Actividad:

Modelos conceptual y lógico para el proyecto desarrollo de software

GA4-220501095-AA1-EV02

Aprendiz:

Wilmer Jair Espinosa Silva

CC: 1.095.910.391

Instructor:

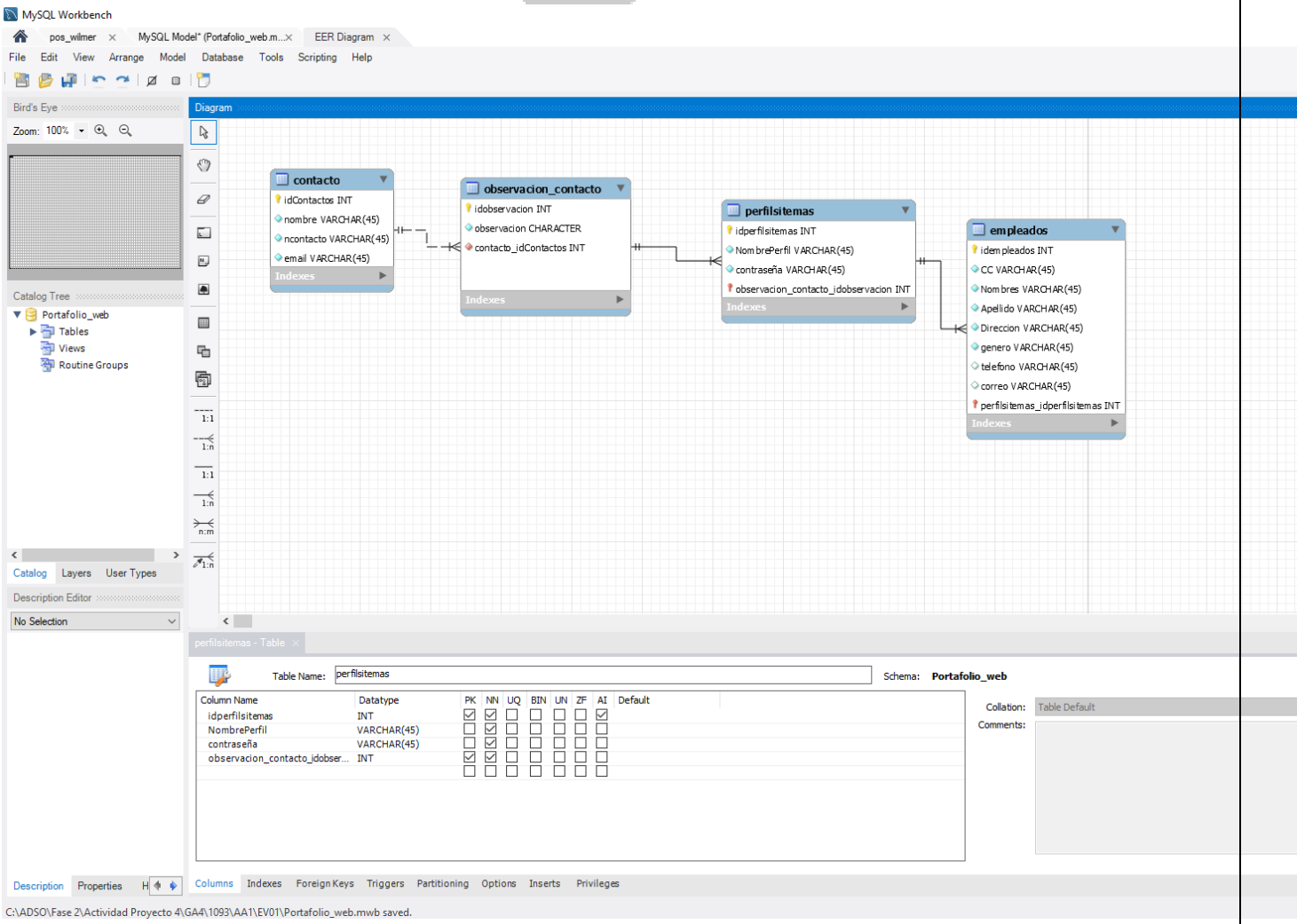
ISRAEL ARBONA GUERRERO

Servicio Nacional de aprendizaje-SENA

Curso: TECNOLOGÍA EN ANÁLISIS Y DESARROLLO DE SOFTWARE

Ficha: 2455285

- Generar el modelo lógico de acuerdo con la técnica seleccionada
- Normalizar el modelo lógico de acuerdo con el tipo de base de datos.



● Tener en cuenta el tipo de base de datos seleccionada.

RTA: Hasta el momento la Base de datos que deseo utilizar en MYSQL o en su defecto POSTGRESQL todo se basa a las necesidades de mi portafolio WEB pero por el momento lo que tengo planteado es guna de estas dos BD.

- Crear el diccionario de datos según el modelo lógico.

Campo	Longitud	Tipo de Dato	Descripción
ID	18	Auto numérico	Clave única de las tablas auto incremental
Nombre	45	Carácter	Nombre del cliente
Ncontacto	45	Numérico	teléfono del cliente
email	45	Carácter	Email del cliente
Observacion	70	Carácter	Comentario de lo que se requiere o lo que necesite expresar el mismo cliente
NombrePerfil	45	Carácter	Nombre del perfil para la pagina
Contraseña	45	Carácter	Este campo estará encriptado para la contraseña del perfil
CC	45	Numerico	En este campo digitara el numero de documento del empleado para el perfil
Nombres	45	Carácter	En este campo digitamos los nombres del empleado al cual se creo el perfil
Apellidos	45	Carácter	En este campo digitamos los Apellidos del empleado al cual se creo el perfil
Dirección	45	Carácter	En este campo digitamos la dirección del empleado al cual se creo el perfil
Genero	45	Carácter	En este campo digitamos el genero del empleado al cual se creo el perfil

Teléfono	45	Carácter	En este campo digitamos el numero del teléfono del empleado al cual se creo el perfil
Correo	45	Carácter	En este campo digitamos el correo electrónico del empleado al cual se creo el perfil

POLÍTICAS GENERALES PARA USUARIOS DE LOS ACTIVOS DE INFORMACIÓN

RESPONSABILIDAD DE LOS EMPLEADOS RESPECTO AL CONTROL DE ACCESO A LOS SISTEMAS

Declaración de la Política:

Todo empleado al que se le otorgue un código de usuario (o login), con su respectiva contraseña, o cualquier otra forma de acceso autorizado, es responsable de su uso y protección, estos son únicos e intransferibles.

Objetivo:

Establecer la responsabilidad de los empleados respecto al uso y protección de los códigos de usuarios/contraseñas y otros modos de autenticación asignadas para acceder a los sistemas y aplicaciones de la Empresa. Criterios para la implementación de la política:

- Concientizar la no divulgación de las credenciales de conexión a los diferentes sistemas de la Empresa por parte de los empleados.
- Sólo está permitido el uso de IDs genéricos cuando existen otros controles establecidos (por ejemplo, usuarios de conexión a sistemas, usuarios de mayor privilegio, entre otros).

Alcance:

Esta política va dirigida a la Gerencia de Seguridad de la Información y a todo el personal, que haga uso de sistemas de información y equipos que requieran contraseñas y otros modos de autenticación para su acceso.

ACCESO REMOTO A LA RED

Declaración de la Política:

El acceso remoto a la red y a los recursos de la empresa será permitido sólo cuando los usuarios autorizados son autenticados, la información viaje encriptada a través de la red y los privilegios sobre la misma sean restringidos.

Objetivo:

Proporcionar medios de acceso seguros desde y hacia fuentes externas acordes con el valor de la información que estará expuesta a través de la red. Utilizando medios seguros, tales como la Red Privada Virtual o Virtual Private Network, el cual proporciona el acceso a través de las redes públicas.

Criterios para la implementación de la política:

• Asegurar el acceso a la red interna al personal autorizado y autenticado por los mecanismos de control.

• Asegurar la confidencialidad de los datos e información transmitidos entre los usuarios remotos y la red interna a través de técnicas de cifrado. Alcance: Esta política va dirigida a la Gerencia de Seguridad de la Información y a los usuarios que reciben autorización para tener acceso remoto a la red.

Responsabilidades:

• Todos y cada uno de los Gerentes, Coordinadores y/o Supervisores , deben asegurar que el personal bajo su cargo, que reciba autorización de acceso remoto a la red de la empresa, conozca y le dé cumplimiento a esta política.

• Todo usuario que tenga asignado un equipo de computación tiene responsabilidad directa en el cumplimiento de las políticas de seguridad.

• Es Responsabilidad de la Gerencia de Tecnología de la Información proporcionar canales de comunicación seguros.

PROCESAMIENTO DE INFORMACIÓN Y USO DEL INTERNET USO DEL CORREO ELECTRÓNICO Y LOS RECURSOS INFORMÁTICOS

Declaración de la Política:

El correo electrónico y los recursos informáticos deben ser utilizados solo para los propósitos de la empresa y deben tomarse las previsiones de seguridad requeridas para la protección de la información de la empresa. Objetivo: Establecer normas en el uso del correo electrónico y los recursos informáticos, asegurando la confidencialidad e integridad del contenido del correo y en los dispositivos de almacenamiento de los recursos informáticos, evitando el mal uso del mismo y de los recursos tecnológicos en la red interna.

Criterios para la implementación de la política:

• Definir los requisitos para la revisión periódica de los controles de acceso.

• Indicar los requisitos para la autorización formal de las solicitudes de acceso.

• Señalar los perfiles de acceso de usuario normales para los roles de trabajo regulares en la organización.

• Controlar el envío de correos electrónicos tanto en la red interna de la empresa como por líneas públicas inseguras que puede comprometer la confidencialidad y la integridad de la información transmitida.

• El envío de copias de archivos a los colegas en la red interna, crea duplicados innecesarios y también compromete la integridad del documento y/o archivo original.

• La recepción, la falta de detección, y la introducción de virus, no sólo puede dañar los sistemas y datos propios, sino que también pueden distribuirse a través de la red de la empresa, originando impactos mayores.