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.

COMPROMISO ÉTICO:

YO, ____aldo puchuri galindo_____ con DNI __77495303_____ 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. **CONTENIDO DE LA EVALUACIÓN:**
   1.1. (10 PUNTOS)

   Usted trabajar a una empresa de servicios de TI y el dueño de la compañía le comenta que como parte de su plan estratégico ha decidido aplicar a la certificación del estándar ISO 27000 para lo cual le encarga la misión de elaborar un documento de política de seguridad de la información para su empresa en donde este deberá tener como mínimo las siguientes las partes:

   - Resumen
   - Introducción
   - Ámbito de aplicación
   - Objetivos
   - Principios
   - Responsabilidades
   - Resultados importantes
   - Políticas relacionadas

   Desarrolle cada uno de los puntos mencionados para su empresa.

Resumen

La Política de Seguridad de la Información establece los principios y directrices para proteger la confidencialidad, integridad y disponibilidad de los activos de información de nuestra organización.

Introducción

La seguridad de la información es fundamental para garantizar la continuidad del negocio y la confianza de nuestros clientes y socios. Esta política define nuestro compromiso con la seguridad y establece las responsabilidades de todos los empleados.

Ámbito de Aplicación

Esta política se aplica a todos los empleados, contratistas, proveedores y terceros que interactúan con los sistemas y datos de nuestra empresa.

Objetivos

Nuestra política tiene como objetivo establecer los requisitos para proteger la confidencialidad de la información, salvaguardar la integridad de los datos y garantizar la disponibilidad de los sistemas y servicios.

Principios

Los siguientes principios guían nuestras decisiones de seguridad:

Confidencialidad:

- **Acceso restringido solo a usuarios autorizados.**
- **Encriptación de datos confidenciales**
- **Política de clasificación y manejo de la información.**

Integridad:

- **Mantenimiento de la precisión y consistencia de los datos.**

Disponibilidad:

- **Garantía de acceso oportuno y continuo a los recursos.**
- **Planificación de contingencias y recuperación ante desastres.**

Responsabilidades

Dirección

- **Proporciona liderazgo y recursos para implementar medidas de seguridad.**
- **Aprobar y respaldar la política.**

Equipo de Seguridad

- **Supervisa y ejecuta las políticas y controles.**
- **Evaluar riesgos y actualizar la política.**

Empleados

- **Cumplen con las políticas y reportan incidentes de seguridad.**
- **Reportar incidentes de seguridad**

Resultados Importantes

- **Reducción de incidentes de seguridad.**
- **Mayor conciencia de seguridad entre los empleados.**

Políticas Relacionadas

- **Política de Acceso y Control de Usuarios.**
- **Política de Clasificación de Información.**

1.2. (10 PUNTOS)

Usted labora en un organismo gubernamental y como parte del proceso de auditoría ISO 27000 la empresa auditora le solicita que les envíen como evidencia el formato del Control de Cambios que manejan con los 5 últimos cambios que han realizado en su institución para su verificación, los campos mínimos que debe tener su formato son los siguientes:

- Nombre del Sistema
- Fecha
- Paginación
- Descripción del cambio
- N° de solicitud de cambio
- Aprobado por
- Fecha de Aprobación
- Comentarios

Desarrolle un cuadro con el formato de control de cambios con los registros de los 5 últimos cambios realizados.

NOMBRE DEL PROYECTO	Proyecto Gurmanental			FECHA DE CREACIÓN	19/05/2023		
Nombre del Sistema	**Fecha**	**Paginacion**	**Descripcion del cambio**	**N de solicitud de cambio**	**Aprobado por•**	**Fecha de Aprobación**	**Comentarios**
Actividad 1	30/06/2023	pag 1/3	Actualización de parches	SC-001	Guillermo Torrez	25/07/2023	Cambio aplicado sin problemas.
Actividad 2	23/07/2023	pag 2/4	Actualizacion de nuevos usuarios	SC-002	Juan Pérez	13/08/2023	Se verificó la correcta implementación.
Actividad 3	10/08/2023	pag 1/2	Actualización de software	SC-003	Angel Vazques	10/09/2023	Usuario autorizado por Recursos Humanos.
Actividad 4	14/01/2024	pag 1/5	Cambio en la política de contraseñas	SC-004	Juan Pérez	3'0/01/2024	Cambios comunicados a todos los usuarios.
Actividad 5	12/03/2024	pag 1/6	Implementación de nueva funcionalidad	SC-005	Ricado Gonzales	12/04/2024	Se verificó la integridad de los datos.