SEGURIDAD Y CONTINUIDAD DE SISTEMAS

**EXAMEN PARCIAL**

**INSTRUCCIONES:**

* **El alumno debe leer el compromiso ético de la evaluación.**
* **El alumno debe redactar su apellido, nombre y DNI, en el párrafo del compromiso ético caso contrario la evaluación no será corregida.**
* El alumno deberá leer detenidamente cada una de las indicaciones de la evaluación con la finalidad de cumplir con todos los puntos solicitados.
* Si el alumno tuviera dudas con respecto a lo solicitado en uno o varios puntos deberá comunicarlo oportunamente al docente para que la duda sea aclarada en un plazo prudente y pueda cumplir con los plazos de entrega de la evaluación.

**COMPROMISO ÉTICO:**

*YO,* ***Jimmy Niels PAYTAN VILLAVICENCIO*** *con DNI* ***46292623*** *me responsabilizo por el contenido de esta evaluación. Afirmo ser el autor de las respuestas a las preguntas realizadas. Asimismo, aseguro no haber tomado parcial o totalmente ningún texto académico de alumnos de esta institución u otras ni documentos generales de la web u otras fuentes sin haber colocado la cita correspondiente.*

*Sé que esta actividad podrá ser analizada con los filtros de****SafeAssign,****los cuales compararán los textos con Global Reference Database, archivos de documentos institucionales, internet y ProQuest ABI/Inform Journal Database. Soy consciente de que se aplicará el reglamento vigente de estudios y las sanciones que correspondan de encontrarse irregularidades en cuanto al contenido enviado en la evaluación.*

1. **FINALIDAD / OBJETIVO DE LA EVALUACIÓN**

Evaluar el nivel de conocimiento adquirido durante el desarrollo de las 7 primeras sesiones del curso de **Seguridad y Continuidad de Sistemas**. Para lo cual, se evaluarán los conocimientos relacionados a los controles de la norma ISO 27001.

1. **CONSIDERACIONES GENERALES PARA EL DESARROLLO DEL PROYECTO**

El examen parcial es una evaluación INDIVIDUAL que mide el nivel de entendimiento de cada participante del curso.

1. **CONSIDERACIONES DEL ENTREGABLE**

El desarrollo del examen parcial debe presentarse en formato de documento con extensión “.doc” o “.docx” y debe ser entregado entre las 00.00 - 23.59 horas del día correspondiente a la sesión 8 del curso.

1. **INSTRUCCIONES DE LA EVALUACIÓN**
   1. Lea detenidamente las instrucciones y responda de forma clara.
   2. Para seleccionar la opción de las preguntas múltiples utilice la herramienta resaltador de Word, use el color amarillo.

SEGURIDAD Y CONTINUIDAD DE SISTEMAS

**EXAMEN PARCIAL**

1. **Sombrear la alternativa que describa adecuadamente el concepto indicado:**
2. **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Este proceso se basa en la fecha de creación de los archivos y la primera vez que se ejecute realiza un respaldo completo. (1 punto)**
3. Backup completo.
4. Backup incremental.
5. Backup diferencial.
6. Backup seguro.
7. **Documento de seguridad de la información que indica las obligaciones y derechos de los usuarios (internos, externos) (1 punto)**
8. Normativa.
9. Procedimiento.
10. ISO.
11. Política.
12. **El siguiente enunciado “A.12 Seguridad de las operaciones”, corresponde a un \_\_\_\_\_\_\_\_\_\_\_. (1 punto)**
13. Control.
14. Objetivo de Control.
15. Dominio.
16. Política.
17. **El siguiente enunciado “A.12.3 Respaldo”, corresponde a un \_\_\_\_\_\_\_\_\_\_\_. (1 punto)**
18. Control.
19. Objetivo de Control.
20. Dominio.
21. Política.
22. **Respecto a la gestión de claves asimétricas, en un proceso de cifrado de información. El siguiente escenario “Brittany y Bryan desean comunicarse. Si Brittany cifra el mensaje con su clave privada, y se lo envía a Bryan. Esté deberá abrir el mensaje con la clave Pública de \_\_\_\_\_\_\_\_\_\_\_\_\_, con lo cual se garantiza la \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ del mensaje. (1 punto)**
23. Brittany - Confidencialidad.
24. Bryan - Confidencialidad.
25. Brittany - Autenticidad.
26. Bryan - Autenticidad.
27. **Las políticas de desarrollo seguro de software de una organización, deben ser cumplidos por \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ de la organización. (1 punto)**
28. Desarrolladores internos.
29. Desarrolladores externos.
30. Desarrolladores internos y desarrolladores externos.
31. Desarrolladores internos, desarrolladores externos y todo aquel que participe en el proceso.
32. **El siguiente enunciado “A.10.1.2 Gestión de Claves”, corresponde a un \_\_\_\_\_\_\_\_\_\_\_. (1 punto)**
33. Control.
34. Objetivo de Control.
35. Dominio.
36. Política.
37. **El cifrado simétrico se basa en \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, tanto para hacer el cifrado como para el descifrado. (1 punto)**
38. Una política.
39. Un par de claves.
40. Una sola clave.
41. Un criterio.
42. **La política de seguridad de la información debe ser \_\_\_\_\_\_\_\_\_\_\_\_\_\_ y alineada los \_\_\_\_\_\_\_\_\_\_\_\_\_\_. (1 punto)**
43. Clara – objetivos del negocio.
44. Técnica – problemas del negocio.
45. Clara – problemas del negocio.
46. Técnica – objetivos del negocio.
47. **Respecto al proceso de elaboración de la política. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, tiene como objetivo “el equipo encargado redacta la política y escribe las diferentes secciones”. (1 punto)**
48. Identificar los componentes de la política.
49. Escribir las secciones.
50. Validación de contenido y de forma.
51. Validación por parte de las partes interesadas.
52. **\_\_\_\_\_\_\_\_\_\_\_\_\_\_, el término se utiliza normalmente para correo no deseado. (1 punto)**
53. Ransomware.
54. Phishing.
55. SPAM.
56. Malware.
57. **La copia de seguridad/respaldo de información, es un control preventivo contra la \_\_\_\_\_\_\_\_\_\_\_\_\_\_de la información. (1 punto)**
58. Disponibilidad.
59. Integridad.
60. Confidencialidad.
61. Confiabilidad.
62. **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Solo copia aquellos archivos nuevos o modificados. (1 punto)**
63. Backup completo.
64. Backup incremental.
65. Backup diferencial.
66. Backup seguro.
67. **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ es un evento que potencialmente puede causar daño. (1 punto)**
68. Vulnerabilidad.
69. Riesgo.
70. Control.
71. Amenaza.
72. **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ es la probabilidad de que una amenaza en particular explote una vulnerabilidad causando un impacto negativo sobre los activos. (1 punto)**
73. Vulnerabilidad.
74. Riesgo.
75. Control.
76. Amenaza.
77. **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Propiedad que determina que la información no esté disponible, ni sea divulgada a personas, entidades o procesos no autorizados. (1 punto)**
78. Disponibilidad.
79. Integridad.
80. Confidencialidad.
81. Confiabilidad.
82. **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, proceso para asignar valores a la probabilidad y las consecuencias de un riesgo. (1 punto)**
83. Estimación del riesgo.
84. Identificación del riesgo.
85. Evaluación del riesgo.
86. Eliminación del riesgo.
87. **El detalle de los controles de seguridad de la información se encuentran establecidos en la norma \_\_\_\_\_\_\_\_\_\_\_\_. (1 punto)**
88. ISO 27000.
89. ISO 27001.
90. ISO 27002.
91. ISO 27003.
92. **En base a los acontecimientos actuales, donde se ha detectado que se están manipulando las bases de datos del Sistema Nacional de Defunciones (SINADEF), que medidas de seguridad crees que deben implementarse.**

**Indica 4 recomendaciones que permitan garantizar la integridad de la información. (2 puntos)**

|  |
| --- |
| **Política de contraseñas seguras**  **Política de uso dispositivos autorizados**  **Política de sensibilización y concientización**  **Política de acceso a los sistemas de información y aplicaciones**  **Política de auditorías**  **Política de consultorías**  **Política de registros y monitoreo**  **Política de gestión de activos**  **Política de gestión por procesos**  **Política de gestión de riesgos**  **Política de gestión de incidentes**  **Política de continuidad del negocio**  **Política de gestión del cumplimiento**  **Política de transferencia de datos**  **Política de transferencia de informaciones**  **Política de las comunicaciones**  **Retirar del servicio web tradicional todo sistema de información y migrar a los servicios con conectividad VPN y proxys, con dispositivos autenticados.** |