

PAUTA DE EVALUACIÓN FINAL CON RÚBRICA

1. Antecedentes del participante

Datos Personales

Nombre	:	
Fecha de nacimiento	:	
Rut	:	
Correo electrónico	:	
Teléfono celular	:	
Cargo	:	
Área	:	
Dirección Particular	:	
Comuna y ciudad	:	

2. Antecedentes del OTEC

Nombre del OTEC	:	
Representante Legal	:	
Rut OTEC	:	
Correo electrónico	:	
Teléfono celular	:	
Dirección	:	
Comuna y ciudad	:	

Curso Protocolos Para El Control De Situaciones De Emergencia Laboral Y Desastres Naturales

50 hrs.

Aprendizajes esperados	Contenidos
Identificar fundamentos legales de prevención asociados a accidentes y enfermedades profesionales	Módulo 1: Fundamentos de la Gestión de Emergencias - Conceptos básicos: Definición de emergencia, desastre natural, riesgo, vulnerabilidad. - Marco legal y normativo: Análisis de la legislación laboral y de seguridad industrial aplicable. - Importancia de la prevención: Beneficios de la prevención y preparación ante emergencias.
Describir métodos de análisis de riesgos y vulnerabilidades en situación de riesgo para la empresa.	Módulo 2: Análisis de Riesgos y Vulnerabilidades - Identificación de peligros: Evaluación de los riesgos internos y externos que pueden afectar a la empresa. - Análisis de vulnerabilidades: Identificación de las debilidades de la organización frente a cada tipo de amenaza. - Elaboración de un mapa de riesgos: Visualización gráfica de los riesgos y sus posibles consecuencias.
Reconocer Implementación de Planes de Emergencia considerando psicología de la emergencia	Módulo 3: Desarrollo e Implementación de Planes de Emergencia - Elementos clave de un plan de emergencia: Objetivos, alcance, estructura, responsabilidades, procedimientos, recursos, etc. - Procedimientos de emergencia: Evacuación, primeros auxilios, comunicación, control de activos, etc. - Simulacros: Importancia de los simulacros para evaluar la eficacia del plan y capacitar al personal.
Aplicar gestión de crisis y comunicación dentro de la empresa, considerando el marco legal y la relación con los medios de comunicación	Módulo 4: Gestión de Crisis y Comunicación - Comunicación efectiva: Establecimiento de canales de comunicación internos y externos para informar y coordinar acciones durante una emergencia. - Gestión de crisis: Estrategias para controlar y resolver situaciones críticas. - Relaciones con los medios de comunicación: Manejo de la información y comunicación con los medios durante una emergencia.

Nombre Participante	Rut Participante	Dirección Participante
Nombre OTEC	Nombre Evaluador	Fecha Evaluación

RÚBRICA DE EVALUACIÓN

INSTRUCCIONES DE APLICACIÓN • Debe contestar con lápiz pasta color azul o negro; si requiere hacer una corrección tache la respuesta incorrecta y vuelva a marcar la que considere correcta • Sólo debe utilizar el espacio dispuesto para responder • Cuenta con 60 minutos para responder esta evaluación • Si tiene dudas acerca de la evaluación o alguno de sus puntos, consulte al evaluador sus inquietudes para que le sean aclaradas	PAUTA DE EVALUACIÓN; PUNTAJE TOTAL: 40 PUNTOS		
	AE 1: (ejercicio 1)	Nombre Ítem	Puntaje
		Selección Múltiple	10
	AE 2: (ejercicio 2)	Nombre Ítem	Puntaje
		Juego de Roles	10
	AE 3: (ejercicio 3)	Nombre Ítem	Puntaje
		Estudio de caso	10
	AE 4: (ejercicio 4)	Nombre Ítem	Puntaje
		Resolución de un problema	10
	Criterios de evaluación		
	PUNTAJE MÍNIMO PARA APROBAR: 16 puntos (40% de exigencia)		

AE 1: (ejercicio 1)	Nombre Ítem	Puntaje
	Selección múltiple	10

Instrucciones específicas

Marque con una X la letra de la alternativa que considere correcta.

Ejercicio**1. ¿Cuál de las siguientes definiciones describe mejor el concepto de "emergencia"?**

- a) Una situación controlada que no representa ningún riesgo.
- b) Un evento repentino que requiere una acción inmediata para proteger la salud, la vida, la propiedad o el medio ambiente.
- c) Un fenómeno natural que ocurre periódicamente sin causar daños.
- d) Un estado de tranquilidad sin amenazas.

Respuesta: b) Un evento repentino que requiere una acción inmediata para proteger la salud, la vida, la propiedad o el medio ambiente.

Las emergencias son situaciones imprevistas y críticas que demandan una respuesta rápida y eficiente para evitar o minimizar daños. Esto puede incluir desde desastres naturales, como terremotos e inundaciones, hasta incidentes tecnológicos o humanos, como incendios, accidentes industriales o ataques terroristas. La característica principal de una emergencia es la necesidad de tomar acciones inmediatas para proteger la vida y la salud de las personas, así como la integridad de la propiedad y el entorno.

2. ¿Qué término se refiere a la "posibilidad de que ocurra un evento adverso y sus consecuencias"?

- a) Vulnerabilidad
- b) Riesgo
- c) Desastre natural
- d) Prevención

Respuesta: b) Riesgo

El término "riesgo" se refiere a la **posibilidad de que ocurra un evento adverso y sus consecuencias**. En el contexto de la gestión de riesgos, esto implica la probabilidad de que un peligro o amenaza cause daños a las personas, la propiedad, el medio ambiente o los

procesos de una organización. El riesgo se cuantifica generalmente en función de la probabilidad de que ocurra el evento y la gravedad de sus consecuencias.

3. Según la legislación laboral chilena, ¿cuál de las siguientes leyes se centra en la prevención de accidentes y enfermedades profesionales?

- a) Ley N°19.300 sobre Bases Generales del Medio Ambiente
- b) Ley N°16.744 sobre Accidentes del Trabajo y Enfermedades Profesionales
- c) Ley N°20.123 sobre Subcontratación y Trabajo en Régimen de Subcontratación
- d) Ley N°19.518 sobre Estatuto de Capacitación y Empleo

Respuesta: b) Ley N°16.744 sobre Accidentes del Trabajo y Enfermedades Profesionales

La Ley N°16.744 de la legislación chilena es la que se centra específicamente en la prevención de accidentes y enfermedades profesionales. Esta ley establece el seguro obligatorio contra riesgos de accidentes del trabajo y enfermedades profesionales, define las prestaciones que se deben otorgar y establece las obligaciones tanto de los empleadores como de los trabajadores en materia de prevención de riesgos laborales.

4. ¿Cuál es uno de los beneficios de la prevención y preparación ante emergencias?

- a) Incrementar los costos operativos de la empresa
- b) Reducir el riesgo y minimizar las consecuencias de eventos adversos
- c) Desalentar la implementación de medidas de seguridad
- d) Crear un ambiente de incertidumbre en el lugar de trabajo

Respuesta: b) Reducir el riesgo y minimizar las consecuencias de eventos adversos

Uno de los principales beneficios de la prevención y preparación ante emergencias es precisamente la reducción del riesgo y la minimización de las consecuencias de eventos adversos. Al estar preparados y contar con planes de emergencia bien estructurados, las empresas y organizaciones pueden actuar de manera rápida y efectiva ante situaciones críticas, protegiendo la salud, la vida, la propiedad y el medio ambiente. Esto no solo ayuda a prevenir daños graves, sino que también puede mejorar la resiliencia y la capacidad de recuperación de la organización ante crisis.

Las otras opciones, como incrementar los costos operativos, desalentar la implementación de medidas de seguridad y crear un ambiente de incertidumbre en el lugar de trabajo, no son beneficios de la prevención y preparación ante emergencias y, de hecho, van en contra de los objetivos de estas prácticas.

5. ¿Cuál de los siguientes conceptos se refiere a la "incapacidad para resistir o adaptarse a los efectos de un evento adverso"?

- a) Riesgo
- b) Vulnerabilidad
- c) Desastre natural
- d) Emergencia

Respuesta: b) Vulnerabilidad

El concepto de vulnerabilidad se refiere a la **incapacidad para resistir o adaptarse a los efectos de un evento adverso**. En el contexto de la gestión de riesgos y desastres, la vulnerabilidad se refiere a la susceptibilidad de una comunidad, sistema o activo a sufrir daños debido a un evento adverso. Esto puede estar influenciado por factores como la falta de recursos, infraestructura débil, condiciones socioeconómicas desfavorables y falta de preparación.

AE 2: (ejercicio 2)	Nombre Ítem	Puntaje
	Juego de Roles	10

Instrucciones específicas

Responda cada una de las preguntas ajustándose al espacio asignado.

Ejercicio

Escena: Una reunión en SeguriCorp para el análisis de riesgos y vulnerabilidades

Contexto: Estás en la sala de reuniones con tu equipo directivo y conmigo, tu consultor especializado. En la mesa hay planos del edificio, reportes de ciberseguridad y un mapa de la región. Fuera de la ventana, se siente el bullicio de la planta de producción.

Tú (Responsable de Seguridad): "Gracias a todos por venir. Tenemos varios riesgos potenciales que amenazan la operación de SeguriCorp. Nuestro objetivo es identificarlos claramente, analizar nuestras vulnerabilidades y crear un mapa de riesgos para priorizar acciones. Empecemos con los peligros. ¿Qué tenemos hasta ahora?"

Consultor (yo): "Desde nuestra evaluación inicial, hemos detectado:

1. Desastres naturales, como terremotos, dado que estamos en una región sísmica.
2. Amenazas cibernéticas, incluyendo intentos de hackeo a nuestros servidores.
3. Fugas de materiales químicos en la planta, que podrían tener consecuencias ambientales y operativas.
4. Fallas estructurales detectadas en el edificio principal.

Estos son los principales riesgos identificados, pero quiero escuchar tu perspectiva. ¿Crees que deberíamos considerar algo más?"

Director de Operaciones: "Tal vez deberíamos agregar posibles interrupciones en la cadena de suministro. Si algo falla, podríamos quedarnos sin materiales críticos para la producción."

Tú: (respondes según lo que consideres importante agregar o ajustar).

Pregunta 1: ¿Cuál de los siguientes se considera un riesgo interno en una organización?

- A) Desastres naturales
- B) Fugas de materiales químicos en la planta de producción
- C) Intentos de hackeo desde el exterior
- D) Interrupciones en el transporte público

Respuesta correcta: B) Fugas de materiales químicos en la planta de producción.

Las fugas de materiales químicos en la planta de producción se consideran un riesgo interno porque ocurren dentro de la propia organización y están bajo su control. Este tipo de riesgos son el resultado de operaciones internas y factores que la empresa puede gestionar directamente, como la seguridad de los procesos, el mantenimiento de equipos y la capacitación del personal.

Por otro lado, los desastres naturales (A), los intentos de hackeo desde el exterior (C) y las interrupciones en el transporte público (D) son riesgos externos, ya que provienen de fuentes fuera del control directo de la organización. Aunque la empresa debe estar preparada para enfrentarlos, no puede prevenir su ocurrencia de la misma manera que puede hacerlo con los riesgos internos.

Pregunta 2: ¿Qué herramienta se utiliza para visualizar gráficamente los riesgos y sus consecuencias?

- A) Análisis FODA
- B) Auditoría externa
- C) Mapa de riesgos
- D) Plan de continuidad

Respuesta correcta: C) Mapa de riesgos.

Un mapa de riesgos es una herramienta utilizada para visualizar gráficamente los riesgos y sus consecuencias en una organización. Este tipo de mapa ayuda a identificar, evaluar y priorizar los riesgos, permitiendo a la organización tomar decisiones informadas sobre cómo manejarlos. Al representar los riesgos de manera visual, se facilita la comprensión de su impacto potencial y se pueden desarrollar estrategias efectivas para mitigarlos.

Las otras opciones, aunque útiles en otros contextos, no son herramientas específicas para visualizar los riesgos y sus consecuencias de manera gráfica:

- **Análisis FODA (A)** se utiliza para identificar fortalezas, oportunidades, debilidades y amenazas.
- **Auditoría externa (B)** se emplea para evaluar la conformidad y eficiencia de las operaciones y controles internos.
- **Plan de continuidad (D)** es un plan para mantener las operaciones críticas durante y después de una crisis.

Pregunta 3: ¿Qué aspecto se evalúa al analizar las vulnerabilidades de una organización?

- A) Las políticas de seguros disponibles
- B) Las debilidades que pueden facilitar el impacto de una amenaza
- C) El tipo de amenaza externa más probable
- D) La percepción de los empleados sobre los riesgos

Respuesta correcta: B) Las debilidades que pueden facilitar el impacto de una amenaza.

Al analizar las vulnerabilidades de una organización, se busca identificar las debilidades internas que pueden hacerla más susceptible al impacto de una amenaza. Estas debilidades pueden incluir aspectos como falta de capacitación adecuada, deficiencias en la infraestructura, insuficiencia de recursos, problemas en los procesos operativos, entre otros. Evaluar estas vulnerabilidades es fundamental para desarrollar estrategias de mitigación y mejorar la resiliencia de la organización ante posibles riesgos.

Las otras opciones, aunque pueden ser relevantes en otros contextos, no son el enfoque principal al analizar las vulnerabilidades:

- **Las políticas de seguros disponibles (A)** están más relacionadas con la protección financiera ante riesgos.

- **El tipo de amenaza externa más probable (C)** se refiere a la identificación de riesgos, no a la vulnerabilidad en sí.
- **La percepción de los empleados sobre los riesgos (D)** es útil para la cultura organizacional, pero no es el principal aspecto al analizar vulnerabilidades.

AE 3: (ejercicio 3)	Nombre Ítem	Puntaje
	Estudio de caso	10

Instrucciones específicas

Lea atentamente el siguiente estudio de caso y responda cada pregunta asociada en el espacio consignado.

Ejercicio

Escenario:

Estudio de Caso:

La empresa "Seguridad S.A." se dedica a la manufactura de productos químicos y recientemente ha decidido mejorar sus planes de emergencia. Tras una evaluación de riesgos, la empresa ha identificado varios peligros potenciales, incluidas fugas de sustancias peligrosas, incendios y explosiones. La dirección ha decidido implementar un plan de emergencia y ha asignado responsabilidades claras a cada miembro del equipo. Además, se han planificado simulacros periódicos para asegurar la preparación del personal.

Pregunta 1: ¿Qué es un análisis de vulnerabilidades?

- A) Un proceso para identificar las debilidades de la organización frente a amenazas específicas
- B) Un informe sobre los logros financieros de la empresa
- C) Una revisión de los productos que ofrece la competencia
- D) Un plan de evacuación en caso de emergencia

Respuesta correcta: A) Un proceso para identificar las debilidades de la organización frente a amenazas específicas.

Un análisis de vulnerabilidades es un proceso sistemático para identificar y evaluar las debilidades dentro de una organización que podrían ser explotadas por amenazas específicas. Este análisis es fundamental para la gestión de riesgos, ya que permite a la organización identificar áreas que necesitan ser fortalecidas y desarrollar estrategias para mitigar posibles impactos negativos.

Las otras opciones no se relacionan con el concepto de análisis de vulnerabilidades

Pregunta 2: ¿Cuál de los siguientes NO es un tipo de amenaza externa para una empresa?

- A) Terremotos
- B) Hackeo de datos por un agente externo
- C) Fugas de información interna por empleados
- D) Inundaciones

Respuesta correcta: C) Fugas de información interna por empleados.

Las fugas de información interna por empleados se consideran una amenaza interna porque provienen del interior de la organización. Este tipo de amenazas surgen debido a la acción de los empleados que, ya sea intencionalmente o por descuido, divulgan información sensible de la empresa.

Por otro lado, los terremotos (A), el hackeo de datos por un agente externo (B) y las inundaciones (D) son amenazas externas. Los terremotos y las inundaciones son eventos naturales que están fuera del control directo de la organización. El hackeo de datos por un agente externo es una amenaza cibernética que proviene de fuera de la organización.

Pregunta 3: ¿Por qué es importante elaborar un mapa de riesgos?

- A) Para reducir los costos de los productos
- B) Para visualizar los riesgos y priorizar las estrategias de mitigación
- C) Para comparar la empresa con los competidores
- D) Para eliminar cualquier posibilidad de amenaza

Respuesta correcta: B) Para visualizar los riesgos y priorizar las estrategias de mitigación.

Elaborar un mapa de riesgos es importante porque permite a la organización visualizar de manera clara los riesgos a los que está expuesta y priorizar las estrategias necesarias para mitigarlos. Un mapa de riesgos ayuda a identificar cuáles son los riesgos más críticos y cuáles podrían tener un mayor impacto en la organización. Con esta información, se pueden asignar recursos de manera más eficiente y desarrollar planes de acción específicos para reducir la probabilidad y el impacto de dichos riesgos.

AE 4: (ejercicio 4)	Nombre Ítem	Puntaje
	Resolución de un problema	10

Instrucciones específicas

Complete según corresponda

Ejercicio**Ejercicio: El caso de "DataSafe Ltd."**

"DataSafe Ltd." es una empresa dedicada al almacenamiento de datos sensibles de clientes. Recientemente, experimentaron un intento de hackeo que no tuvo éxito, pero reveló varias debilidades en su sistema de seguridad cibernética. Por otro lado, su sede está ubicada en una zona con alto riesgo de inundaciones y la última auditoría identificó fallas estructurales en el edificio, como un sistema de drenaje obstruido y techos en mal estado.

La tarea de la empresa es analizar los riesgos y vulnerabilidades relacionados con:

1. La ciberseguridad.
2. La infraestructura del edificio.
3. La posibilidad de inundaciones.

Como parte del equipo encargado de resolver este problema, responde las siguientes preguntas:

Pregunta 1: ¿Qué acción inmediata debería tomar "DataSafe Ltd." para reducir el riesgo cibernético?

- A) Contratar personal especializado en ciberseguridad.
- B) Cambiar la ubicación de la empresa a una zona con menos riesgo de inundaciones.
- C) Ignorar el intento de hackeo porque no tuvo éxito.
- D) Mejorar el sistema de drenaje del edificio.

Respuesta correcta: A) Contratar personal especializado en ciberseguridad.

Contratar personal especializado en ciberseguridad es una acción inmediata y fundamental para "DataSafe Ltd." que mejorará su capacidad para detectar, prevenir y responder a ciberataques. Este personal puede implementar medidas de protección más robustas, llevar a cabo auditorías de seguridad regulares y capacitar al personal existente sobre las mejores prácticas en ciberseguridad.

Pregunta 2: ¿Cuál es la principal vulnerabilidad en la infraestructura de "DataSafe Ltd." identificada en la auditoría?

- A) Ausencia de protocolos de seguridad en caso de hackeo.
- B) El sistema de drenaje obstruido y los techos en mal estado.
- C) La falta de entrenamiento del personal en gestión de datos.
- D) La ubicación en una zona con alto riesgo de inundaciones.

Respuesta correcta: B) El sistema de drenaje obstruido y los techos en mal estado.

La auditoría identificó problemas específicos en la infraestructura del edificio de "DataSafe Ltd.", a saber, un sistema de drenaje obstruido y techos en mal estado. Estas vulnerabilidades estructurales son críticas porque pueden agravar el riesgo de daños en caso de inundaciones, especialmente considerando que la empresa está ubicada en una zona con alto riesgo de este tipo de desastres naturales. Abordar estos problemas es fundamental para garantizar la integridad del edificio y proteger los datos sensibles almacenados.

Pregunta 3: ¿Qué medida debería priorizar "DataSafe Ltd." para abordar el riesgo de inundaciones?

- A) Instalar barreras contra inundaciones y reparar los sistemas de drenaje.
- B) Optimizar los servidores para procesar más datos en menos tiempo.
- C) Cambiar todo su personal de tecnología.
- D) Ignorar el riesgo porque las inundaciones son poco frecuentes.

Respuesta correcta: A) Instalar barreras contra inundaciones y reparar los sistemas de drenaje.

Para "DataSafe Ltd.", una empresa ubicada en una zona con alto riesgo de inundaciones, es crucial priorizar las medidas que directamente aborden y mitiguen este riesgo. Instalar barreras contra inundaciones y reparar los sistemas de drenaje son acciones esenciales para proteger la infraestructura del edificio y garantizar la seguridad de los datos sensibles almacenados. Estas medidas ayudarán a evitar que el agua entre en las instalaciones, minimizando los daños potenciales durante una inundación.

