UNIVERSITARIO DE FORMACIÓN	**INSTITUTO SUPERIOR TECNOLÓGICO DE FORMACIÓN PROFESIONAL ADMINISTRATIVA Y COMERCIAL**	
	CÓDIGO:2258	**VERSIÓN: 1**

GUÍA DE CLASES PRÁCTICA DE LA ASIGNATURA	
PROGRAMA: Maestría Tecnológica en Desarrollo e Innovación Digital en Inteligencia de Negocios	**ASIGNATURA:** Seguridad de la Información y Protección de Datos
UNIDADES: Unidad 1: Fundamentos de la Seguridad de la Información. Unidad 2: Marco Legal y Normativo en Protección de Datos. Unidad 3: Gestión de Continuidad y Seguridad en Tecnologías de la Información.	
TÍTULO DE LA CLASE PRÁCTICA: Respaldo y recuperación de información ante una pérdida simulada	
OBJETIVO: Aplicar un procedimiento básico de respaldo y recuperación de archivos y proponer medidas para mantener la continuidad de un proceso empresarial ante una pérdida de información, considerando principios de seguridad, protección de datos y gestión responsable de la información.	
TIEMPO DE DURACIÓN: 64 horas de aprendizaje práctico-experimental (APE).	
MOMENTO DE EJECUCIÓN: La actividad se desarrollará progresivamente durante las tres unidades de la asignatura. En las unidades 1 y 2 se realizarán actividades de fundamentación, análisis y preparación que contribuirán a la ejecución de la prueba de respaldo y recuperación en la Unidad 3. Todas las fases forman parte de una única actividad práctico-experimental y no constituyen actividades ni entregas independientes.	
1. FUNDAMENTOS:	
La presente guía práctica se fundamenta en el PEA de la asignatura **Seguridad de la Información y Protección de Datos** y articula los resultados de aprendizaje de las tres unidades mediante una única actividad práctico-experimental. El análisis de una empresa real, documentada o simulada permitirá al maestrante reconocer los activos de información, las amenazas, las vulnerabilidades y los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de los datos. La actividad integra los fundamentos de seguridad de la información, los principios de protección de datos, los controles de seguridad y la continuidad operativa. A partir de esta fundamentación, el maestrante realizará una prueba controlada de respaldo y recuperación de un archivo con datos ficticios, comprobará la integridad de la información recuperada y propondrá acciones para mantener temporalmente el proceso afectado. La actividad se desarrollará progresivamente durante las tres unidades, con una duración total de **64 horas**, y	

culminará con la presentación de un informe acompañado de evidencias digitales de la prueba realizada. Las fases corresponden a momentos articulados de una única actividad práctico-experimental y no constituyen actividades ni entregas independientes.

2. OBJETIVO A ALCANZAR:

Objetivos cognitivos:

- Analizar los principios de confidencialidad, integridad y disponibilidad de la información.
- Comprender las amenazas, vulnerabilidades y riesgos que pueden afectar los activos de información.
- Interpretar los principios de protección de datos y los fundamentos de continuidad, respaldo y recuperación de información.

Objetivos procedimentales:

- Identificar los activos, amenazas, vulnerabilidades y controles relacionados con un proceso empresarial.
- Aplicar medidas básicas de seguridad y protección de datos.
- Ejecutar una prueba controlada de respaldo y recuperación de un archivo con datos ficticios.
- Comprobar la integridad y disponibilidad de la información recuperada.
- Proponer acciones para mantener temporalmente el proceso y mejorar el procedimiento de respaldo.

Objetivos actitudinales:

- Actuar con ética, responsabilidad y respeto por la privacidad y confidencialidad de la información.
- Demostrar orden, precaución y pensamiento crítico durante la prueba de recuperación.
- Valorar la prevención, la continuidad operativa y el uso responsable de los recursos tecnológicos.

3. BREVE DESCRIPCIÓN DE LAS CAPACIDADES PRÁCTICAS A DESARROLLAR:

Capacidades técnicas: Identificar activos de información, amenazas, vulnerabilidades y riesgos; relacionar los principios de confidencialidad, integridad y disponibilidad; seleccionar controles básicos de seguridad; y aplicar fundamentos de respaldo, recuperación y continuidad operativa.
Capacidades operativas: Crear archivos con datos ficticios, generar y almacenar copias de seguridad, ejecutar una pérdida controlada, recuperar la información desde el respaldo, comprobar su contenido y registrar evidencias digitales del procedimiento realizado.
Capacidades analíticas y de toma de decisiones: Analizar las consecuencias de la pérdida de información, valorar la efectividad del respaldo, identificar debilidades del procedimiento y proponer medidas de protección, continuidad y mejora fundamentadas en los riesgos identificados.
Capacidades comunicativas y actitudinales: Documentar y comunicar los resultados de manera clara, organizar las evidencias y actuar con ética, responsabilidad, precaución, confidencialidad y respeto por la protección de datos y la información organizacional.

4. EVALUACIÓN DEL APRENDIZAJE:

Evidencia principal: Informe en formato PDF sobre la ejecución de una prueba de respaldo y recuperación de información ante una pérdida simulada.
El informe deberá incluir la descripción del proceso empresarial y del archivo seleccionado, las consecuencias de su pérdida, las evidencias del respaldo, la recuperación y la comprobación del contenido, una alternativa para mantener temporalmente el proceso, dos medidas de protección y una reflexión sobre el resultado y la mejora del procedimiento.
Criterios de evaluación:

- Descripción del proceso y comprensión de las consecuencias de la pérdida de información.
- Ejecución correcta de la copia de seguridad y recuperación del archivo.
- Comprobación de la integridad y disponibilidad del contenido recuperado.
- Pertinencia de la alternativa propuesta para mantener temporalmente el proceso.
- Aplicación de medidas de seguridad y protección de la información.
- Claridad y legibilidad de las evidencias digitales presentadas.
- Reflexión sobre los resultados y formulación de una mejora del procedimiento.
- Organización, redacción académica y aplicación de las normas APA, séptima edición.

El informe será valorado sobre **25 puntos**, conforme a la rúbrica establecida en el documento del APE. La evaluación incluirá seguimiento formativo y retroalimentación durante las fases, sin asignar calificaciones independientes a los avances parciales.

5. PREPARACIÓN PREVIA DEL MAESTRANTE:

Antes de iniciar el desarrollo de la actividad, el maestrante deberá:

1. Revisar los contenidos y resultados de aprendizaje de las tres unidades.
2. Consultar la bibliografía básica y de apoyo establecida en el PEA.
3. Seleccionar una empresa real, documentada o simulada y uno de sus procesos.
4. Identificar la información digital utilizada en el proceso y las consecuencias de su posible pérdida.
5. Revisar los principios de confidencialidad, integridad y disponibilidad de la información.
6. Estudiar las amenazas, vulnerabilidades, riesgos y controles básicos de seguridad.
7. Revisar los principios de protección de datos y continuidad operativa aplicables.
8. Preparar un archivo exclusivamente con datos ficticios para realizar la prueba.
9. Seleccionar una ubicación segura y diferenciada para almacenar la copia de respaldo.
10. Verificar la disponibilidad de las herramientas necesarias para crear, respaldar, eliminar y recuperar el archivo.
11. Revisar las instrucciones, el producto esperado y los criterios de evaluación del APE.

6. PROCEDIMIENTOS A EMPLEAR:

La actividad se desarrollará progresivamente durante las tres unidades, con una duración total de **64 horas de aprendizaje práctico-experimental**, distribuidas de la siguiente manera:

Fase 1. Fundamentación y análisis del riesgo – Unidad 1 (16 horas)

- Seleccionar una empresa real, documentada o simulada y uno de sus procesos.
- Identificar la información digital utilizada en el proceso.
- Reconocer los activos de información relacionados.
- Analizar las amenazas y vulnerabilidades que podrían ocasionar la pérdida de información.
- Explicar las consecuencias operativas de la pérdida de un archivo importante.
- Relacionar el caso con los principios de confidencialidad, integridad y disponibilidad.
- Identificar medidas básicas de prevención y protección.

Fase 2. Protección de datos y preparación de la prueba – Unidad 2 (20 horas)

- Analizar los principios de protección de datos aplicables al caso.
- Revisar controles de seguridad relacionados con ISO/IEC 27001 y el marco de ciberseguridad del NIST.
- Seleccionar dos medidas de protección pertinentes.
- Definir una alternativa para mantener temporalmente el proceso ante la pérdida de información.
- Crear un archivo exclusivamente con datos ficticios.
- Seleccionar una ubicación diferenciada para almacenar la copia de seguridad.
- Planificar el procedimiento de respaldo, pérdida simulada, recuperación y comprobación.
- Establecer las evidencias digitales que se registrarán durante la prueba.

Fase 3. Respaldo, recuperación y evaluación – Unidad 3 (28 horas)

- Crear y revisar el archivo con datos ficticios.
- Guardar una copia de seguridad en otra carpeta o ubicación.
- Registrar una captura que evidencie la realización del respaldo.
- Eliminar únicamente el archivo original utilizado para la simulación.
- Recuperar el archivo desde la copia de seguridad.
- Registrar una captura que evidencie la recuperación.
- Abrir el archivo y comprobar que conserva su contenido.
- Registrar una captura de la comprobación realizada.
- Aplicar la alternativa propuesta para mantener temporalmente el proceso.
- Analizar el resultado de la prueba e identificar una mejora del procedimiento.

- Organizar las evidencias e integrar el informe final.

Como producto final, el maestrante presentará un **informe en formato PDF de dos a tres páginas**, sin contar portada y referencias, sobre la prueba de respaldo y recuperación de información ante una pérdida simulada. Las fases forman parte de una única actividad práctico-experimental y no constituyen actividades ni entregas independientes.

7. NORMAS DE SEGURIDAD:

La actividad se realizará exclusivamente con archivos creados para la práctica y con datos ficticios. No se utilizarán archivos originales, información personal, datos confidenciales ni documentos necesarios para el funcionamiento real de una organización. Antes de efectuar la pérdida simulada, se deberá verificar que la copia de seguridad exista, pueda abrirse y se encuentre almacenada en una ubicación diferente.

La eliminación se limitará al archivo de prueba y no deberá ejecutarse sobre carpetas, unidades completas, sistemas institucionales o dispositivos compartidos. El maestrante protegerá sus credenciales, verificará los permisos de acceso, evitará compartir información sensible y conservará una copia adicional hasta comprobar que la recuperación y el contenido del archivo sean correctos.

8. FORMACIÓN EN VALORES Y DESARROLLO DE HABILIDADES BLANDAS.

La actividad promoverá los siguientes valores:

- **Ética profesional:** utilización responsable de la información y de los recursos tecnológicos.
- **Confidencialidad:** protección de los datos y prevención de accesos o divulgaciones no autorizadas.
- **Responsabilidad:** ejecución cuidadosa de los procedimientos de respaldo y recuperación.
- **Integridad:** conservación de la exactitud y consistencia de la información durante la prueba.
- **Prevención:** anticipación de riesgos y adopción de medidas para evitar la pérdida de datos.
- **Respeto por la privacidad:** tratamiento adecuado de la información personal y organizacional.
- **Compromiso con la continuidad operativa:** formulación de acciones que permitan mantener los procesos ante incidentes.

Asimismo, se fortalecerán las siguientes habilidades blandas:

- Pensamiento crítico y analítico.
- Resolución de problemas.
- Toma de decisiones fundamentadas.
- Organización y planificación.
- Comunicación técnica.
- Adaptabilidad ante incidentes.
- Gestión del tiempo.

- Atención al detalle.

9. CONCLUSIONES:

Al finalizar la actividad práctico-experimental, el maestrante habrá desarrollado capacidades para identificar riesgos asociados con la pérdida de información, aplicar principios básicos de seguridad y protección de datos y ejecutar un procedimiento controlado de respaldo y recuperación. Asimismo, podrá comprobar la integridad y disponibilidad de la información recuperada y formular medidas de protección, continuidad operativa y mejora sustentadas en las evidencias obtenidas.

10. RECOMENDACIONES:

- Utilizar exclusivamente archivos creados para la práctica y datos ficticios.
- Verificar la existencia y el funcionamiento de la copia de seguridad antes de eliminar el archivo de prueba.
- Almacenar el respaldo en una ubicación diferente de la utilizada para el archivo original.
- Registrar evidencias claras del respaldo, la recuperación y la comprobación del contenido.
- Evitar la incorporación de datos personales, confidenciales o estratégicos en el informe y las capturas.
- Comprobar la integridad y disponibilidad del archivo después de recuperarlo.
- Relacionar las medidas de protección con los riesgos identificados.
- Proponer una alternativa viable para mantener temporalmente el proceso afectado.
- Fundamentar la mejora del procedimiento en los resultados obtenidos durante la prueba.