de denegación de servicio (DDoS)?
Respuesta	Sí
Valoración	**1 / 1**

Pregunta	¿Qué tipo de protección de endpoints utiliza?
Respuesta	Antivirus tradicional
Valoración	**1 / 2**

Pregunta	¿Gestiona de forma centralizada los dispositivos de los usuarios (MDM/UEM)?
Respuesta	No
Valoración	**0 / 2**

Pregunta	¿Están los discos duros de los portátiles de la empresa cifrados?
Respuesta	No
Valoración	**0 / 1**

Pregunta	¿Utiliza un servicio de directorio centralizado?
Respuesta	Active Directory On-Premise
Valoración	**1 / 2**

Pregunta	¿Ha implementado la autenticación multifactor (MFA) para los usuarios?
Respuesta	No
Valoración	**0 / 2**

Pregunta	¿Tiene una estrategia para la gestión de accesos con privilegios (PAM)?
Respuesta	Sí
Valoración	**1 / 1**

Pregunta	¿Cómo se protege el acceso a sistemas críticos como el correo electrónico o el sistema de gestión (ERP)?

Respuesta	Se obliga a los usuarios a cambiar sus contraseñas complejas cada 30 días.
Valoración	**1 / 2**

Pregunta	¿Tiene políticas de seguridad de la información definidas y comunicadas?
Respuesta	Sí
Valoración	**2 / 2**

Pregunta	¿Realiza auditorías de seguridad o pruebas de penetración periódicamente?
Respuesta	No
Valoración	**0 / 2**

Pregunta	¿Cumple su infraestructura con normativas como el RGPD u otras específicas de su sector?
Respuesta	Sí
Valoración	**1 / 1**

Pregunta	¿Con qué frecuencia recibe el personal capacitación sobre ciberseguridad (por ejemplo, cómo identificar correos de phishing)?

Respuesta	Se envió un correo electrónico con recomendaciones de seguridad una vez, hace varios años.
Valoración	**0 / 2**

Pregunta	¿Cómo se gestionan las actualizaciones de seguridad para los sistemas operativos y el software (parches)?
Respuesta	Solo se actualizan los computadores cuando un usuario reporta un problema.
Valoración	**0 / 2**

Pregunta	Para la gestión de procesos clave como inventario, producción y finanzas, ¿qué sistema utiliza la empresa?
Respuesta	Un sistema ERP (Planificación de Recursos Empresariales) integrado que centraliza la información de todos los departamentos.
Valoración	**2 / 2**

Pregunta	En cuanto a la trazabilidad de los productos, ¿qué tecnología se utiliza?
Respuesta	Un sistema de gestión de almacenes (WMS) integrado con el ERP, que utiliza códigos de barras o QR para rastrear cada lote desde la recepción de materia prima hasta el despacho.

Valoración	**2 / 2**

Pregunta	En el área de producción, ¿cómo se gestiona la tecnología de control de procesos (sistemas SCADA, PLCs)?
Respuesta	Los equipos de producción no están conectados a ninguna red.
Valoración	**1 / 2**

📊 Metodología de Evaluación y Criterios de Madurez

Cómo se Calcula su Nivel de Madurez

La evaluación se basa en un sistema de puntuación por áreas clave de su infraestructura y seguridad TI. Cada pregunta contribuye a la puntuación de un área específica, y las respuestas de mayor madurez suman más puntos.

Puntuación por Área:

- **Infraestructura Red:** 4 / 8 puntos.
- **Servidores Almacenamiento:** 2 / 11 puntos.
- **Seguridad Perimetral:** 5 / 5 puntos. **Aprobado**
- **Seguridad Endpoint:** 1 / 5 puntos.
- **Gestion Identidad:** 3 / 7 puntos.
- **Cumplimiento Politicas:** 3 / 9 puntos.
- **Sistemas Empresariales:** 4 / 4 puntos. **Aprobado**
- **Seguridad Operacional Ot:** 1 / 2 puntos.

Niveles de Madurez:

- **Inicial (0-49%):** Procesos de TI reactivos, falta de controles de seguridad básicos y alta exposición a riesgos.

- **En Desarrollo (50-79%):** Procesos de TI definidos pero no integrados, controles de seguridad implementados pero no optimizados.
- **Optimizado (80-100%):** Procesos de TI proactivos y optimizados, controles de seguridad avanzados y una fuerte postura de seguridad.

Umbrales de Diagnóstico y Recomendaciones:

Se generan diagnósticos y recomendaciones específicas cuando la puntuación de un área cae por debajo de ciertos umbrales, indicando oportunidades de mejora:

- **Advertencia (Amarillo):** Indica áreas con configuración básica o reactiva, con riesgo potencial.
- **Peligro (Rojo):** Señala brechas críticas o falta de implementación de prácticas esenciales, con alto riesgo.

Si un área no muestra diagnósticos específicos, significa que su nivel de madurez en esa área es alto y cumple con las mejores prácticas. **Aprobado**

📎 Próximos Pasos Sugeridos

Basado en el diagnóstico, le recomendamos las siguientes acciones para mejorar la madurez de su infraestructura y seguridad.

> **Evaluar la Adopción de un Modelo Híbrido o Cloud-Native:** Recomendamos explorar una estrategia de nube híbrida o migrar cargas de trabajo a la nube para ganar agilidad, optimizar costes y mejorar la continuidad del negocio.

> **Implementar una Segmentación de Red Robusta (VLANs):** Es prioritario crear redes virtuales (VLANs) para aislar el tráfico de sistemas críticos (OT/Producción), servidores (IT), estaciones de trabajo administrativas y la red de invitados. Esto contiene las amenazas y reduce la superficie de ataque.

> **Acelerar la Adopción de la Virtualización:** Recomendamos implementar o expandir el uso de tecnologías de virtualización (como VMware vSphere o Microsoft Hyper-V) para consolidar servidores, mejorar la utilización de recursos, agilizar la recuperación ante desastres y reducir costes operativos.

Establecer un Ciclo de Vida y Plan de Renovación de Hardware: Es fundamental definir un ciclo de vida para el hardware de servidores (típicamente 3-5 años) y crear un plan de renovación proactivo. Priorizar la migración de servicios críticos a hardware moderno y bajo garantía.

Implementar una Estrategia de Backup Robusta (Regla 3-2-1): Recomendamos implementar urgentemente una solución de backup automatizada que siga la regla 3-2-1: 3 copias de los datos, en 2 tipos de medios diferentes, con al menos 1 copia off-site (fuera de la oficina, por ejemplo, en la nube). Las restauraciones deben probarse periódicamente.

Desarrollar y Probar un Plan de Recuperación de Desastres (DRP): Es crítico desarrollar un DRP que detalle los roles, responsabilidades y procedimientos para restaurar los servicios de TI. El plan debe estar accesible fuera de la infraestructura principal y debe ser probado al menos una vez al año mediante simulacros.

Desplegar una Solución de EDR (Endpoint Detection and Response): Sugerimos reemplazar el antivirus tradicional por una solución EDR. El EDR no solo bloquea amenazas conocidas, sino que también monitoriza el comportamiento de los sistemas para detectar y responder a ataques desconocidos o en curso.

Implementar Autenticación Multifactor (MFA) de Forma Universal: Es prioritario habilitar MFA para todos los usuarios y en todas las aplicaciones críticas (correo electrónico, VPN, ERP, etc.). Esto añade una capa de seguridad esencial que protege contra el robo de credenciales.

Proteger el Acceso a Sistemas Críticos con MFA: Se debe implementar de forma inmediata la Autenticación de Dos Factores (2FA/MFA) en todos los sistemas críticos. Confiar únicamente en contraseñas, incluso si son complejas y se cambian con frecuencia, ya no es una práctica segura.

Definir y Comunicar un Conjunto de Políticas de Seguridad: Recomendamos desarrollar un conjunto de políticas de seguridad de la información que cubran áreas como el uso aceptable de los activos, la gestión de contraseñas, el acceso remoto y la respuesta a incidentes. Estas políticas deben ser comunicadas a todo el personal.

Establecer un Programa de Concienciación y Capacitación en Ciberseguridad: Es fundamental implementar un programa de capacitación anual obligatoria para todo el personal sobre cómo identificar amenazas de ciberseguridad. Esto debe complementarse con simulaciones de phishing periódicas para medir la eficacia de la formación.

Implementar un Proceso Formal de Gestión de Parches: Recomendamos establecer un proceso proactivo para la gestión de parches que incluya la identificación de activos, el monitoreo de vulnerabilidades, la prueba de parches en un entorno de no producción y su despliegue controlado en toda la organización.

Aislar y Proteger las Redes de Tecnología Operacional (OT): Es imperativo segmentar la red de OT de la red de TI mediante firewalls y zonas desmilitarizadas (DMZ). El acceso a los sistemas de OT debe ser estrictamente controlado y monitorizado. La seguridad de la tecnología operacional es una prioridad absoluta.

Sesión de Seguimiento: Proponemos una reunión para discutir este informe en detalle y definir un plan de trabajo conjunto.

Imprimir o Guardar como PDF | Modificar Respuestas

Limpiar y Empezar de Nuevo

Implementación: Francisco Cedillo