Unidad # 2
Seguridad de los Datos

Administración de Bases de Datos II

Gisela Yasmín García Espinoza

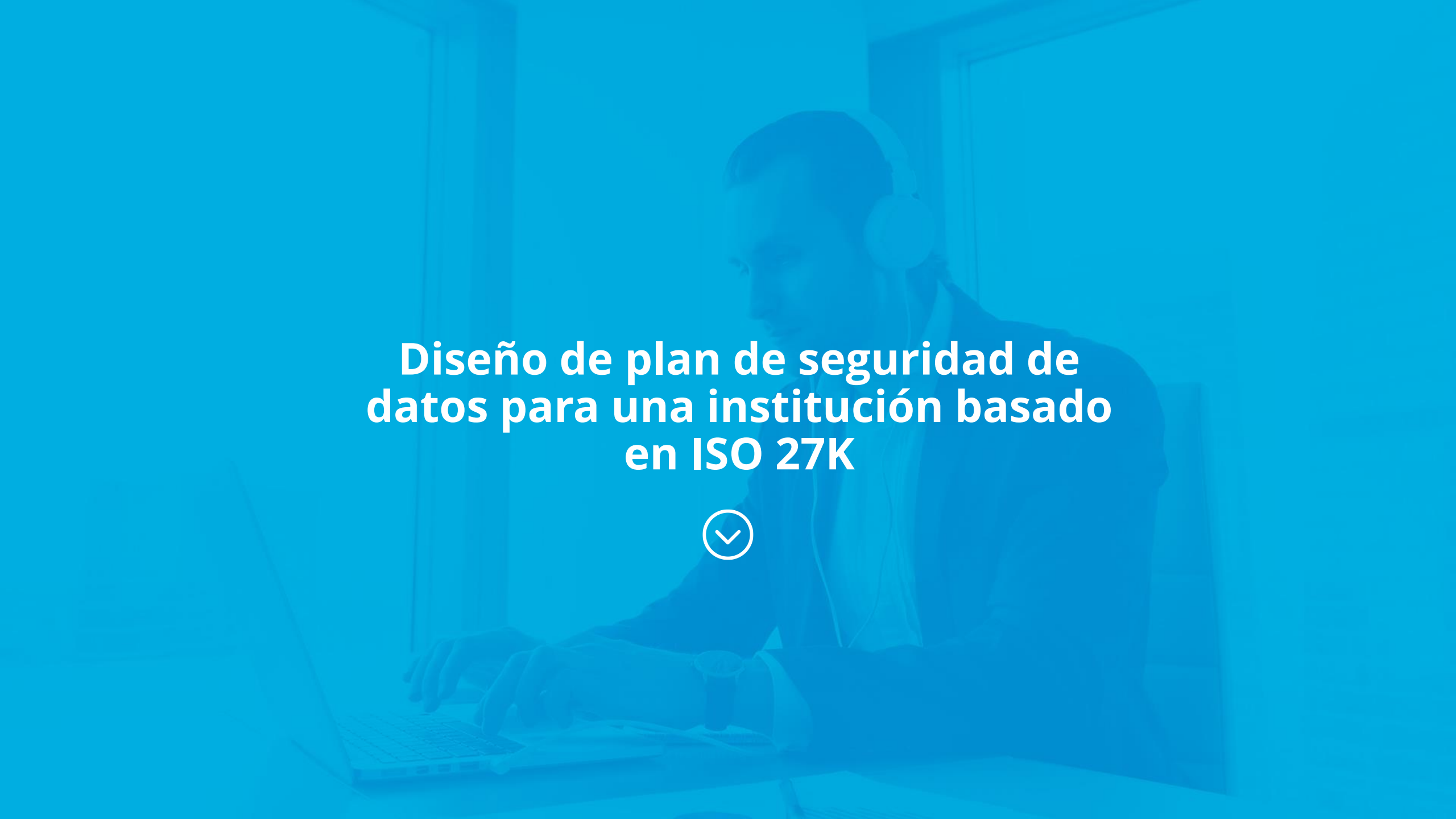
Competencia de la asignatura

Crear bases de datos no relacionales y consistentes para almacenar la data empresarial aplicando la metodología del diseño, gestión de base de datos, lenguaje No SQL y considerando las reglas de negocios desarrolladas de manera individual y colaborativa.

Contenidos a desarrollar

- ¿Qué es un plan de seguridad?
- Protocolos de seguridad de la información
- Sistema de gestión de seguridad de la información, según la norma ISO 27001

Diseño de plan de seguridad de datos para una institución basado en ISO 27K



¿Qué es un plan de seguridad?

Un plan de seguridad de la información es la documentación del plan de una empresa y los sistemas implementados para proteger la información personal y los datos confidenciales de la empresa. Este plan puede mitigar las amenazas contra una organización, así como ayudar a la empresa a proteger la integridad, confidencialidad y disponibilidad de sus datos.

¿Por qué es importante un plan de seguridad?

En el cambiante panorama regulatorio e inversor de hoy, los planes de seguridad de la información son fundamentales para que las empresas cumplan con las regulaciones, las solicitudes de diligencia debida de los inversores y las leyes estatales. Además, las amenazas a la ciberseguridad son cada vez más comunes y sofisticadas. Además de proteger la integridad de sus datos y mantenerlos confidenciales.

Protocolos de seguridad de la información

Estos protocolos se diseñaron con el fin de prevenir que agentes externos no autorizados puedan tener acceso a estos datos y están compuestos por:

- **Cifrado de datos:** cuando el mensaje es enviado por el emisor lo que hace es ocultar la información hasta que esta llegue al receptor.
- **Lógica:** debe contar con un orden en el que primero van los datos del mensaje, el significado y en qué momento se va a enviar este.
- **Autenticación:** esta técnica se utiliza para saber que la información está siendo manipulada por un ente autorizado y no está sufriendo algún tipo de intervención por agentes externos.

Sistema de gestión de seguridad de la información, según la norma ISO 27001

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye la norma ISO 27001. De acuerdo con la norma, la seguridad de la información consiste en la preservación de la confidencialidad, integridad y disponibilidad; bajo estos tres términos se realiza el análisis y evaluación de los activos de información.

Sistema de gestión de seguridad de la información, según la norma ISO 27001

Disponibilidad	Confidencialidad	Integridad	Autenticación
Tener acceso a la información necesaria. En este punto es importante evitar que el sistema tenga problemas o que algún ente externo intente acceder de manera ilícita a los programadores de la compañía.	Información que solo está disponible para el personal autorizado, por ende esta no debe ser distribuida por terceros.	La información que está registrada debe ser la correcta y no contar con errores o algún tipo de modificaciones. Esto se hace con el fin de evitar amenazas externas o errores humanos.	Esta información la brinda directamente un usuario y se debe validar que los datos otorgados son los correctos.

Fuente: https://www.piranirisk.com/es/academia/especiales/manual-para-implementar-la-seguridad-de-la-informacion-segun-la-iso-27001

Este proceso permite garantizar que se está gestionando de manera adecuada la seguridad de la información, debe ser documentado y registrado para que toda la organización tenga conocimiento del mismo y sepa cómo actuar frente a situaciones de posible amenaza.

¿Para que sirve?

La información de una compañía es uno de los activos más importantes que se tiene, es por esto que es tan indispensable protegerla, ya que esta es esencial para el cumplimiento de los objetivos.

Un SGSI es un instrumento de gran ayuda para cumplir con la legalidad y la protección de los datos, pues este permite que se definan los procedimientos y controles que se llevarán a cabo para mantener los datos blindados. Además, permite que se establezcan las políticas que se le darán a conocer a todos los miembros de la organización y saber a profundidad cuáles son los riesgos que pueden sufrir y de qué manera pueden mitigarlos.

¿Que incluye?

- **Manual de seguridad:** este es el documento el cual contiene la guía de cómo se debe implementar y seguir el sistema de gestión de seguridad de la información. Allí se va a radicar toda la información como objetivos, alcance, responsables, políticas, directrices, entre otras actividades que se decidan llevar a cabo.
- **Procedimientos:** estos van relacionados a las actividades operativas, ya que estos serán los encargados de dar los parámetros que se deben seguir para que la gestión sea eficaz, la planificación, la operación y el control sean los adecuados en los procesos de seguridad de la información.
- **Instrucciones:** es la descripción de lo que se debe hacer paso a paso, cuáles son las tareas y actividades que se deben cumplir para que la gestión sea eficiente.
- **Registros** es la evidencia de la información que ha sido documentada a lo largo de la gestión, para verificar que se estén cumpliendo con los objetivos propuestos.

Pasos a seguir para su elaboración

- Apoyo de la alta gerencia, directores y junta directiva.
- Establecer la metodología que se va a implementar.
- Definir el alcance del SGSI.
- Redactar una política de seguridad de la información.
- Definir evaluación de riesgos.
- Llevar a cabo la evaluación y el tratamiento de riesgos.
- Dar a conocer cómo va ser su aplicabilidad.
- Tener claro el plan de tratamiento de riesgos.
- Definir cómo se medirá la efectividad de los controles.
- Implementar todos los controles y procedimientos necesarios.
- Crear cultura dentro de la empresa a través de programas de
- capacitación y concientización.
- Monitorear y medir el SGSI para verificar si está siendo efectivo.
- Hacer auditoría interna.
- Si hay que hacer mejoras en algunas de las fases ponerlo
- en práctica.

Pasos a seguir para su elaboración

- **Definir la política de seguridad:** aquí se deben determinar los objetivos, el marco general , los requerimientos legales, los criterios con los que serán evaluados los riesgos y para esto se debe establecer la metodología, y estar aprobada por la dirección o junta directiva.
- **Definir el alcance del SGSI:** que se logrará una vez se ponga en marcha el plan de acción dentro de la organización teniendo en cuenta los activos, las tecnologías y descripción de cada uno de ellos.
- **Identificación de los riesgos:** reconocer las posibles amenazas a las que puede estar expuesta la compañía, quienes son los responsables directos, a qué son vulnerables y cuál será el impacto en caso de que se llegue a violar la confidencialidad, integridad y disponibilidad de los activos. 4. Análisis y evaluación de los riesgos: evaluar el impacto que tendría alguno de los riesgos si se llega a materializar, identificar cuál es la probabilidad de ocurrencia y cómo esto podría afectar a los controles que ya están implementados, de igual manera verificar si se puede aceptar o debe ser mitigado.

Pasos a seguir para su elaboración

- **Tratamiento de riesgos:** aplicar los controles adecuados, clasificar los niveles de riesgo, evitarlo si es posible o transferirlo a terceros si es posible.
- **Aplicabilidad:** establecer los objetivos de control y seleccionar los controles que se van a implementar.
- **Gestión:** definir cómo será el tratamiento de los riesgos, aplicar este tratamiento teniendo en cuenta los controles que fueron identificados, y las responsabilidades de cada uno, implementar estos controles, definir el sistema de métricas, generar conciencia dentro de la oficia y fomentar una cultura que permita que todos los empleados tenga conocimiento de SGSI, gestionar su operación y utilizar los recursos necesarios para su cumplimiento.
- **Monitoreo:** revisión periódica del SGSI para identificar si se está cumpliendo con la normativa, con los objetivos planteados y la efectividad de la misma, así mismo como reportar las mejoras que se deben hacer y cuáles serán las acciones que se van a llevar a cabo para lograr esto.

Ventajas de implementar la norma ISO 27001

- Permite que los procesos de seguridad estén equilibrados y a la vez coordinados entre sí.
- Aunque es imposible reducir a cero el riesgo si da la oportunidad de que se creen metodologías que contribuyan a la mitigación de los mismos y a aumentar la seguridad en la información que se tiene.
- En caso de que se llegue a presentar un riesgo permite que este no cause pérdidas tan profundas y que se cuente con un plan de acción para actuar de manera eficaz.

Ventajas de implementar la norma ISO 27001

- Permite que se cumplan con los requerimientos legales exigidos por los entes de control.
- Genera valor agregado dentro de la compañía, pues cabe resaltar que no son muchas las empresas que cuenten con esta certificación.
- Gracias a la eficiencia que se emplea permite reducir costos.
- Genera confianza con todos los miembros de la entidad, ya sean clientes, proveedores o empleados.

Ventajas de implementar la norma ISO 27001

- Da la posibilidad de que se puedan activar alertas en caso de que se llegue a presentar alguna actividad sospechosa.
- Permite hacerles seguimiento a los controles de seguridad.
- Es una herramienta que da la posibilidad de planificar y darle seguimiento a los procesos.

Ventajas de implementar la norma ISO 27001

- Contribuye a la imagen corporativa (reputación).
- Contar con una metodología clara y eficaz.
- Reduce el riesgo de pérdida o robo de la información.

Tabla de actividades	
Nombre de la actividad	Seguridad de información
Tipo de actividad	Tarea
Tipo de participación	En equipos (5 integrantes)
Competencias especifica de la asignatura	Crear bases de datos no relacionales y consistentes para almacenar la data empresarial aplicando la metodología del diseño, gestión de base de datos, lenguaje No SQL y considerando las reglas de negocios desarrolladas de manera individual y colaborativa.
Instrucciones	Después de haber dado lectura a los contenidos de la semana y participar activamente en la video conferencia, deberá presentar un avance de la creación de un plan de seguridad según norma ISO 27k, de acuerdo con indicaciones del docente.
Fecha de entrega	La fecha límite de participación será el domingo al final de la semana, a las 11:59 p.m.
Instrumento de evaluación	Rúbrica
Ponderación	

Recursos Complementarios		
Recurso	Título	Cita Referencial
Sitio Web	ISO 27000 y el conjunto de estándares de Seguridad de la Información	https://www.intedya.com/internacional/intedya-noticias.php?id=757
Sitio Web	¿Qué es norma ISO 27001?	https://advisera.com/27001academy/es/que-es-iso-27001/

¿Preguntas?

¡Muchas gracias!

UNIVERSIDAD GERARDO BARRIOS
Líderes en Gestión del Conocimiento

Comisión de Acreditación de la Calidad de la Educación Superior
UNIVERSIDAD GERARDO BARRIOS (UGB)
ACREDITADA
2019- 2024