**Actividad: Creando, Gestionando Cuentas y Restringiendo Accesos**

|  |  |  |
| --- | --- | --- |
| **Sigla** | **Nombre Asignatura** | **Tiempo Asignado** |
| **BDY1102** | BASE DE DATOS APLICADA II | 5 h pedagógicas |

**1.** **Instrucciones generales para el/la estudiante**

El docente deberá desarrollar y explicar, durante las horas de clases, los requerimientos 1 incluyendo la creación de los usuarios **BDY1102\_P9\_1, BDY1102\_P9\_3 y las acciones respectivas, para** que posteriormente cada estudiante genere las soluciones de los casos restantes del Sistema Informático de la cooperativa KOPERA, para que la compañía pueda cumplir con las exigencias de transparencia que la Superintendencia de Bancos e Instituciones Financieras de Chile (SBIF) va a requerir.

**2. Actividad a resolver**

* Conéctese a la base de datos como usuario SYS o SYSTEM ADMIN (si está usando Oracle Cloud) para crear los usuarios definidos.
* Cree las conexiones necesarias a la base de datos para poder trabajar con los usuarios creados.
* El script de poblado de tablas está construido para que en las filas de algunas tablas el año se asigne dinámicamente (año actual, año(s) anterior(es)) según el año en que se ejecute el script.
* En los casos que se indique que el informe o proceso debe obtener la información del año anterior, año actual, mes anterior, día siguiente, etc., significa que la sentencia SQL se debe construir usando las FUNCIONES adecuadas para obtener la fecha requerida y NO USANDO FECHAS FIJAS.

**IMPLEMENTACIÓN ETAPA 3 DEL CASO:** Diseñar e implementar una política de creación y gestión de cuentas de usuarios de base de datos de acuerdo con el trabajo que cada uno de ellos desempeña.

**REQUERIMIENTO N°1:**

La seguridad de datos, también conocida como seguridad de la información o seguridad informática, es un aspecto esencial de TI en organizaciones de cualquier tamaño y tipo. Se trata de un aspecto que tiene que ver con la protección de datos contra accesos no autorizados y para protegerlos de una posible corrupción durante todo su ciclo de vida.

Hoy en día, organizaciones de todo el mundo invierten fuertemente en la tecnología de información relacionada con la ciberdefensa con el fin de proteger sus activos críticos: su marca, capital intelectual y la información de sus clientes.

En todos los temas de seguridad de datos existen elementos comunes que todas las organizaciones deben tener en cuenta a la hora de aplicar sus medidas: las personas, los procesos y la tecnología.

La seguridad de datos es un tema de suma importancia que nos afecta a casi todos nosotros. Cada vez son más los productos tecnológicos que de una u otra forma se deben tener en cuenta para temas de seguridad y que se están introduciendo en nuestra vida cotidiana.

Las bases de datos representan componentes de infraestructura que son imprescindibles en las arquitecturas de servicios o aplicaciones informáticas ya que permiten el almacenamiento de datos e información. A su vez, proporcionan la operatividad de los servicios informáticos, lo que permite realizar actividades de análisis de datos a través de la información almacenada. De esta forma, se logra una visibilidad del panorama competitivo de la empresa en el mercado ayudando en el proceso de toma de decisiones.

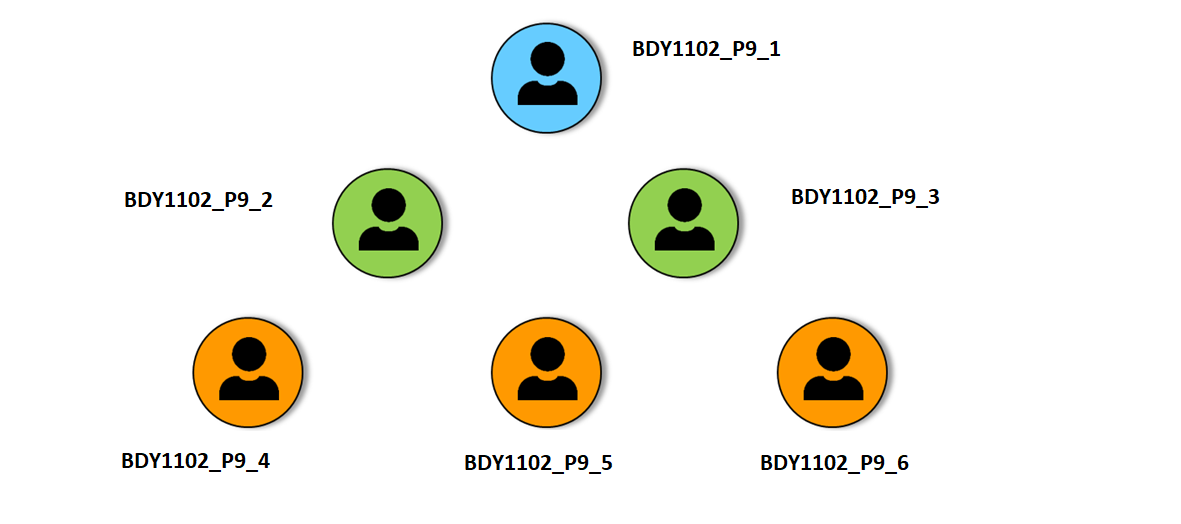
La información (DATOS) constituye uno de los activos más importantes de cualquier organización, independientemente de su tamaño o actividad. La cartera de clientes, las ofertas, contratos, protocolos internos, los planes estratégicos, nóminas, cuentas bancarias, etc. son ejemplos de información que se deben proteger en la empresa ya que los ataques a las bases de datos de una empresa pueden ser variadas, sin embargo, se relacionan directamente con las acciones que se puedan realizar en la base de datos y con la vulneración de la información o datos que se puedan extraer de ella tanto usuarios externos como usuarios del misma organización.

Para ello se deben implantar medidas preventivas y proactivas en las empresas, destinadas a preservar y proteger la confidencialidad, la disponibilidad, integridad de la información y las acciones que cualquier usuario pueda realizar en las Bases de Datos. La habilitación de esquemas de protección para las Bases de Datos permite asumir estrategias de protección y seguridad sobre cualquier acción que los usuarios puedan realizar en ella.

Desde esta perspectiva, la implantación de un sistema de gestión de la calidad para lograr la certificación ISO 9001 obliga a que KOPERA cuente con una estrategia integral y eficiente de creación de usuarios de base de datos, asignación de privilegios y acceso a los objetos de la base de datos.

Esta estrategia deberá ser implementada por Ud., de acuerdo a la redefinición de tipos de usuarios y acciones que pueden realizar según el trabajo que realizan en KOPERA:

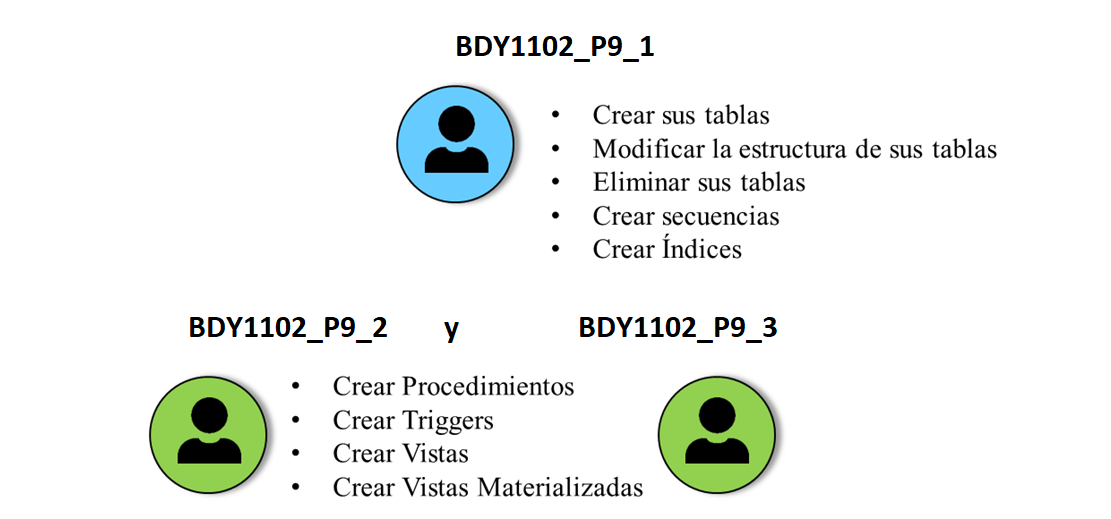
**1.- USUARIOS DE BASE DE DATOS**



**2.- TAREAS QUE REALIZAN**

|  |  |  |
| --- | --- | --- |
| **USUARIO** | | **TAREAS QUE REALIZAN** |
|  | **BDY1102\_P9\_1** | Usuario dueño (owner) de las tablas definidas en el Modelo que se adjunta como ANEXO A, y que se crean en la base de datos ejecutando el script **crea\_pobla\_tablas\_bd\_KOPERA.sql** |
|  | **BDY1102\_P9\_2** | Usuario genérico que será usado por todos los Desarrolladores del Sistema Informático Bancario. |
|  | **BDY1102\_P9\_3**  **BDY1102\_P9\_4** | Usuarios genéricos que ejecutan los informes y sentencias SQL que los desarrolladores construyen. |

**3.- ACCIONES QUE PUEDEN REALIZAR EN LA BASE DE DATOS**



**4.- ACCESO A LOS DATOS Y OBJETOS**

|  |  |  |
| --- | --- | --- |
| **USUARIO** | | **ACCESOS** |
|  | **BDY1102\_P9\_2**  **BDY1102\_P9\_3** | * Consultar información de todas las tablas del usuario MDY2131\_P13\_1. * Modificar, insertar y eliminar información en las tablas del usuario MDY2131\_P13\_1: * CREDITO\_CLIENTE * PRODUCTO\_INVERSION\_CLIENTE * CUOTA\_CREDITO\_CLIENTE. * Por seguridad de los objetos, todos los informes y consultas SQL que desarrollen NO pueden usar los nombres reales de las tablas. |
|  | **BDY1102\_P9\_4** | * Usuario genérico que ejecuta los informes construidos por el usuario MDY2131\_P13\_2 relacionados a las transacciones realizadas por los clientes de KOPERA. * Consultar información de las tablas del MDY2131\_P13\_1: * TIPO\_MOVIMIENTO * SUCURSAL * TIPO\_CONTRATO * CLIENTE * REGION * PROVINCIA * COMUNA * Por seguridad de los objetos NO puede acceder a las tablas usando los nombres reales de las tablas. |
|  | **BDY1102\_P9\_5**  **BDY1102\_P9\_6** | * Usuarios genéricos que ejecutan los informes construidos por el usuario MDY2131\_P13\_3 relacionados a información general de los clientes de KOPERA. * Consultar información de las tablas del MDY2131\_P13\_1: * CLIENTE * REGION * PROVINCIA * COMUNA * Por seguridad de los objetos NO pueden acceder a las tablas usando los nombres reales de las tablas. |

**5.- CONSIDERACIONES AL CREAR LAS CUENTAS DE USUARIOS**

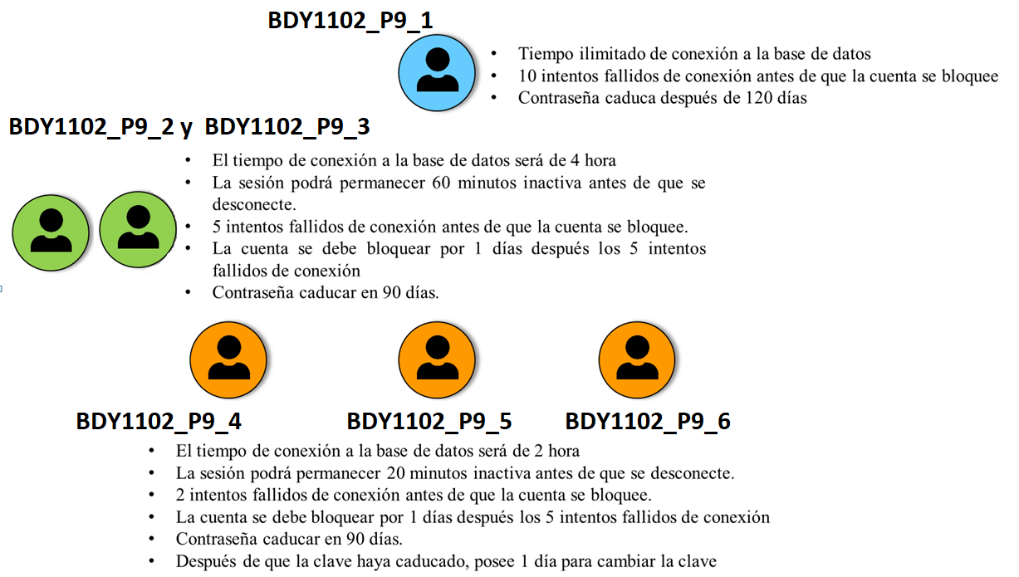
**5.1.- Gestión de Contraseñas:**

* + Debe contener un mínimo de 12 caracteres.
  + Debe contener mínimo 1 caracter en minúscula
  + Debe contener mínimo 2 caracteres en mayúscula
  + Debe contener mínimo 2 números
  + No puede contener el nombre de la cuenta de usuario

**5.2.- Gestión de Espacio:**

* + Tablespace por defecto: USERS si está usando la Base de Datos es Oracle XE y DATA si está usando la Base de Datos Oracle Cloud.
  + Cuota del Tablespace por defecto:
    - Usuarios desarrolladores: Ilimitada
    - Usuarios que sólo ejecuta informes: 100 MB
  + Tablespace temporal: TEMP

**5.3.- Límites de Recursos y Gestión del Estado de las Cuentas de Usuarios**



**6.- ESTRATEGIA DE ASIGNACIÓN DE PRIVILEGIOS**

* Para la implementación, se debe considerar la eficiencia en la asignación de privilegios a los diferentes usuarios. Esto significa que se debe tener presente:
  + En qué escenario la mejor opción es asignar privilegios individuales a los usuarios.
  + En qué escenario la mejor opción es asignar a un conjunto de privilegios relacionados (ROLES) a los usuarios.
  + Seguir el principio de Menor Privilegio

**7.- ESTRATEGIA PARA USAR NOMBRES ALTERNATIVOS DE LOS OBJETOS**

* Para la implementación, se debe considerar la eficiencia en crear sinónimos públicos y privados para los objetos:
  + En qué escenario la mejor opción es crear un sinónimo privado para el objeto.
  + En qué escenario la mejor opción es crear un sinónimo público para el objeto.

**REQUERIMIENTO N°2**

Los usuarios **BDY1102\_P9\_2** y **BDY1102\_P9\_3 han** construido Vistas para solucionar los requerimientos de información que se relacionan a los datos de los clientes y el total de créditos que los clientes han solicitado.

Estas Vistas ahora se deben crear en la base ya que los usuarios BDY1102\_P9\_5 y BDY1102\_P9\_6 requieren de esta información a la brevedad. Para esto, el requisito es primero haber implementado la estrategia de creación de usuarios de base de datos, asignación de privilegios y acceso a los objetos de la base de datos del **REQUERIMIENTO N°1.** Realizado esto, debe efectuar lo siguiente:

**1.- CREACIÓN VISTA EN USUARIO BDY1102\_P9\_2:**

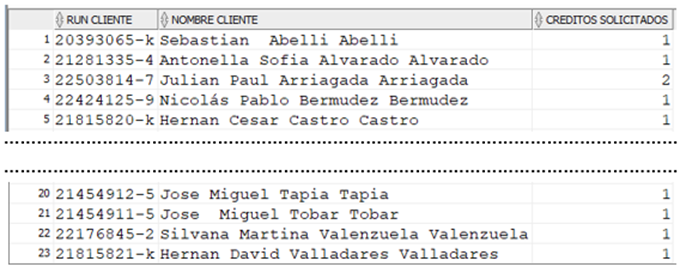
* Conéctese a la base de datos como usuario BDY1102\_P9\_2.
* Ejecute el script del archivo 2.4.7\_Creación\_de\_Vista\_usuario\_P9.SQL para crear la vista V\_TOTAL\_CREDITOS\_CLIENTE. Siguiendo las normas de seguridad para acceder a los objetos, la vista accede a las tablas reales a través de sinónimos, los que deben haber sido creados en la implementación del **REQUERIMIENTO N°1.**

**2.- CREACIÓN VISTA EN USUARIO BDY1102\_P9\_3:**

* Conéctese a la base de datos como usuario BDY1102\_P9\_3.
* Ejecute el script del archivo 2.4.8\_Creación\_de\_Vista\_en\_usuario\_P9.SQL para crear la vista V\_DATOS\_CLIENTES. Siguiendo las normas de seguridad para acceder a los objetos, la vista accede a las tablas reales a través de sinónimos, los que deben haber sido creados en la implementación del **REQUERIMIENTO N°1.**

**3.- EJECUCIÓN VISTA**  **V\_TOTAL\_CREDITOS\_CLIENTE**

* Conéctese a la base de datos como usuario BDY1102\_P9\_3
* Ejecute la vista V\_TOTAL\_CREDITOS\_CLIENTE y debería ver la siguiente información:



**4.- EJECUCIÓN VISTA V\_DATOS\_CLIENTES**

* Conéctese a la base de datos como usuario BDY1102\_P9\_4
* Ejecute la vista V\_DATOS\_CLIENTES y debería ver la siguiente información:

