Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 14/01/2026 | Aceptado: 17/01/2026 | Publicación: 20/01/2026

Resiliencia tecnológica en pequeñas y medianas empresas: continuidad operativa, copias de seguridad y recuperación de entornos informáticos.
Resiliencia tecnológica en pequeñas y medianas empresas: continuidad del negocio, copias de seguridad y TI.
Recuperación ambiental
Resiliencia tecnológica en pequeñas y medianas empresas: continuidad del negocio, copias de seguridad y recuperación del entorno informático.

Guilherme Gallo Zazeri

Profesional de las Tecnologías de la Información, consultor y emprendedor en infraestructura, conectividad y soluciones tecnológicas, con más de 25 años de experiencia profesional.

Resumen

La creciente dependencia de servidores, servicios en la nube, redes y aplicaciones ha convertido la continuidad tecnológica en una condición indispensable para el funcionamiento de las pequeñas y medianas empresas (PYME). Este artículo analiza la resiliencia de TI mediante la identificación de activos críticos, el análisis de impacto, las estrategias de respaldo, las pruebas de restauración, la documentación y el monitoreo. La investigación adopta una revisión narrativa estructurada de estándares institucionales verificables, guías técnicas, libros e informes, destacando NIST CSF 2.0, NIST SP 800-34 Rev. 1, ISO 22301 y Verizon DBIR. El análisis demuestra que poseer copias de datos no equivale a poseer capacidad de recuperación: la continuidad depende de prioridades y responsabilidades definidas, copias protegidas, pruebas periódicas y procedimientos ejecutables. Para las PYME, el principal desafío es establecer controles proporcionales al riesgo y la capacidad operativa, evitando tanto la falta de planificación como arquitecturas excesivamente complejas.

Palabras clave: resiliencia tecnológica; continuidad del negocio; copias de seguridad; recuperación ante desastres; pequeñas y medianas empresas; infraestructura de TI.

Abstracto

La creciente dependencia de servidores, servicios en la nube, redes y aplicaciones ha convertido la continuidad tecnológica en una condición operativa fundamental para las pequeñas y medianas empresas (PYME). Este artículo analiza la resiliencia de TI mediante la identificación de activos críticos, el análisis del impacto en el negocio, las estrategias de respaldo, las pruebas de restauración, la documentación y el monitoreo. El estudio adopta una revisión narrativa estructurada de estándares verificables, guías técnicas, libros e informes institucionales, con especial énfasis en NIST CSF 2.0, NIST SP 800-34 Rev. 1, ISO 22301 y el DBIR de Verizon. El análisis demuestra que poseer copias de datos no equivale a poseer capacidad de recuperación: la continuidad depende de prioridades definidas, responsabilidades, copias protegidas, pruebas periódicas y procedimientos ejecutables. Para las PYME, el principal desafío es establecer controles proporcionales al riesgo y la capacidad operativa, evitando tanto la falta de planificación como arquitecturas innecesariamente complejas.

Palabras clave: resiliencia tecnológica; continuidad del negocio; copias de seguridad; recuperación ante desastres; pequeñas y medianas empresas; infraestructura de TI.

Introducción

La infraestructura tecnológica ha dejado de ser simplemente un soporte administrativo y se ha convertido en parte de...

Las operaciones diarias de las empresas en prácticamente todos los sectores. Sistemas de gestión, archivo,

El correo electrónico, la comunicación, el acceso remoto y los servicios en la nube forman cadenas de dependencias en las que

Una falla técnica puede interrumpir las ventas, el servicio al cliente, la facturación o la producción. Whitman y

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 14/01/2026 | Aceptado: 17/01/2026 | Publicación: 20/01/2026

Mattord (2021) observa que la seguridad de la información debe abordarse en relación con la
objetivos organizativos, y no como una actividad aislada del área técnica.
En las pequeñas y medianas empresas, esta dependencia suele ir acompañada de equipos reducidos.
y entornos heterogéneos. El NIST publicó una guía específica para pequeñas empresas en 2024.
basado en el Marco de Ciberseguridad 2.0, reconociendo que las organizaciones con recursos modestos
También necesitan estructurar la gobernanza, la identificación, la protección, la detección, la respuesta y la recuperación.
(ELIOT, 2024). Por lo tanto, la cuestión no es reproducir la arquitectura de una gran corporación, sino
Establecer prioridades que sean compatibles con el riesgo.
La continuidad operativa es una de estas prioridades. Swanson et al. (2010), en NIST SP
800-34 Rev. 1, relacionar el análisis de impacto, los controles preventivos, las estrategias de recuperación,
Probar y mantener un programa de contingencia consistente. Partiendo de esta base, este artículo...
Este estudio examina seis dimensiones de la resiliencia tecnológica en las PYMES, con especial atención a la capacidad real.
para restablecer los servicios después de fallas, incidentes o interrupciones.

2. Metodología

El estudio utiliza una revisión narrativa estructurada, adecuada para integrar normas técnicas y bibliografía.
Seguridad de la información, continuidad del negocio y evidencia institucional reciente. Fueron...
Se da prioridad a las fuentes con autoría identificable, institución responsable, editorial y contenido.
El núcleo normativo está formado por el Marco de Ciberseguridad 2.0 del NIST, por la norma NIST SP 1300 destinada a...
a las pequeñas empresas, según NIST SP 800-34 Rev. 1 e ISO 22301:2019. Estas referencias
Nos permiten distinguir entre gestión de riesgos, continuidad organizativa y recuperación de sistemas.
La literatura de Whitman y Mattord (2021) y Stallings (2018) se utilizó para contextualizar
Seguridad, gobernanza y controles. Se utilizó el Informe de Investigaciones de Violaciones de Datos de Verizon de 2025.
como fuente empírica contemporánea sobre incidentes y violaciones.
La selección no se basó en marcas comerciales de hardware, hipervisores o servicios en la nube.
El objetivo era preservar la aplicabilidad en diferentes entornos tecnológicos y evitar recomendaciones.
Las preferencias arquitectónicas debían confundirse con las preferencias del proveedor.
Los materiales se organizaron en seis áreas: criticidad, análisis de impacto, copia de seguridad, recuperación,
documentación y seguimiento. En cada área, el objetivo era diferenciar entre la existencia de recursos técnicos y
Capacidad operativa comprobada.
El artículo no propone certificación, auditoría ni un modelo universal para la continuidad del negocio. Las recomendaciones
Deben adaptarse al tamaño, al sector, a los requisitos normativos, al presupuesto y a la tolerancia al tiempo de inactividad.
y la importancia crítica de los datos de cada organización.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 14/01/2026 | Aceptado: 17/01/2026 | Publicación: 20/01/2026

3.1 Dependencia tecnológica y criticidad de los activos

Una estrategia de resiliencia comienza por identificar qué es lo que realmente sostiene la operación.
NIST CSF 2.0 (PASCOE; QUINN; SCARFONE, 2024) incluye la función Identificar precisamente porque
Las organizaciones necesitan comprender sus activos, dependencias y riesgos antes de seleccionar los controles.
Los inventarios técnicos ganan valor cuando se vinculan a los procesos de negocio. Un servidor puede
Puede parecer simplemente un equipo, pero puede albergar autenticación, archivos o una aplicación indispensable para...
ingresos. La criticidad debe definirse por el impacto del tiempo de inactividad, no por el precio de
activo.

Swanson et al. (2010) relacionan el análisis de impacto empresarial con la determinación de prioridades para
Recuperación. El análisis ayuda a identificar qué sistemas dan soporte a las funciones esenciales y qué se está perdiendo.
La disponibilidad puede ser tolerada.
En las PYMES, las dependencias ocultas son comunes: credenciales en poder de una sola persona,
Equipos sin documentación o aplicaciones heredadas cuya integración se desconoce.
La documentación técnica reduce este riesgo al transformar el conocimiento tácito en información.
organizativo.
La clasificación también evita el desperdicio. No todos los servicios requieren el mismo nivel de...
redundancia o el mismo período de recuperación. Stallings (2018) destaca que los controles deben ser
La selección se basa en el riesgo, lo que permite concentrar los recursos en los componentes más relevantes.
Por lo tanto, mapear la criticidad es una decisión de gestión. La infraestructura deja de ser una colección de
dispositivos y llega a entenderse como un conjunto de dependencias que sustentan resultados.
negocio.

3.2 Análisis de impacto, RTO y RPO

La planificación de la recuperación debe responder a dos preguntas: ¿cuánto tiempo podrá la organización...
Puede soportar estar sin un servicio en particular y la cantidad de datos que se pueden perder. Swanson et al. (2010) relacionan
Estas decisiones están vinculadas al análisis de impacto y a los objetivos de recuperación.
El objetivo de tiempo de recuperación representa el período previsto para restaurar una función o un sistema.
El objetivo de punto de recuperación indica la cantidad de datos, medida a lo largo del tiempo, que la organización acepta.
perder. Si bien los conceptos son técnicos, su definición depende de las decisiones empresariales.
Un RTO muy corto puede requerir redundancia, automatización e infraestructura adicional. Un RPO
Una respuesta cercana a cero puede requerir replicación frecuente o continua. Por lo tanto, los objetivos de recuperación
Deben ser compatibles en cuanto a impacto y presupuesto.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 14/01/2026 | Aceptado: 17/01/2026 | Publicación: 20/01/2026

La norma ISO 22301 (2019) refuerza que la continuidad debe estructurarse en torno a las necesidades de
La organización y su capacidad de respuesta ante las interrupciones. Esto impide la toma de decisiones.
Decisiones tomadas basándose únicamente en la conveniencia técnica.
También es importante considerar las dependencias entre sistemas. Restaurar una aplicación sin base de datos.
Los problemas de datos, autenticación o conectividad pueden impedir que la operación se devuelva al usuario. La secuencia de
La recuperación debe reflejar estas relaciones.
Por lo tanto, RTO y RPO funcionan como un puente entre la gestión y la tecnología. Cuando se definen de una manera...
Las directrices realistas ofrecen orientación sobre copias de seguridad, redundancia, contratos, pruebas y prioridades de inversión.

3.3 La copia de seguridad no es sinónimo de recuperación.

Las copias de seguridad son un componente de la recuperación, pero su mera existencia no garantiza la continuidad.
NIST SP 800-34 Rev. 1 establece que los procesos de respaldo efectivos son cruciales para la estrategia de
recuperación y relaciona su frecuencia con las necesidades identificadas en el análisis de impacto.
(SWANSON et al., 2010).
Una copia de seguridad puede fallar debido a corrupción, configuración incorrecta, credenciales comprometidas o problemas de retención.
Insuficiente. Por lo tanto, la gestión de copias de seguridad debe tener en cuenta la cobertura, la frecuencia, la integridad y la protección.
y capacidad de recuperación.
Whitman y Mattord (2021) consideran la disponibilidad como una dimensión central de la seguridad.
Información. Esta perspectiva muestra que proteger los datos incluye garantizar que puedan recuperarse.
cuando sea necesario.
La separación lógica o física de las copias reduce la posibilidad de que un único incidente comprometa el sistema.
Producción y respaldo simultáneos. El diseño adecuado depende del entorno, pero el principio es...
Evite los puntos únicos de fallo.
Las políticas de retención también deben tener en cuenta las versiones. Una eliminación o modificación accidental...
La actividad maliciosa puede detectarse días después; si todas las copias ya reflejan el estado comprometido,
Las copias de seguridad pierden parte de su utilidad.
Por lo tanto, la pregunta relevante no es solo si existen copias de seguridad, sino si la organización sabe qué es lo que está respaldando.
Está protegido; ¿cuánto tiempo podrá regresar y cuánto tiempo le llevaría hacerlo?

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 14/01/2026 | Aceptado: 17/01/2026 | Publicación: 20/01/2026

3.4 Pruebas de restauración y capacidad comprobada

La recuperación de las pruebas transforma una expectativa en evidencia. Swanson et al. (2010) incluyen pruebas,
La capacitación y los ejercicios se incluyen entre las etapas de la planificación de contingencias, precisamente porque los planes
Las declaraciones no ejecutadas pueden contener premisas incorrectas.
Una prueba de restauración puede revelar archivos incompletos, dependencias olvidadas y contraseñas.
Recursos no disponibles o cronogramas incompatibles con el objetivo definido. Estos problemas son menos costosos.
cuando se encuentra antes de una emergencia.
La frecuencia debe reflejar la criticidad y el ritmo del cambio. Los sistemas se modifican con frecuencia.
Pueden requerir validaciones más frecuentes. Los entornos estables aún necesitan pruebas, porque
El hardware, el software, las credenciales y las personas cambian con el tiempo.
Los ejercicios también evalúan la comunicación. La recuperación implica decidir quién autoriza, quién
Implica quién ejecuta, quién valida y quién informa a los usuarios o clientes. La norma ISO 22301 (2019) aborda la preparación.
continuidad organizativa, no solo restauración técnica.
Es necesario registrar los resultados de la prueba. Esto incluye el tiempo de observación, los errores detectados y las medidas correctivas adoptadas.
Los responsables se encargan de supervisar el progreso y demostrar que el plan se está cumpliendo.
Por lo tanto, la capacidad de recuperación se expresa mejor mediante la evidencia de las pruebas que mediante...
El número de herramientas instaladas. La resiliencia es una propiedad operativa comprobada, no...
una promesa.

3.5 Documentación y reducción de la dependencia del conocimiento individual

Los entornos de TI acumulan conocimiento informal: direcciones, credenciales, reglas de firewall,
topologías, rutinas y excepciones. Cuando esta información se concentra en una persona,
El propio equipo se convierte en un único punto de fallo.
El Marco de Ciberseguridad 2.0 del NIST (2024) amplía el énfasis en la gobernanza y la comunicación de responsabilidades.
Documentar los activos, los procedimientos y las decisiones ayuda a la organización a mantener...
Se mantienen los controles incluso ante cambios de personal.
La documentación útil no necesita ser extensa. Inventarios actualizados, diagramas de red, listas de...
dependencias, contactos, procedimientos de recuperación y ubicación segura de credenciales pueden
para generar mayor valor que los manuales extensos y obsoletos.
El control de versiones es igualmente importante. Un diagrama obsoleto puede llevar a decisiones erróneas.
Durante un incidente, la documentación debe formar parte del proceso de cambio, no ser simplemente una actualización.
solo cuando se produce una auditoría o un fallo.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS – Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 14/01/2026 | Aceptado: 17/01/2026 | Publicación: 20/01/2026

Stallings (2018) vincula las políticas y los procedimientos con la ejecución consistente de la seguridad. En
Siguiendo con el mismo proceso, la documentación cumple una función similar: permite repetir acciones críticas.
De forma predecible.
Reducir la dependencia individual también facilita la formación y la transferencia de conocimientos.
En este sentido, la resiliencia tecnológica incluye la capacidad de preservar el conocimiento operativo.
además de las personas que originalmente crearon el entorno.

3.6 Ciclo de seguimiento, prevención y resiliencia

La monitorización permite identificar las degradaciones antes de que provoquen tiempos de inactividad.
percibido por el usuario. Capacidad de almacenamiento, fallas del servicio, pérdida de conectividad y
Los errores de copia de seguridad son ejemplos de señales que se pueden monitorizar.
El marco CSF 2.0 del NIST organiza la gestión de riesgos en las fases de Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar.
Esta estructura demuestra que la recuperación no es un paso aislado: depende de la gobernanza y del conocimiento.
del medio ambiente, protección, detección y respuesta coordinada.
Para las PYMES, el valor del monitoreo radica en la priorización. Las alertas excesivas producen ruido;
Pocas advertencias logran ocultar los fallos. La criticidad y el impacto deben guiar la identificación de los eventos que requieren atención.
acción inmediata.
El informe DBIR 2025 de Verizon analizó más de 22.000 incidentes y 12.195 violaciones confirmadas, registrando
Mayor explotación de vulnerabilidades y participación de terceros. Este escenario refuerza la
La necesidad de combinar disponibilidad y seguridad dentro de una misma disciplina operativa.
La monitorización también debe extenderse al propio mecanismo de protección. Una rutina de respaldo.
Si no se ejecuta, debería generarse una alerta; de lo contrario, el fallo podría permanecer invisible hasta que...
período de recuperación.
La resiliencia, por lo tanto, es cíclica. Las organizaciones identifican riesgos, protegen activos, detectan desviaciones,
Responden, se recuperan e incorporan las lecciones aprendidas en el diseño posterior del entorno.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google
RCMOS - Revista Científica Multidisciplinaria El Conocimiento.
ISSN: 2675-9128. São Paulo-SP.

Año VII, vol. 2, 2026 | Envío: 14/01/2026 | Aceptado: 17/01/2026 | Publicación: 20/01/2026

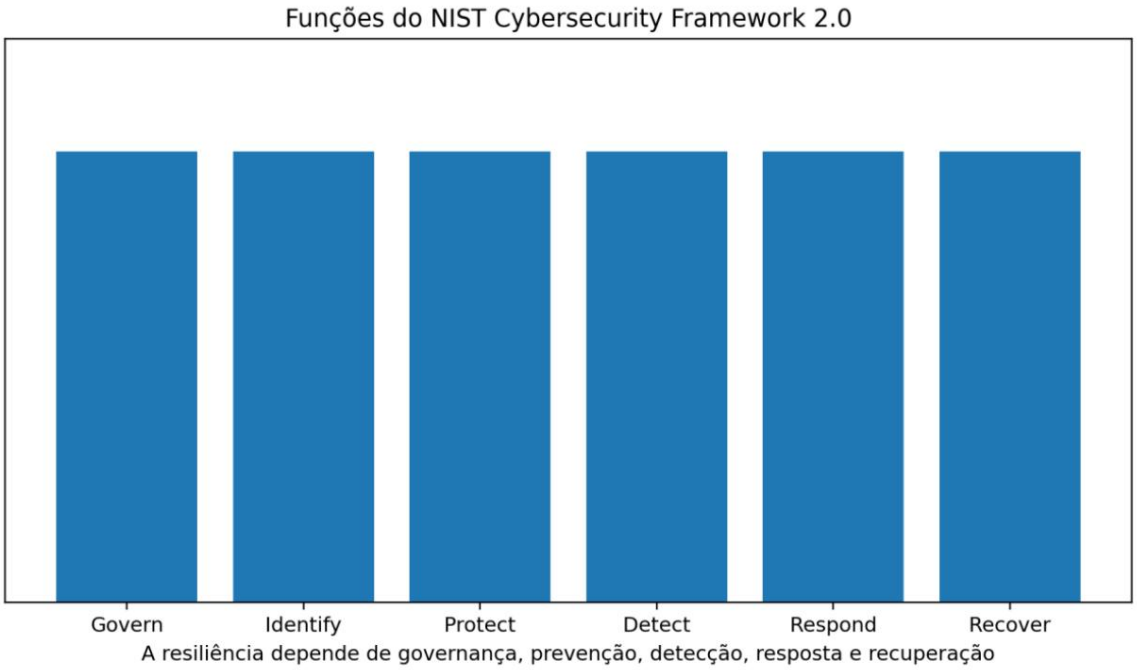

Figura 1. Las seis funciones del Marco de Ciberseguridad 2.0 del NIST. Fuente: elaboración propia del autor. basado en Pascoe, Quinn y Scarfone (2024).

3.7 Costo del tiempo de inactividad y proporcionalidad de la inversión

El debate sobre la resiliencia también tiene una dimensión económica. Inversiones en respaldo, La redundancia y la seguridad compiten con otras prioridades, especialmente en las empresas más pequeñas. Por lo tanto, el análisis no debe partir de la idea de protección absoluta, sino de una comparación de impactos. potencial, probabilidad y costo del control. El NIST CSF 2.0 (PASCOE; QUINN; SCARFONE, 2024) fue diseñado precisamente para permitir a las organizaciones priorizar los resultados de seguridad. dependiendo del contexto y del riesgo.

El costo de una interrupción no se limita a la sustitución de equipos. Horas improductivas, incapacidad para facturar, retrasos en la entrega, recuperación de datos, contratación de emergencia de La falta de experiencia y la pérdida de confianza pueden amplificar el impacto financiero. Whitman y Mattord (2021) Vinculan la seguridad de la información con la continuidad de las funciones organizativas, lo que refuerza la Es necesario considerar los impactos indirectos.

En 2025, una investigación internacional publicada por Mastercard con más de cinco mil propietarios de Las pequeñas y medianas empresas de cuatro continentes informaron que el 46% había sufrido un ataque. La ciberseguridad afecta a su actividad empresarial actual. Entre los afectados, casi uno de cada cinco declaró haber... Posteriormente, la empresa se declaró en bancarrota o cerró sus puertas. Los datos no permiten establecer una relación de causalidad.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 14/01/2026 | Aceptado: 17/01/2026 | Publicación: 20/01/2026

Es económicamente uniforme, pero demuestra la gravedad potencial de los incidentes para las organizaciones con menor capacidad de absorción.

La misma publicación de Mastercard cita una estimación de 2024 según la cual el costo promedio de un Un ciberataque dirigido a empresas con entre 25 y 299 empleados alcanzó los 250.000 dólares estadounidenses. Valores de este La naturaleza no debe trasplantarse automáticamente a ninguna empresa, debido al sector, el tamaño, etc. El tipo de incidente altera el impacto. Sin embargo, sirven para demostrar por qué la continuidad y Las cuestiones de seguridad también deben evaluarse como decisiones financieras.

La proporcionalidad en la inversión exige distinguir entre los controles esenciales y las soluciones deseables. Una PYME puede obtener beneficios significativos con un inventario fiable, una autenticación adecuada y copias. Protegido, sometido a pruebas de restauración, con actualizaciones del sistema y documentación antes de adoptar las arquitecturas. de alta complejidad. Eliot (2024) refuerza este enfoque al dirigir la guía del NIST a organizaciones con planes modestos o inexistentes.

Por lo tanto, la resiliencia tecnológica debe incluirse en la planificación empresarial como una herramienta de gestión. Exposición. El objetivo económico no es eliminar todo riesgo, sino prevenir un fallo previsible. producir un impacto desproporcionado en la capacidad financiera y operativa de la organización.

Conclusión

La continuidad tecnológica en las pequeñas y medianas empresas depende menos de la cantidad de Herramientas y más sobre la coherencia entre riesgo, prioridad y capacidad de recuperación. Mapeo Gestionar los activos críticos le permite comprender qué dependencias sustentan las operaciones y evita Inversiones distribuidas sin criterios. El análisis de impacto transforma la indisponibilidad en... Parámetros de decisión. El RTO y el RPO ayudan a alinear las expectativas del negocio con el diseño técnico. Las copias de seguridad son indispensables, pero no deben confundirse con la recuperación. Integridad, retención, Es necesario verificar la protección y la cobertura. Las pruebas de restauración proporcionan la evidencia más sólida. Pruebas concretas de que un plan puede funcionar. También revelan dependencias y plazos que no son visibles. La documentación reduce el riesgo de concentración de conocimientos y facilita la continuidad. Ante cambios en el personal, los proveedores o la infraestructura, el monitoreo conecta la prevención y... respuesta, permitiendo detectar fallas antes de que produzcan un mayor impacto y que Se deben monitorear los mecanismos de protección. Se concluye que la resiliencia tecnológica es una La capacidad organizativa se desarrolla de forma continua. Para las PYMES, soluciones proporcionales. Las arquitecturas documentadas y probadas pueden ofrecer mayor valor que las arquitecturas complejas que no lo están. Se pueden manipular o reparar de forma segura.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.

Machine Translated by Google

Año VII, vol. 2, 2026 | Envío: 14/01/2026 | Aceptado: 17/01/2026 | Publicación: 20/01/2026

Referencias

PASCOE, Cherilyn; QUINN, Stephen; SCARFONE, Karen. El Marco de Ciberseguridad (CSF) 2.0 del NIST. NIST CSWP 29. Gaithersburg: Instituto Nacional de Estándares y Tecnología, 2024.

ELIOT, Daniel. Marco de Ciberseguridad 2.0 del NIST: Guía de inicio rápido para pequeñas empresas. NIST SP 1300. Gaithersburg: Instituto Nacional de Estándares y Tecnología, 2024.

SWANSON, Marianne M.; BOWEN, Pauline; PHILLIPS, Amy W.; GALLUP, Dean; LYNES, David. Guía de planificación de contingencias para sistemas de información federales. NIST SP 800-34 Rev. 1. Gaithersburg: Instituto Nacional de Estándares y Tecnología, 2010.

INSTITUTO NACIONAL DE ESTÁNDARES Y TECNOLOGÍA (NIST). Controles de seguridad y privacidad para sistemas y organizaciones de información. NIST SP 800-53 Rev. 5. Gaithersburg, 2020.

ISO. ISO 22301:2019 Seguridad y resiliencia — Sistemas de gestión de la continuidad del negocio — Requisitos. Ginebra: Organización Internacional de Normalización, 2019.

VERIZON. Informe de investigaciones de filtraciones de datos de 2025. Basking Ridge, 2025.

STALLINGS, William. Ciberseguridad eficaz: una guía para el uso de las mejores prácticas y estándares. Boston: Addison-Wesley, 2018.

WHITMAN, Michael E.; MATTORD, Herbert J. Principios de seguridad de la información. 7.ª ed. Boston: Cengage, 2021.

MASTERCARD. Un experto en pequeñas empresas responde a sus preguntas más urgentes. 2025.

Este artículo se publica en acceso abierto bajo la licencia Creative Commons Attribution, que permite el uso, la distribución y la reproducción sin restricciones en cualquier medio, siempre que se cite correctamente la obra original.