Machine Translated by Google

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

Año IV, vol. 2, 2023 | Envío: 14/12/2023 | Aceptado: 17/12/2023 | Publicación: 20/12/2023

Continuidad del negocio y recuperación ante desastres: estrategias resilientes para Entornos de misión crítica

Continuidad del negocio y recuperación ante desastres: estrategias resilientes para entornos de misión crítica.
Continuidad del negocio y recuperación ante desastres: estrategias resilientes para entornos de misión crítica

Ricardo Saddi Becker es

licenciado en Informática por la Universidad Federal de Mato Grosso (2009).
Especialista certificado en continuidad del negocio por DRII

RESUMEN

La creciente dependencia de las organizaciones de las infraestructuras digitales ha elevado la continuidad operativa a la categoría de elemento estratégico para la sostenibilidad empresarial. En entornos críticos, las interrupciones del sistema pueden comprometer la prestación de servicios esenciales, generar pérdidas financieras significativas, acarrear sanciones regulatorias y afectar la credibilidad institucional. En este contexto, este estudio analiza la integración entre la Continuidad del Negocio (BC) y la Recuperación ante Desastres (DR), examinando su relación con la planificación de la capacidad de la infraestructura de TI, el gobierno corporativo y los mecanismos de ciberseguridad contemporáneos. La investigación se desarrolló mediante una revisión bibliográfica basada en autores clásicos y literatura técnica especializada, con el fin de comprender cómo las prácticas preventivas, las políticas de gestión de riesgos y los modelos de resiliencia operativa contribuyen a garantizar altos niveles de disponibilidad del servicio. Los resultados indican que las estrategias de continuidad efectivas dependen de la convergencia de la planificación tecnológica, los procesos organizacionales, la capacitación de equipos y los mecanismos permanentes de monitoreo y respuesta ante incidentes. Se puede concluir que la resiliencia operativa ha dejado de ser un mero requisito tecnológico para convertirse en un componente esencial de la estrategia empresarial.

PALABRAS CLAVE: Continuidad del negocio; Recuperación ante desastres; Misión crítica; Planificación de capacidad; Seguridad de la información.

ABSTRACTO

La creciente dependencia de las organizaciones de las infraestructuras digitales ha elevado la continuidad operativa a un componente estratégico de la sostenibilidad empresarial. En entornos críticos, las interrupciones del sistema pueden afectar servicios esenciales, generar pérdidas financieras significativas, acarrear sanciones regulatorias y socavar la credibilidad institucional. Este estudio examina la integración entre la Continuidad del Negocio (BC) y la Recuperación ante Desastres (DR), explorando su relación con la planificación de la capacidad de la infraestructura de Tecnologías de la Información, el gobierno corporativo y las prácticas contemporáneas de ciberseguridad. La investigación se llevó a cabo mediante una revisión bibliográfica basada en autores clásicos y publicaciones técnicas especializadas, con el objetivo de comprender cómo las medidas preventivas, las políticas de gestión de riesgos y los marcos de resiliencia operativa contribuyen a mantener altos niveles de disponibilidad del servicio. Los hallazgos indican que las estrategias de continuidad efectivas se basan en la convergencia de la planificación tecnológica, los procesos organizacionales, la preparación del personal y los mecanismos de monitoreo continuo y respuesta a incidentes. El estudio concluye que la resiliencia operativa ha evolucionado más allá de una preocupación puramente tecnológica para convertirse en un pilar fundamental de la estrategia organizacional.

PALABRAS CLAVE: Continuidad del negocio; Recuperación ante desastres; Entornos de misión crítica; Planificación de capacidad; Seguridad de la información.

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 IV, vol. 2, 2023 | Envío: 14/12/2023 | Aceptado: 17/12/2023 | Publicación: 20/12/2023

INTRODUCCIÓN

La transformación digital ha aumentado significativamente la dependencia de las organizaciones de...
Infraestructuras de tecnología de la información. Procesos de producción, operaciones financieras, cadenas de suministro.
La logística y los servicios públicos han llegado a depender de sistemas cuya indisponibilidad, incluso si es por...
En estos cortos periodos, puede producir impactos operativos y económicos de gran magnitud.
En este escenario, la continuidad del negocio ya no se considera exclusivamente una responsabilidad.
Las habilidades técnicas de los departamentos de TI son necesarias para asumir una posición estratégica en la gestión empresarial.
La intensificación de las ciberamenazas, junto con la creciente complejidad de las arquitecturas
Los avances computacionales y la adopción de entornos híbridos y multi-nube han expandido sustancialmente la
Exposición de las organizaciones a eventos disruptivos. Ataques de ransomware, fallas de infraestructura,
Errores humanos, indisponibilidad de proveedores, desastres naturales e interrupciones del servicio.
Los datos esenciales demuestran que los incidentes capaces de comprometer las operaciones se han convertido en posibilidades reales.
cuestiones concretas que requieren una planificación continua y una capacidad de respuesta estructurada.
En este contexto, los programas de continuidad del negocio (BC) y
La recuperación ante desastres (DR) constituye un instrumento fundamental para
para reducir el impacto de estos sucesos. Si bien la continuidad del negocio establece directrices
Organizaciones centradas en mantener funciones esenciales, enfoques de recuperación ante desastres
para restaurar la infraestructura tecnológica necesaria para restablecer los servicios críticos.
Aunque tienen propósitos distintos, ambas disciplinas son complementarias y dependen de...
planificación integrada.
Otro elemento indispensable en este proceso es la planificación de la capacidad de la infraestructura.
Computacional. El dimensionamiento adecuado de los recursos de procesamiento, almacenamiento y red.
La conectividad influye directamente en la capacidad de recuperarse de incidentes, así como
Estabilidad operativa en condiciones normales de funcionamiento. Paralelamente, las políticas
Los enfoques modernos de seguridad de la información, basados en principios como Zero Trust y la segmentación de...
Las redes y la monitorización continua amplían la capacidad de las organizaciones para prevenir, detectar y...
Responder a amenazas cada vez más sofisticadas.
Dado este escenario, este estudio tiene como objetivo analizar la interacción entre la continuidad de
negocios, recuperación ante desastres, planificación de capacidad y seguridad de la información en

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 IV, vol. 2, 2023 | Envío: 14/12/2023 | Aceptado: 17/12/2023 | Publicación: 20/12/2023

Apoyo a entornos de misión crítica. Basado en literatura especializada, este estudio busca demostrar que la resiliencia organizacional depende menos de soluciones tecnológicas aisladas y más de... Integración entre gobernanza, infraestructura, procesos y personas.

METODOLOGÍA

La investigación se caracteriza como un estudio descriptivo y exploratorio, desarrollado por método de revisión bibliográfica. Según Gil (2019), este procedimiento metodológico permite sistematización del conocimiento existente sobre un fenómeno dado, lo que permite identificarlo. Convergencias, lagunas y diferentes enfoques presentes en la literatura científica.

La revisión bibliográfica incluyó libros, normas técnicas y publicaciones especializadas. relacionado con la continuidad del negocio, la recuperación ante desastres, la ingeniería de infraestructura, Planificación de capacidades, gobernanza de las tecnologías de la información y ciberseguridad.

Se priorizaron los trabajos reconocidos por la comunidad académica y técnica, incluidos los autores de referencias como Kenneth Laudon, William Stallings, Andrew Tanenbaum, Daniel Menascé y James Burtles, además de documentos ampliamente utilizados en la gestión y administración de servicios riesgos tecnológicos.

Las fuentes seleccionadas se analizaron comparativamente, buscando identificar principios. Principios comunes, recomendaciones recurrentes y prácticas establecidas aplicables a entornos corporativos de misión crítica. El material se organizó en cinco áreas temáticas: fundamentos de continuidad de Negocios; recuperación ante desastres; planificación de la capacidad de la infraestructura; ciberseguridad aplicado a entornos críticos; y gobernanza estratégica de la tecnología de la información. Esta estructura Permitió el establecimiento de relaciones entre aspectos técnicos, operativos y de gestión, fomentando una Un análisis integral de los factores que sustentan la resiliencia organizacional.

Además de la revisión conceptual, se consideraron los impactos resultantes de la reciente evolución de la [palabra faltante]. arquitecturas computacionales, especialmente la consolidación de la computación en la nube, de entornos Tecnologías distribuidas, virtualización de recursos y la creciente sofisticación de las ciberamenazas.

De este modo, el debate busca reflejar tanto los fundamentos clásicos de la literatura como los desafíos que plantea. desafíos contemporáneos que enfrentan las organizaciones que dependen de la alta disponibilidad de sus sistemas.

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 IV, vol. 2, 2023 | Envío: 14/12/2023 | Aceptado: 17/12/2023 | Publicación: 20/12/2023

1. FUNDAMENTOS DE LA CONTINUIDAD DEL NEGOCIO

La continuidad del negocio (BC) se refiere al conjunto de estrategias,
procesos y políticas diseñados para garantizar que las funciones esenciales permanezcan operativas, incluso
que la organización sea sometida a eventos capaces de comprometer su infraestructura o su
Procesos críticos. Si bien se asocian frecuentemente con las Tecnologías de la Información, su alcance es...
significativamente más grande, que involucra aspectos relacionados con la gobernanza, la gestión de riesgos,
Operaciones, recursos humanos, comunicación institucional y cumplimiento normativo.

El desarrollo de un programa de continuidad coherente presupone un compromiso de
alta dirección, responsable de establecer directrices, definir niveles de riesgo aceptables y garantizar
que los recursos necesarios estén disponibles. La efectividad de estas iniciativas depende de su
incorporación en la planificación estratégica, ya que la continuidad operativa influye
afecta directamente la capacidad de la organización para preservar los ingresos, cumplir con las obligaciones legales y mantener su...
Confianza por parte de clientes, inversores y organismos reguladores.
Entre los pasos fundamentales de este proceso, destaca el Análisis de Impacto Empresarial (BIA, por sus siglas en inglés).
Metodología diseñada para identificar procesos críticos, dependencias operativas y sus efectos.
resultante de la indisponibilidad de sistemas, personal o instalaciones. Más que una simple estimación de pérdidas.
En términos financieros, el BIA permite comprender las repercusiones en los aspectos reputacionales, legales y regulatorios.
y operativas, proporcionando información para priorizar las inversiones en resiliencia. Los resultados
Este análisis guía la definición de los parámetros que guiarán los planes de continuidad y
Recuperación. Los procesos cuya interrupción compromete actividades esenciales requieren estrategias.
capaz de reducir significativamente el tiempo de inactividad, mientras que las funciones
Las tareas administrativas de menor criticidad pueden permitir períodos de interrupción más prolongados sin
comprometiendo la sostenibilidad del negocio. Por lo tanto, la clasificación de los activos críticos se vuelve...
Un elemento indispensable para el uso racional de los recursos tecnológicos y financieros.
Otro aspecto que con frecuencia se pasa por alto se refiere a la documentación de los procedimientos.
Los planes operativos, ya sean demasiado genéricos o desactualizados, tienden a perder eficacia.
Precisamente cuando más se necesitan. En situaciones de crisis, hay que tomar decisiones.
debe tomarse bajo alta presión y a intervalos cortos. La existencia de procedimientos
claramente documentado, acompañado de responsabilidades previamente definidas, reduce la
Reduce la probabilidad de fallos operativos y mejora la coordinación entre los equipos técnicos y ejecutivos.

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 IV, vol. 2, 2023 | Envío: 14/12/2023 | Aceptado: 17/12/2023 | Publicación: 20/12/2023

La literatura especializada también enfatiza que los programas de continuidad no deben permanecer restringido al entorno documental. Simulaciones periódicas, ejercicios de mesa, Las pruebas de recuperación y la formación operativa permiten validar los procedimientos e identificar problemas. vulnerabilidades y mejorar continuamente los planes establecidos. Según Burtles (2015), la La madurez organizacional en continuidad está directamente relacionada con la frecuencia con la que estos Los procesos se practican y se revisan.

Otro factor determinante es la actualización continua de los planes. Cambios en la infraestructura tecnológica, cambios organizativos, adquisición de nuevos sistemas, expansión de operaciones o modificaciones Los cambios normativos pueden hacer que procedimientos previamente válidos resulten parcialmente inadecuados. Por esta razón Por lo tanto, los programas de continuidad del negocio maduros incorporan mecanismos de revisión continua. garantizar que la documentación se mantenga alineada con la realidad operativa de la organización.

En un escenario caracterizado por una creciente dependencia digital, la continuidad del negocio se ha convertido en una prioridad. desde representar simplemente una práctica preventiva hasta consolidarse como un elemento estructurador de Gobierno corporativo. Organizaciones capaces de responder con rapidez a eventos disruptivos. Demuestran una mayor estabilidad operativa, reducen las pérdidas financieras y fortalecen su capacidad. Adaptación a entornos cada vez más dinámicos e impredecibles.

2. ESTRUCTURACIÓN TÉCNICA DE LA RECUPERACIÓN ANTE DESASTRES

La recuperación ante desastres (DR) comprende el conjunto de procesos técnicos. destinado a la restauración de la infraestructura tecnológica tras sucesos capaces de interrumpirla. Interrupción parcial o total del funcionamiento de los sistemas corporativos. Mientras tanto, continuidad del negocio. La recuperación ante desastres, si bien es de naturaleza organizativa, se centra en la restauración de recursos. recursos informáticos necesarios para restablecer los servicios críticos a niveles aceptables. disponibilidad según se definió previamente.

El desarrollo de una estrategia de recuperación ante desastres requiere la definición objetiva de los requisitos para recuperación, teniendo en cuenta tanto las necesidades operativas como las limitaciones financieras de organización. Sin embargo, las soluciones altamente resilientes ofrecen tiempos de inactividad más cortos. Esto implica inversiones significativamente elevadas en infraestructura, conectividad y redundancia. Por lo tanto, una planificación adecuada consiste en equilibrar los niveles de riesgo aceptables con el Viabilidad económica del entorno tecnológico.

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 IV, vol. 2, 2023 | Envío: 14/12/2023 | Aceptado: 17/12/2023 | Publicación: 20/12/2023

En este contexto, destacan dos indicadores por su amplio uso tanto en la literatura como en la práctica.
Profesional: el Objetivo de Tiempo de Recuperación (RTO) y el Objetivo de Punto de Recuperación (RPO). El primero
Establece el tiempo máximo permitido para restablecer los servicios después de una interrupción.
mientras que el segundo define la cantidad máxima de datos cuya pérdida se puede tolerar en
un proceso de recuperación específico. Estos parámetros guían las decisiones relacionadas con la arquitectura.
desde la infraestructura hasta las tecnologías de replicación, las políticas de respaldo y la capacidad de procesamiento.
de entornos secundarios.

La definición de estos objetivos influye directamente en las inversiones en tecnología.
Organizaciones que operan aplicaciones financieras en tiempo real, sistemas hospitalarios,
Las telecomunicaciones o los servicios públicos esenciales a menudo requieren costes reducidos y...
cercano a cero, lo que requiere replicación de datos síncrona, almacenamiento distribuido y alta...
Disponibilidad entre centros de procesamiento geográficamente distintos. Por el contrario,
Las aplicaciones administrativas menos críticas pueden utilizar modelos de replicación asíncrona.
Reducir los costes sin comprometer significativamente la continuidad de las operaciones.

La distribución geográfica de los entornos de contingencia representa otro aspecto esencial de
Arquitectura de recuperación. La simple duplicación de infraestructura en instalaciones cercanas a
El entorno primario no siempre ofrece la protección adecuada contra desastres y perturbaciones naturales.
cortes de energía prolongados o fallas en los proveedores de conectividad regional. Estrategias modernas
Priorizan la dispersión geográfica de los centros de datos, minimizando así la probabilidad de fallos simultáneos.
derivados de eventos compartidos.

Según Tanenbaum y Wetherall (2011), la arquitectura de las propias redes debe incorporar mecanismos.
mecanismos de redundancia capaces de mantener la comunicación entre usuarios y servicios incluso frente a
Falta de disponibilidad de enlaces primarios. Protocolos de enrutamiento dinámico, múltiples proveedores.
Las alternativas accesibles y las vías de comunicación reducen significativamente el impacto operativo.
resultante de fallos en la infraestructura de red.

En los últimos años, la computación en la nube ha cambiado profundamente la forma en que funcionan los entornos.
Los modelos de recuperación ante desastres están diseñados para ser implementados. Los modelos de recuperación ante desastres como servicio (DRAAS) permiten...
Mantener infraestructuras de contingencia parcialmente aprovisionadas mediante la activación de recursos informáticos.
El mantenimiento adicional solo es necesario durante los periodos de inactividad. Este enfoque reduce los costes de mantenimiento.
Aumenta la escalabilidad de las soluciones y facilita la implementación de entornos distribuidos en
diferentes regiones geográficas.

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 IV, vol. 2, 2023 | Envío: 14/12/2023 | Aceptado: 17/12/2023 | Publicación: 20/12/2023

Sin embargo, la adopción de la nube no elimina la necesidad de planificación. Recuperación eficiente
Sigue dependiendo de la correcta definición de las prioridades empresariales y de la automatización de los procesos.
de conmutación por error, consistencia de las réplicas de datos y pruebas periódicas. Entornos cuya
La recuperación sigue dependiendo exclusivamente de procedimientos manuales y tiende a presentar
mayor susceptibilidad a errores operativos precisamente durante situaciones de crisis.
Desde esta perspectiva, la automatización adquiere un papel estratégico. Las herramientas de orquestación permiten
ejecutar secuencias previamente validadas para la inicialización y redirección de máquinas virtuales
tráfico, restauración del servicio y sincronización de la base de datos, reduciendo significativamente
el tiempo necesario para reanudar las operaciones. Además de acelerar la recuperación, la estandarización
Estos procedimientos aumentan su predictibilidad y reducen la variabilidad inherente a las intervenciones.
Humanos.

La evolución de las arquitecturas distribuidas, la virtualización y los servicios en la nube ha transformado...
La recuperación ante desastres como componente permanente de la ingeniería de infraestructuras. Más de
Además de restaurar los sistemas después de una falla, las estrategias contemporáneas buscan construir entornos
capaz de absorber interrupciones con un impacto mínimo en la continuidad del negocio,
consolidar la resiliencia tecnológica como un requisito esencial para las organizaciones impulsadas por
servicios digitales.

3. PLANIFICACIÓN DE LA CAPACIDAD DE LA INFRAESTRUCTURA DE TI

La planificación de la capacidad es una de las disciplinas fundamentales de la gestión de infraestructuras.
Tecnología de la Información, ya que su propósito es garantizar que los recursos informáticos
Los recursos disponibles deben ser suficientes para satisfacer las demandas actuales y futuras del negocio. Ese no es el objetivo.
Se limita a ampliar la capacidad instalada, pero implica un equilibrio entre rendimiento,
Disponibilidad, escalabilidad y eficiencia económica, al tiempo que se reducen los riesgos.
asociado con la subutilización o saturación de los activos tecnológicos.

A medida que las organizaciones amplían la digitalización de sus procesos, el comportamiento de la carga de trabajo...
Los procesos computacionales son cada vez más impredecibles. El crecimiento acelerado del volumen de datos y las nuevas...
Las aplicaciones corporativas, la integración de sistemas, los servicios en la nube y los eventos de temporada pueden
alterar significativamente el consumo de recursos en intervalos de tiempo cortos. En este contexto,
Las decisiones basadas únicamente en la percepción operativa ya no son suficientes, y requieren mecanismos.
Monitorización continua y análisis predictivo.

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 IV, vol. 2, 2023 | Envío: 14/12/2023 | Aceptado: 17/12/2023 | Publicación: 20/12/2023

Según Menascé, Almeida y Dowdy (2004), la planificación de la capacidad se basa en la recopilación

ancho de banda y latencia. Estos datos permiten la construcción de modelos capaces de estimar tendencias en
crecimiento e identificación anticipada de posibles puntos de degradación del rendimiento.
El análisis histórico representa solo un paso en este proceso. Los entornos corporativos están sujetos a
Las variaciones significativas en la demanda requieren la incorporación de pruebas de carga, simulaciones de tensión y...
proyecciones basadas en diferentes escenarios de crecimiento. Este enfoque permite evaluar no
no solo la capacidad máxima de los recursos informáticos, sino también su comportamiento frente a
En situaciones extremas, se reduce la probabilidad de indisponibilidad durante períodos de alta demanda.
usar.
La virtualización y la computación en la nube han cambiado sustancialmente la forma en que...
Se realiza una planificación de capacidad. Posibilidad de aprovisionamiento dinámico de recursos.
Aumentó la flexibilidad operativa y redujo el tiempo necesario para la expansión de la infraestructura.
Sin embargo, esta flexibilidad no elimina la necesidad de planificación. Recursos escalables
Siguen estando sujetos a limitaciones físicas, costes variables y restricciones contractuales impuestas por...
proveedores de servicios en la nube.
Otro aspecto frecuentemente subestimado se relaciona con la infraestructura de comunicaciones. Rendimiento
El rendimiento general de un entorno informático depende de la interacción equilibrada entre los servidores.
Almacenamiento de datos y redes. Cuellos de botella en el ancho de banda, mayor latencia o fallos.
Los problemas de conectividad recurrentes pueden comprometer las aplicaciones críticas incluso cuando hay
Disponibilidad suficiente de potencia de procesamiento y memoria. Por lo tanto, la planificación debe tener esto en cuenta.
Toda la cadena tecnológica involucrada en la prestación de los servicios.
La gestión de la capacidad también tiene una importante dimensión financiera. Adquisición anticipada
La escasez de equipos da como resultado activos subutilizados y un mayor costo total de propiedad, mientras que
Las inversiones tardías aumentan el riesgo de interrupciones operativas y pérdidas derivadas de la degradación.
de desempeño. El uso de indicadores técnicos asociados con proyecciones de crecimiento permite
para proporcionar una base más objetiva para las decisiones presupuestarias, acercando la gestión tecnológica a...
Estrategias corporativas.
En los últimos años, las técnicas basadas en inteligencia artificial y aprendizaje automático han comenzado a...
Integrar plataformas de observabilidad avanzadas. Estas características amplían la capacidad de
Identificar patrones de consumo, predecir comportamientos anómalos y recomendar ajustes antes de que se produzcan.
Se observan impactos notables en los usuarios. Si bien estas tecnologías no reemplazan el análisis.

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 IV, vol. 2, 2023 | Envío: 14/12/2023 | Aceptado: 17/12/2023 | Publicación: 20/12/2023

Los gestores especializados representan un importante paso adelante en la creación de entornos cada vez mejores.
Resiliente y autónomo.

Desde esta perspectiva, la planificación de capacidades deja de entenderse como una actividad.
Su función exclusivamente operativa es asumir un papel estratégico en la gobernanza de la infraestructura.
Las organizaciones que supervisan continuamente sus recursos son capaces de responder con mayor eficacia.
agilidad para adaptarse a los cambios en el entorno empresarial, preservando al mismo tiempo el rendimiento, la disponibilidad y
Sostenibilidad financiera a lo largo de todo el ciclo de vida de sus sistemas.

4. Ciberseguridad aplicada a entornos de misión crítica

La creciente sofisticación de las amenazas digitales ha transformado la ciberseguridad en un componente clave.
inseparable de la gestión de infraestructuras críticas. Ataques dirigidos, explotación de
Vulnerabilidades conocidas, compromiso de la cadena de suministro, campañas de ransomware
y las operaciones llevadas a cabo por grupos organizados demuestran que la falta de disponibilidad de sistemas ni
Siempre se origina en fallas técnicas, pero con frecuencia resulta de acciones deliberadas dirigidas a
interrupción de los servicios u obtención de ventajas económicas.
En este escenario, la disponibilidad, la integridad y la confidencialidad dejan de ser objetivos.
entidades independientes que constituyen dimensiones complementarias de la seguridad de la información. Según
Según Stallings (2020), la protección efectiva de los activos digitales depende de la adopción integrada de controles.
procesos técnicos y organizativos y mecanismos de monitoreo permanente, capaces de reducir
Evaluar simultáneamente la probabilidad y el impacto de los incidentes.
Entre los cambios más relevantes observados en la última década, destaca la consolidación del modelo.
Confianza cero. A diferencia de las arquitecturas tradicionales, que presuponían un alto grado de...
Confianza en las comunicaciones internas, este paradigma establece que cada solicitud de acceso debe
Debe estar autenticado, autorizado y supervisado de forma continua, independientemente de su ubicación.
El usuario o el dispositivo utilizado. La adopción de este modelo reduce significativamente el movimiento.
El atacante queda fuera de combate tras la vulneración inicial de las credenciales.
Otro principio fundamental consiste en aplicar el Principio del Mínimo Privilegio.
Según esta norma, los usuarios, las aplicaciones y los servicios reciben únicamente los permisos estrictamente necesarios.
para la ejecución de sus actividades. Este enfoque limita la propagación de los ataques y reduce su impacto.
como resultado de la explotación de cuentas privilegiadas, una de las técnicas más recurrentes en incidentes
seguridad en grandes organizaciones.

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 IV, vol. 2, 2023 | Envío: 14/12/2023 | Aceptado: 17/12/2023 | Publicación: 20/12/2023

La visibilidad operativa se ha vuelto igualmente indispensable. Plataformas SIEM (Sistemas de Gestión de Seguridad e Información)
Gestión de información y eventos), asociada con SOAR (Orquestación de seguridad,
La automatización y respuesta (ADR) mejora la capacidad de los equipos de seguridad para correlacionar
gestionar eventos, automatizar las respuestas iniciales e identificar comportamientos que no se ajusten a los estándares.
Procedimientos operativos normales. Sin embargo, la eficacia de estas herramientas depende de la calidad de los registros.
recopilados, a partir de la correcta parametrización de las reglas de correlación y la madurez de los procesos internos.
respuesta ante incidentes.

La segmentación lógica de la infraestructura sigue siendo un importante mecanismo de contención.
separación entre entornos administrativos, redes corporativas, sistemas industriales, bases de datos
Los servicios críticos y los servicios expuestos a Internet reducen significativamente la superficie de ataque a la que están expuestos.
intrusos. Junto con los cortafuegos de próxima generación, la inspección profunda de paquetes,
La autenticación multifactor y el cifrado de datos, tanto en tránsito como en reposo, refuerzan esta estrategia.
resiliencia de la arquitectura tecnológica.

La protección contra el ransomware ahora requiere enfoques más completos que simplemente...
Realizar copias de seguridad. Además de mantener copias de seguridad inmutables y geográficamente dispersas.
En entornos distribuidos, se recomienda que los entornos de recuperación permanezcan aislados de la infraestructura.
principal, lo que dificulta su propagación durante los ataques. De manera similar, las pruebas periódicas de
La restauración es esencial para garantizar que se pueda acceder eficazmente a la información almacenada.
para ser recuperado cuando sea necesario.

La ciberseguridad también depende de la evaluación continua de las vulnerabilidades existentes en
Infraestructura. Auditorías técnicas, pruebas de penetración, evaluaciones de cumplimiento y ejercicios RED.
Las herramientas de equipo permiten identificar vulnerabilidades antes de que sean explotadas por actores maliciosos. Más de
Al demostrar el cumplimiento de las normas y reglamentos, estas prácticas fortalecen la capacidad.
Objetivo institucional de anticipar riesgos y mejorar continuamente sus controles de seguridad.

En entornos de misión crítica, la protección de los activos digitales debe entenderse como un proceso.
Permanente y adaptable. La rápida evolución de las técnicas empleadas por los actores de amenazas exige
que las estrategias defensivas se revisen continuamente, incorporando nuevas tecnologías,
Actualizaciones de seguridad y mecanismos de detección avanzados. En este contexto, la resiliencia.
La ciberseguridad ahora representa no solo la capacidad de evitar ataques, sino principalmente la...
La capacidad de la organización para mantener sus operaciones incluso ante incidentes inevitables.

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 IV, vol. 2, 2023 | Envío: 14/12/2023 | Aceptado: 17/12/2023 | Publicación: 20/12/2023

5. Gestión estratégica y apoyo institucional

La efectividad de las estrategias de continuidad del negocio y recuperación ante desastres depende de factores que trascienden la infraestructura tecnológica. Aunque los servidores, las redes y las plataformas de Los mecanismos de almacenamiento y seguridad constituyen la base operativa de estas iniciativas, su La sostenibilidad está directamente relacionada con la capacidad de una organización para incorporar prácticas de Herramientas de gobernanza capaces de integrar tecnología, procesos, personas y objetivos institucionales. En este contexto, la gobernanza de las Tecnologías de la Información juega un papel decisivo en el establecimiento mecanismos formales para la toma de decisiones, la definición de responsabilidades y la gestión riesgos. Los marcos establecidos, como ITIL, COBIT y la familia de estándares ISO 27000, proporcionan directrices que permiten estandarizar procesos, aumentar la trazabilidad de los cambios y fortalecer La alineación entre las inversiones en tecnología y las estrategias corporativas. Más que Estos modelos prescriptivos representan herramientas de gestión orientadas a la mejora. madurez organizacional continua.

La gestión del cambio juega un papel central en este proceso. Los entornos de misión crítica son Sujeto a actualizaciones frecuentes de software, reemplazo de equipos y ajustes de configuración. y la integración de nuevos servicios. Cuando se ejecuta sin una planificación o validación adecuadas, Los cambios aparentemente simples pueden tener un impacto significativo en la disponibilidad de sistemas. Por esta razón, los procesos estructurados de gestión del cambio reducen la probabilidad de interrupciones resultantes de fallas operativas y promueven una mayor previsibilidad en la evolución de infraestructura.

Otro aspecto frecuentemente asociado con el desempeño institucional es la estandarización tecnológica. Las infraestructuras excesivamente heterogéneas aumentan la complejidad operativa y dificultan... La gestión de activos aumenta el tiempo necesario para el diagnóstico y la resolución de incidentes. Adopción de estándares arquitectónicos, políticas de configuración y procedimientos operativos uniformes. Simplifica el soporte técnico, mejora la interoperabilidad entre plataformas y reduce los costes. relacionado con el mantenimiento ambiental.

La gestión del conocimiento también es un elemento estratégico. Alta especialización Las exigencias de las infraestructuras contemporáneas hacen que depender únicamente del conocimiento resulte insuficiente. Restringido a ciertos profesionales. Las organizaciones resilientes invierten en documentación. entornos sistemáticos, en el mantenimiento de bases de conocimiento, en la estandarización de Procedimientos técnicos y formación continua de sus equipos. Este enfoque reduce los riesgos.

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 IV, vol. 2, 2023 | Envío: 14/12/2023 | Aceptado: 17/12/2023 | Publicación: 20/12/2023

como resultado de la rotación de personal y acelera el proceso de respuesta durante situaciones de crisis.
La comunicación institucional también influye directamente en la eficacia de los programas.
Continuidad. Durante incidentes críticos, la disponibilidad de información clara y oportuna reduce...
Elimina las incertidumbres, mejora la coordinación entre las áreas técnicas y administrativas y fortalece la confianza en
Clientes, socios y organismos reguladores. En este sentido, los planes de comunicación deben integrar la
programas de continuidad desde su inicio, incluidos los flujos de información internos y
Factores externos compatibles con diferentes escenarios de crisis.
Finalmente, el seguimiento sistemático de los indicadores de desempeño permite evaluar la eficacia.
de las estrategias implementadas e identificar oportunidades de mejora. Métricas relacionadas
para el cumplimiento de los acuerdos de nivel de servicio (SLA), disponibilidad del sistema, tiempos promedio
Las tasas de recuperación, la recurrencia de incidentes y la eficiencia operativa sirven de base para las decisiones de gestión.
Basándose en la evidencia, promueve la evolución continua de los programas de gobernanza.
tecnológico.
De este modo, la gestión estratégica deja de actuar únicamente como un elemento de coordinación administrativa.
asumir un papel estructurador en la construcción de entornos resilientes, capaces de sostener el
Continuidad operativa incluso en escenarios altamente complejos e inciertos.

CONCLUSIÓN

La creciente digitalización de las actividades económicas e institucionales ha convertido la continuidad operativa en uno
de los principales retos de la gestión contemporánea de las tecnologías de la información.
A medida que las organizaciones dependen cada vez más de infraestructuras altamente interconectadas,
La indisponibilidad del sistema deja de ser simplemente un problema técnico y se convierte en...
importantes implicaciones financieras, regulatorias, operativas y de reputación.
El análisis desarrollado en este estudio muestra que los programas eficaces de continuidad del negocio
La recuperación y gestión de desastres no pueden entenderse como iniciativas aisladas. Su eficacia
Esto resulta de la integración de la planificación estratégica, la ingeniería de infraestructuras y la gestión de riesgos.
Ciberseguridad y gobernanza organizacional. La capacidad de anticipar vulnerabilidades,
Establecer prioridades de recuperación y estructurar mecanismos de seguimiento permanentes.
Este es un factor determinante para mantener la disponibilidad de los servicios esenciales.
También se observó que la planificación de la capacidad juega un papel decisivo en
Apoyando esta estrategia. Monitoreo continuo del comportamiento de la infraestructura,

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 IV, vol. 2, 2023 | Envío: 14/12/2023 | Aceptado: 17/12/2023 | Publicación: 20/12/2023

combinado con el uso de modelos predictivos y la adopción de arquitecturas escalables, permite que
Las organizaciones responden de manera más eficiente a las crecientes demandas y reducen la
Probabilidad de interrupciones resultantes de la saturación de los recursos informáticos.
En el ámbito de la seguridad de la información, se ha observado que la evolución de las ciberamenazas requiere...
enfoques cada vez más integrados. Modelos como Zero Trust, autenticación multifactor,
Segmentación de red, monitorización continua y políticas sólidas de protección contra el ransomware.
Han dejado de representar elementos diferenciadores tecnológicos y se han convertido en requisitos establecidos.
Principios básicos de la resiliencia operativa en entornos de misión crítica.
Otro aspecto destacado por la literatura se refiere a la importancia de la gobernanza institucional.
Procesos formales de gestión del cambio, documentación técnica, formación continua de
Los equipos y el uso de indicadores de desempeño fortalecen la capacidad de las organizaciones para...
Responder con rapidez a los eventos disruptivos, reduciendo los impactos operativos y aumentando...
Previsibilidad de las acciones de recuperación.
Aunque este trabajo se desarrolló a partir de una revisión de la literatura, los resultados obtenidos
Demuestran un alto grado de convergencia entre los marcos teóricos y las prácticas actuales.
adoptado por organizaciones que operan servicios de alta disponibilidad. Esta convergencia refuerza la
comprender que la resiliencia tecnológica no depende exclusivamente de la adquisición de
infraestructura más robusta, pero también una integración consistente entre tecnología, procesos, personas y
gobernancia.
Como perspectiva para futuros estudios, se recomienda investigar más a fondo la aplicación de
Inteligencia artificial en la gestión predictiva de infraestructuras, automatización de procesos de recuperación,
Observabilidad basada en análisis de comportamiento y estrategias de ciberresiliencia dirigidas a
Entornos híbridos y multi-nube. Estos temas tienden a ejercer una influencia cada vez mayor en la forma en que
Cómo diseñarán las organizaciones sus programas de continuidad en los próximos años.
En resumen, se puede concluir que la capacidad de mantener las operaciones críticas ante eventos adversos...
Actualmente constituye una ventaja competitiva y un requisito indispensable para las organizaciones.
impulsado por los servicios digitales. En este contexto, la integración entre la continuidad del negocio,
La recuperación ante desastres, la planificación de capacidades, la ciberseguridad y la gobernanza representan la
La base principal para construir entornos tecnológicos resilientes, sostenibles y preparados.
para afrontar los retos de un entorno operativo en constante cambio.

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 IV, vol. 2, 2023 | Envío: 14/12/2023 | Aceptado: 17/12/2023 | Publicación: 20/12/2023

REFERENCIAS

- BURTLES, J. Principios y práctica de la continuidad del negocio. 2.ª ed. Rothstein Publishing, 2015.
- GIL, AC Cómo desarrollar proyectos de investigación. 6.ª ed. Atlas, 2019.
- LAUDON, K. C.; LAUDON, JP Sistemas de información gerencial. 16.ª ed. Pearson, 2020. • MENASCÉ, DA; ALMEIDA, VAF; DOWDY, LW Rendimiento por diseño. Prentice Hall, 2004.
- STALLINGS, W. Criptografía y seguridad de redes. 8.ª ed. Pearson, 2020.
- TANENBAUM, AS; WETHERALL, Redes informáticas para DJ. 5. Ed. Pearson, 2011.
- ISO 22301:2019 — Seguridad y resiliencia — Sistemas de gestión de la continuidad del negocio.
- ISO/IEC 27001:2022 — Seguridad de la información, ciberseguridad y protección de la privacidad — sistemas de gestión de la seguridad de la información.
- ISO/IEC 27002:2022 — Controles de seguridad de la información.
- NIST SP 800-34 Rev. 1 — Guía de planificación de contingencias para sistemas de información federales.
- Marco de Ciberseguridad (CSF) 2.0 del NIST, 2024.

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.