**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)** | **: MIGUEL ALFONZO CHAVEZ RAMOS** | | |

**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 es el conjunto de técnicas, prácticas y medidas que se utilizan para proteger sistemas, redes y datos digitales de ataques, accesos no autorizados, daños y robos. Su objetivo principal es asegurar la confidencialidad, integridad y disponibilidad de la información, así como proteger los recursos tecnológicos de amenazas como malware, hacking, phishing y otras formas de ciberataques.

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

* Confidencialidad: garantizar que la información solo sea accesible a las personas o organizaciones autorizadas. Esto evita el acceso no autorizado a información confidencial.
* Integridad: asegurarse de que los datos sean precisos y confiables al asegurarse de que la información y los sistemas no sean alterados de manera no autorizada.
* Disponibilidad: garantizar que la información y los servicios estén disponibles para su uso cuando se necesiten y proteger contra interrupciones en el acceso causadas por ataques o fallas técnicas.

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

Un plan de continuidad de negocios (BCP) es un conjunto de medidas predeterminadas que una organización implementa para garantizar que las operaciones críticas continúen durante y después de un evento disruptivo. El objetivo principal es reducir el impacto de interrupciones comerciales causadas por desastres naturales, fallas tecnológicas, pandemias u otras crisis importantes.

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

La primera responsabilidad de un Plan de Continuidad de Negocios es garantizar que las operaciones críticas de la empresa estén protegidas y continuamente funcionando en caso de desastres o interrupciones. Esto implica identificar los procesos esenciales, evaluar los riesgos y crear planes y procedimientos para mantener la operación o recuperarla lo más rápido posible, minimizando el impacto en la organización.

1. Indique las 6 ventajas de la Continuidad de Negocios (2 puntos)
2. Minimización de interrupciones: Reduce el impacto de eventos adversos, asegurando que la empresa pueda seguir operando sin interrupciones significativas.
3. Protección de la reputación: Mantiene la confianza de los clientes, socios y accionistas al demostrar la capacidad de la empresa para manejar crisis y continuar operando.
4. Reducción de pérdidas financieras: Minimiza las pérdidas económicas al permitir la rápida recuperación y la reanudación de operaciones tras un incidente.
5. Cumplimiento regulatorio: Ayuda a cumplir con normativas y estándares que exigen planes de continuidad de negocio, evitando sanciones legales y financieras.
6. Mejora de la resiliencia organizacional: Fortalece la capacidad de la empresa para adaptarse y recuperarse de eventos disruptivos, aumentando su resistencia a futuras crisis.
7. Protección de los recursos críticos: Asegura que los recursos esenciales, como datos, infraestructuras y personal clave, estén protegidos y disponibles para mantener las operaciones críticas en marcha.
8. ¿Qué es la Resiliencia? (2 puntos)

La capacidad de una persona o sistema para enfrentar, adaptarse y recuperarse de circunstancias adversas, desafíos o cambios significativos se conoce como resiliencia. En términos humanos, significa mantener o incluso mejorar el bienestar emocional y psicológico al resistir, superar y aprender de situaciones difíciles. La capacidad de resiliencia no solo ayuda a superar crisis, sino también a crecer a partir de ellas, generando una mayor fortaleza y capacidad de adaptación para enfrentar futuros obstáculos.

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

Un Sitio Alterno en seguridad informática es una ubicación física separada y distinta de la infraestructura principal de una organización, diseñada para albergar sistemas críticos y continuar las operaciones en caso de una interrupción grave, como un desastre natural, ciberataque o fallo técnico.

1. ¿Cuáles son los 5 tipos de ejercicios de plan de pruebas de Continuidad del Negocios (BCP)? (2 puntos)
2. Ejercicio de Revisión del Plan (Plan Review)
3. Ejercicio de Simulación o Walkthrough
4. Ejercicio de Simulacro de Mesa (Tabletop Exercise)
5. Ejercicio de Simulación Funcional (Functional Drill)
6. Ejercicio Completo o Integral (Full-Scale Exercise)
7. ¿Cuál de los siguientes NO es un control en servidores? (1 punto)
8. Configurar la seguridad de los servidores
9. Habilitar el registro de auditoría
10. Actualizaciones de seguridad y funcionalidad
11. Escaneo de malware
12. Bloquear su pantalla del equipo o celular
13. ¿Cuál de los siguientes NO es un control en aplicación? (1 punto)
14. Copias de respaldo de información
15. Manejo de sesiones
16. Contraseñas seguras y cambiadas cada cierto tiempo
17. Revisiones o auditorías a los sistemas de información
18. Protocolo seguro HTTPS
19. ¿Cuál de los siguientes términos NO pertenece a la Tríada de la Ciberprotección? (1 punto)
    1. Integridad
    2. Autenticidad
    3. Disponibilidad
    4. Confidencialidad
20. ¿Qué información NO se puede conseguir en la Deep Web? (1 punto)
21. Repositorios específicos de compañías
22. Inteligencia Gubernamental
23. Sitios de venta de drogas ilegales
24. Información médica
25. Documentos legales