CURSO	**:**	Seguridad			Informática
DOCENTE	**:**	Erick	Kevin	Ramos	Pomari
SEMESTRE	**:**	2024-II			
CICLO	**:**	Sexto			
FECHA	**:**	19/08/2024			

FECHA DE INICIO : Lunes 19 de agosto 21:55 horas.
FECHA DE FIN : Martes 20 de agosto 21:55 horas.

ALUMNO (A) : DAVID KENSHIN VEGA ORTIZ

Examen Final (EF)

LOGRO DE APRENDIZAJE:

- Comprende la importancia de la ciberseguridad, la relación entre la ciberseguridad y la seguridad de la información y el papel de las partes interesadas en la ciberseguridad.
- Identifica los controles de seguridad necesarios para alinear a una organización a un programa de Ciberseguridad.
- Reconoce la importancia de la continuidad de los negocios desde el punto de vista tecnológico y que factores considerar para su implementación o lineamiento.

TEMAS:

- Gestión de la Ciberseguridad.
- Definiendo Controles Ciberseguridad bajo la ISO 27032.
- Conociendo la ISO 22301: Sistema de Gestión de la Continuidad del Negocio.

CONSIDERACIONES GENERALES:

- Lea el enunciado y las indicaciones del ejercicio y la rúbrica de calificación atentamente.
- Deberás guardar tu evaluación en **formato PDF**.
- Tenga en consideración la fecha de entrega. No se recibirá pasado el plazo.
- Todo el desarrollo del examen deberá de ser documentado (Capturas de pantalla) para los laboratorios, en caso aplique.

PREGUNTAS:

1. ¿Qué es la Ciberseguridad? (2 puntos)

La ciberseguridad se define como la práctica de proteger redes, sistemas, dispositivos y datos de amenazas digitales y ataques maliciosos. Su objetivo principal es proteger la información confidencial y garantizar que los sistemas informáticos estén seguros y disponibles frente a accesos no autorizados y ciberataques.

2. ¿Qué busca proteger la Ciberseguridad? (2 puntos)

- Redes y sistemas: Proteger la infraestructura tecnológica, como redes, servidores y dispositivos, de accesos no autorizados y ataques cibernéticos.
- Datos confidenciales: Salvaguardar información sensible, incluyendo datos personales, financieros y de propiedad intelectual, para evitar robos y filtraciones.
- Operaciones comerciales: Asegurar la continuidad de las operaciones al prevenir interrupciones causadas por ciberataques, lo que es fundamental para mantener la confianza de clientes y cumplir con normativas.
- Privacidad y seguridad personal: Proteger la privacidad de los individuos y evitar que se exploten sus datos personales, lo que también contribuye a la seguridad física.
- Reputación organizacional: Mantener la integridad y reputación de la empresa, evitando que incidentes de seguridad dañen la confianza del público y de los clientes.

3. ¿Cómo podemos definir un plan de continuidad de negocios? (2 puntos)

Un plan de continuidad de negocios (PCN) es un conjunto de estrategias y procedimientos que una organización establece para garantizar que pueda continuar operando tanto durante como después de una interrupción significativa. El objetivo principal de este plan es restaurar las funciones críticas de la empresa dentro de un tiempo predeterminado después de un evento no deseado, como desastres naturales, ciberataques o crisis operativas.

4. ¿Cuál es la primera responsabilidad de un Plan de Continuidad de Negocios? (2 puntos)

La primera responsabilidad clave de un Plan de Continuidad de Negocios (PCN) es proteger la vida de las personas. Antes de cualquier otra consideración, un PCN debe asegurar que se tomen las medidas necesarias para salvaguardar la seguridad y bienestar de los empleados, clientes y partes interesadas en caso de una emergencia o desastre.

5. Indique las 6 ventajas de la Continuidad de Negocios (2 puntos)

I. Protección de la Vida Humana: Prioriza la seguridad de los empleados y clientes, estableciendo protocolos claros para emergencias que minimizan riesgos durante situaciones críticas.
II. Minimización de Pérdidas Financieras: Al garantizar que las operaciones críticas continúen durante una interrupción, se reducen las pérdidas económicas que pueden resultar de paradas prolongadas.
III. Recuperación Rápida: Facilita la restauración de operaciones en un tiempo más corto, lo que permite a la empresa volver a la normalidad rápidamente después de un evento disruptivo.

IV. Mejora de la Reputación: Las organizaciones que demuestran su capacidad para manejar crisis de manera efectiva suelen ganar la confianza de clientes y socios, lo que mejora su imagen en el mercado.
V. Cumplimiento Normativo: Ayuda a las empresas a cumplir con regulaciones y estándares de la industria relacionados con la gestión de riesgos y la protección de datos, evitando sanciones legales.
VI. Preparación para el Futuro: Fomenta una cultura de preparación y resiliencia dentro de la organización, lo que permite adaptarse mejor a cambios y desafíos futuros, incluidos los tecnológicos y de mercado.

6. ¿Qué es la Resiliencia? (2 puntos)

La resiliencia se define como la capacidad de una persona o grupo para superar la adversidad y adaptarse a situaciones difíciles, permitiendo así seguir proyectando un futuro positivo. Este concepto se aplica en diversos contextos, desde la psicología hasta la ingeniería, y se refiere a la habilidad de recuperarse de traumas, crisis o desafíos significativos.

7. ¿Qué es un Sitio Alterno? (2 puntos)

un sitio alterno se refiere a una ubicación alternativa designada para operar los sistemas y procesos críticos de una organización en caso de que su sitio principal se vuelva inaccesible debido a desastres, fallos de infraestructura o incidentes de seguridad. Este sitio permite a la empresa mantener la continuidad de sus operaciones y minimizar la interrupción del servicio.

8. ¿Cuáles son los 5 tipos de ejercicios de plan de pruebas de Continuidad del Negocios (BCP)? (2 puntos)

I. Ejercicios de Mesa (Tabletop Exercises
II. Pruebas de Funcionalidad (Functional Tests
III. Simulacros (Drills)
IV. Ejercicios Integrales (Full-Scale Exercises)
V. Revisiones Post-Ejercicio (Post-Exercise Reviews)

9. ¿Cuál de los siguientes NO es un control en servidores? (1 punto)
A. Configurar la seguridad de los servidores
B. Habilitar el registro de auditoría
C. Actualizaciones de seguridad y funcionalidad
D. Escaneo de malware
E. Bloquear su pantalla del equipo o celular

10 ¿Cuál de los siguientes NO es un control en aplicación? (1 punto)
A. Copias de respaldo de información
B. Manejo de sesiones
C. Contraseñas seguras y cambiadas cada cierto tiempo
D. Revisiones o auditorías a los sistemas de información
E. Protocolo seguro HTTPS

11 ¿Cuál de los siguientes términos NO pertenece a la Tríada de la Ciberprotección? (1 punto)
A. Integridad
B. Autenticidad
C. Disponibilidad
D. Confidencialidad

12 ¿Qué información NO se puede conseguir en la Deep Web? (1 punto)
A. Repositorios específicos de compañías
B. Inteligencia Gubernamental
C. Sitios de venta de drogas ilegales
D. Información médica
E. Documentos legales