INSTRUCCIONES COMPLEMENTARIAS PARA LA EJECUCIÓN DE LOS CURSOS AVANZADOS PARA OFICIALES 2026.

1. La fase a distancia de los Cursos Avanzados para Oficiales se desarrollará bajo una modalidad mixta asincrónica y sincrónica con tutor, ejecutándose de manera descentralizada por cada Instituto, conforme a los cronogramas académicos proporcionados por cada uno de ellos.

   Consecuente con lo anterior, los institutos realizarán, entre otras, las siguientes actividades:

   a. Referido a los jefes de curso

      1) Deberá confeccionar una carpeta con los siguientes antecedentes:
         a) Relación nominal de los alumnos designados a curso.
         b) Cronograma del curso.
         c) Relación nominal de los profesores de cada UA.

      2) Mantendrán contacto permanente con el profesor tutor de cada UA y fiscalizarán que las clases sincrónicas se efectúen conforme a lo planificado.

      3) Efectuará las coordinaciones necesarias con la DIVEDUC (DGA-DEADE), para que el curso se realice sin interferencias.

   b. Referido a las tutorías

      Las tutorías constituyen un componente esencial para el aseguramiento de la calidad del proceso formativo, por lo que el docente tutor deberá ejecutar las instancias sincrónicas en estricta coherencia con las horas asignadas a cada Unidad de Aprendizaje, las que se realizarán en los horarios previamente resguardados y deberán ser comunicadas oportunamente a los alumnos mediante los medios disponibles en la Plataforma Tecnológica Educativa (PTE), tales como correo electrónico, foros y mensajería interna.

   c. Referido a las evaluaciones

      1) Las evaluaciones correspondientes a las Unidades de Aprendizaje serán administradas por los institutos, pudiendo utilizar las facilidades de la PTE 3.0, considerando formalmente la instancia de repetición cuando proceda, conforme a la normativa vigente.

      2) Asimismo, el proceso evaluativo deberá resguardar la validez académica y reglamentaria mediante el reconocimiento de la calificación por parte del alumno en el Sistema de Información de Gestión Educacional (SIGED), de acuerdo con los plazos y procedimientos establecidos institucionalmente.

d. Referido a los instrumentos de evaluación

Los institutos que requieran levantar instrumentos de evaluación en la PTE 3.0 deberán remitirlos directamente al correo electrónico **seade@ejercito.cl**, conforme a las instrucciones anexas al presente documento, adoptando las medidas necesarias para resguardar en todo momento la confidencialidad y seguridad del mismo, en consideración a su carácter reservado dentro del proceso formativo.

e. Referido al apoyo técnico de la PTE.

1) DGA

Control de ejecución de contenidos de acuerdo con los cronogramas.

2) DEADE

Levantar a requerimiento de cada instituto los instrumentos de evaluación para cada aula virtual según a Anexos.

2. Finalmente, conforme a lo expuesto precedentemente, se solicita a US., adoptar las medidas correspondientes, velando por la correcta ejecución de la fase a distancia de los cursos y por la integridad académica de los procesos de evaluación desarrollados en la plataforma institucional.

INSTRUCCIONES PARA LA ELABORACIÓN DE EVALUACIONES EN LA PLATAFORMA TECNÓGICA DEL EJÉRCITO (www.seadepte3.cl)

1. Los instrumentos de evaluación deberán ser remitidos al correo electrónico seade@ejercito.cl, con una semana de anticipación a la fecha en la cual deba quedar disponible para los alumnos.

2. El DEADE tendrá la responsabilidad de cargar en la plataforma el respectivo instrumento de evaluación para que esté disponible en la fecha que haya sido solicitada.

3. El instrumento de evaluación se cargará tal cual como sea enviado por la respectiva escuela, en formato .pdf, por lo que el alumno tendrá a la vista y podrá descargar el respectivo instrumento con el objeto de responder lo que se evalúa.

4. El alumno tendrá la responsabilidad de imprimir, responder y subir en la fecha y hora que se haya determinado como plazo, el instrumento de evaluación respectivo.

5. Lo anterior implica que no habrá automatismo en la corrección del instrumento de evaluación en la PTE 3.0, el cual deberá ser revisado y calificado por el respectivo profesor o tutor de la unidad.

6. El formato para remitir el instrumento de evaluación será el siguiente:

    a. Documento digital (.pdf)
    b. El instrumento de evaluación deberá contener:
        - Membrete de la unidad
        - Identificación del curso
        - Unidad de aprendizaje que se evalúa
        - El número de la Evaluación
        - Fecha y hora de entrega al alumno
        - Fecha y hora de devolución al profesor
        - Instrucciones que debe seguir el alumno para rendir el instrumento de evaluación.
        - Ítems de preguntas propiamente tal.
    c. En el siguiente anexo se muestra un ejemplo del contenido de un instrumento de evaluación tipo.

EJEMPLO DE INSTRUMENTO DE EVALUACIÓN

Membrete de la unidad

Curso Avanzado para Oficiales
Ciberdefensa
Evaluación N.º 1

Fecha y hora de entrega al alumno
15 de mayo de 2026 – 08:00 hrs.

Fecha y hora de devolución al profesor
15 de mayo de 2026 – 10:00 hrs.

INSTRUCCIONES
Lea cuidadosamente las siguientes instrucciones antes de responder el instrumento de evaluación.

1. Explore completamente la evaluación antes de comenzar a responder.
2. Responda todas las preguntas de manera clara y fundamentada cuando corresponda.
3. Utilice lenguaje técnico apropiado conforme a los contenidos estudiados en la unidad de aprendizaje.
4. La evaluación consta de tres ítems:
   - Ítem N.º 1: Preguntas de **Verdadero o Falso**.
   - Ítem N.º 2: Preguntas de **desarrollo breve**.
   - Ítem N.º 3: **Ejercicio aplicado**.
5. El instrumento se evaluará conforme a la siguiente ponderación:
6.

Ítem	Tipo de pregunta	Cantidad	Puntaje por pregunta	Puntaje total
Ítem 1	Verdadero / Falso	10	1 punto	10 puntos
Ítem 2	Desarrollo	5	4 puntos	20 puntos
Ítem 3	Ejercicio aplicado	1	70 puntos	70 puntos

Puntaje total de la evaluación: 100 puntos

6. El tiempo máximo para responder la evaluación es de **90 minutos**.

Ítem N.º 1
Preguntas de Verdadero o Falso
Indique si las siguientes afirmaciones son **Verdaderas (V)** o **Falsas (F)**.

1. La ciberseguridad tiene como objetivo principal proteger la confidencialidad, integridad y disponibilidad de la información.
2. Un firewall permite detectar y eliminar virus informáticos dentro de un sistema operativo.
3. El phishing es una técnica utilizada para engañar a los usuarios y obtener información confidencial.
4. El uso de contraseñas complejas reduce el riesgo de accesos no autorizados.
5. Los ataques de denegación de servicio (DoS) buscan impedir el acceso legítimo a un sistema o servicio.

6. El cifrado de la información permite proteger los datos incluso si estos son interceptados por terceros.
7. La ingeniería social explota vulnerabilidades técnicas exclusivamente del software.
8. La autenticación multifactor incrementa el nivel de seguridad en los sistemas informáticos.
9. El malware es cualquier software diseñado para causar daño o comprometer sistemas informáticos.
10. Las actualizaciones de seguridad del sistema operativo no tienen impacto en la protección frente a ataques cibernéticos.

Ítem N.º 2
Preguntas de desarrollo
Responda brevemente las siguientes preguntas.

1. Explique qué se entiende por **ciberseguridad** y cuál es su importancia en las organizaciones modernas.
2. Describa al menos **tres tipos de amenazas cibernéticas** que pueden afectar a una institución.
3. Explique la diferencia entre **autenticación** y **autorización** dentro de un sistema informático.
4. Describa qué es un **ataque de phishing** y mencione dos medidas para prevenirlo.
5. Explique el concepto de **gestión de vulnerabilidades** dentro de la seguridad informática.

Ítem N.º 3
Ejercicio aplicado
Una unidad militar utiliza un sistema informático para la gestión de información administrativa y logística. En los últimos meses se han detectado los siguientes incidentes:

- Intentos reiterados de acceso no autorizado a cuentas de usuario.
- Recepción de correos electrónicos sospechosos que solicitan credenciales.
- Equipos informáticos que no han sido actualizados durante largos periodos.
- Uso de contraseñas débiles por parte del personal.

En consecuencia:

1. Identifique **al menos cuatro riesgos de ciberseguridad** presentes en la situación descrita.
2. Proponga **cinco medidas concretas de seguridad** que permitan mitigar los riesgos identificados.
3. Explique brevemente cómo la **capacitación del personal** contribuye a mejorar la seguridad de la información.