Tema 4

Instrucción: Con base a las definiciones resuelve la sopa de letras

O	S	O	V	I	T	A	R	E	P	O	O	C	P	C
C	C	A	E	T	D	A	D	I	R	U	G	E	S	U
I	D	U	I	L	U	C	A	M	H	P	V	O	A	A
G	E	Ñ	M	T	I	U	D	C	U	A	Q	R	N	N
É	N	E	U	P	V	A	I	C	D	A	N	E	N	T
T	O	Ó	V	I	L	L	T	R	S	A	E	Z	Ó	I
A	L	D	I	N	Ó	I	C	A	T	I	V	E	I	T
R	N	H	E	C	I	T	M	B	R	A	O	S	C	A
T	I	U	N	Y	A	A	P	I	A	L	I	C	A	T
S	O	R	E	U	M	T	D	Á	E	N	S	O	G	I
E	R	L	E	D	A	I	P	O	I	N	V	E	I	V
T	C	N	A	V	D	V	B	E	U	I	T	L	T	A
S	N	V	O	A	Ó	A	I	D	C	N	O	O	I	L
U	G	M	I	C	N	E	Y	L	O	A	C	U	M	Q
A	A	I	C	N	E	R	E	F	S	N	A	R	T	D

1. Estrategia de tratamiento que implementa controles, políticas o tecnologías para reducir la probabilidad o el impacto de una amenaza:
2. Tipo de riesgo que involucra fallas en el hardware, errores en el diseño de software, interrupciones en la red o caídas de bases de datos por concurrencia:
3. Tipo de evaluación que asigna valores descriptivos (alto, medio, bajo) a la probabilidad y al impacto para obtener una visión rápida y priorizar amenazas inminentes:
4. Estrategia de tratamiento que consiste en reconocer una amenaza y decidir no tomar medidas adicionales porque el costo de mitigación supera el impacto potencial:

Equipo 9: -Dulce Denisse Garcia Cruz -Jose Manuel Reyes Morales -Alonso Emanuel Sanchez Castillo

LIVEWORKSHEETS

5. Tipo de riesgo relacionado con el incumplimiento de normativas locales e internacionales sobre el manejo de datos, licencias de software o auditorías:
6. Tipo de evaluación que asigna valores numéricos o monetarios utilizando métricas como la Expectativa de Pérdida Anual (ALE) para justificar inversiones en controles:
7. Estrategia de tratamiento que traslada el impacto financiero de una contingencia a un tercero, generalmente mediante seguros de ciberseguridad o tercerización:
8. Tipo de riesgo que comprende la obsolescencia tecnológica, la adopción de tecnologías incompatibles con los objetivos de negocio o el fracaso en proyectos críticos:
9. Estrategia de tratamiento que consiste en eliminar la causa de una amenaza suspendiendo la actividad que la genera:
10. Tipo de riesgo que comprende ataques cibernéticos como ransomware, phishing, inyecciones SQL, ataques de denegación de servicio (DDoS) o robo de credenciales:

Instrucción: Lee detenidamente cada oración y escribe la palabra o concepto correcto en el espacio en blanco para completar la afirmación sobre los principios de seguridad de la información.

La _____ garantiza que la información de la empresa solo sea accesible para los usuarios, procesos y sistemas que cuentan con la autorización adecuada.

El uso de firmas digitales, control de versiones y funciones hash son mecanismos clave para asegurar la _____ de los datos, evitando modificaciones no autorizadas.

Al implementar arquitecturas redundantes y servidores de respaldo, una organización busca garantizar la _____ de sus servicios frente a posibles interrupciones.

El conjunto fundamental de estos tres principios de seguridad (Confidencialidad, Integridad y Disponibilidad) es conocido en la industria como la _____.

Para cumplir con las normativas legales y proteger la privacidad de los usuarios, es indispensable aplicar procesos de _____, los cuales ocultan la identidad en las bases de datos, así como políticas de retención.

Equipo 9: -Dulce Denisse Garcia Cruz -Jose Manuel Reyes Morales -Alonso Emanuel Sanchez Castillo

LIVEWORKSHEETS

Instrucciones: Relaciona el concepto de la columna izquierda con su definición correspondiente en la columna derecha, trazando una línea:

CAPEX (Inversiones de capital)	**Proceso administrativo que abarca desde el control de inventarios de hardware y gestión de licencias, hasta la evaluación de obsolescencia.**
OPEX (Gastos operativos)	**Métrica financiera fundamental utilizada para medir la rentabilidad y justificar económicamente los proyectos tecnológicos ante la dirección.**
Recursos Humanos	**Factor considerado el eslabón más crítico en TI; requiere de planes de capacitación continua y el fomento de una sólida cultura de ciberseguridad.**
Retorno de Inversión (ROI)	**Gasto destinado a la adquisición de activos a largo plazo o infraestructura física, como la compra de servidores propios o licencias de software perpetuas.**
Ciclo de vida tecnológico	**Gastos recurrentes necesarios para mantener la operación tecnológica diaria, como el pago de suscripciones en la nube (SaaS) o mantenimiento.**

Analiza los siguientes escenarios empresariales y selecciona del menú desplegable el concepto técnico al que hacen referencia.

Un hospital determina que su sistema de expedientes médicos electrónicos no puede estar fuera de servicio por más de 1 hora sin poner en riesgo a los pacientes. Esta métrica de tiempo máximo de caída se conoce como:
[RTO / RPO / BCP / Sitio frío]

Una institución financiera configura sus copias de seguridad (backups) para ejecutarse cada 15 minutos, ya que es la cantidad máxima de información transaccional que están dispuestos a perder ante una falla. Esta métrica de tolerancia a la pérdida de datos se denomina:
[RTO / RPO / DRP / Sitio tibio]

Equipo 9: -Dulce Denisse Garcia Cruz -Jose Manuel Reyes Morales -Alonso Emanuel Sanchez Castillo

LIVEWORKSHEETS

Tras un sismo severo que inhabilita las oficinas corporativas, la empresa activa un documento estratégico y logístico que indica a los empleados a qué oficinas alternas deben dirigirse y cómo se comunicarán con los clientes. Este documento es el:
[Tríada CIA /BCP/DRP]

Después de un ataque de ransomware que encriptó los servidores, el equipo de TI utiliza un subconjunto de manuales técnicos enfocados exclusivamente en levantar nuevamente las bases de datos y la red. Este esfuerzo técnico se rige por el:
[BCP/DRP/Análisis CAPEX]

Equipo 9: -Dulce Denisse Garcia Cruz -Jose Manuel Reyes Morales -Alonso Emanuel Sanchez Castillo

LIVEWORKSHEETS