PROYECTO SEGURIDAD EN BASE DE DATOS

Como requisito para la terminación a satisfacción de la asignatura Seguridad en bases de datos de la Maestría en Seguridad Informática y de las comunicaciones se presenta a continuación la primera entrega del proyecto final.

**Objetivo**: Aplicar el framework de Ciberseguridad planteado por la NIST a una base de datos de una organización de modo que se protejan su integridad, disponibilidad y confidencialidad.

Para el planteamiento del proyecto final se evaluará y protegerá la base de datos de empleados de la empresa *Siemens Corporate Research*, esta base de datos es muy importante debido a que contiene datos personales que según la legislación actual deben ser protegidos contra toda amenaza. Para el debido aseguramiento de la base de datos se utlizarán los controles planteados en el framework de cyberseguridad planteado por el National Institute of Standards and Technology (NIST).

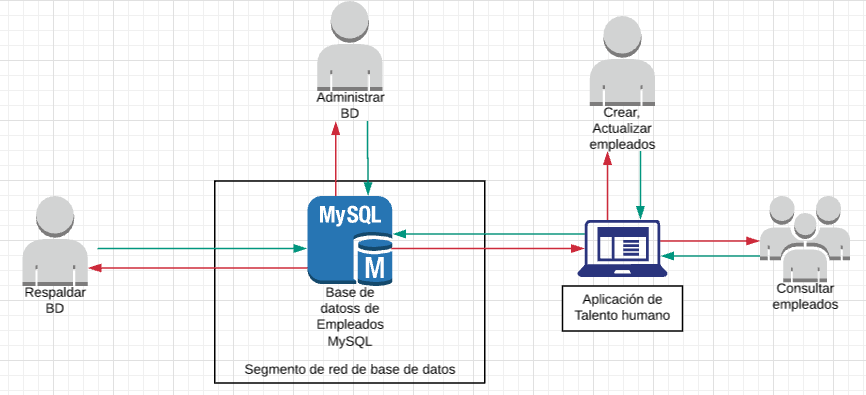
Controles aplicados

**ID.AM-2**: Las plataformas de Software y las aplicaciones dentro de la organización están inventariadas

En auditoría de ISO-27001 a la empresa *Siemens Corporate Research*, se encontró que la base de datos de empleados se encuentra junto con otras bases de datos en un servidor dedicado dentro de un segmento de red donde se encuentran todas las bases de datos de la organización, también se observa que no existe un registro documental de la totalidad de bases de datos que pertenecen a la organización. Dado lo anterior se deja una no conformidad contra el control A.7.1.1.

**ID.AM-3**: Comunicaciones organizacionales y flujos de datos son mapeados

Las comunicaciones y flujos de datos hacia la base de datos de empleados se encuentran documentados en el siguiente diagrama:



**ID.AM-5**: Los recursos son priorizados basados en su clasificación, criticidad y valor de negocio

**ID.AM-6**: Establecer roles y responsabilidades de Ciberseguridad

Un rol de MySQL es una colección de privilegios con nombre. Al igual que las cuentas de usuario, los roles pueden tener privilegios otorgados y revocados.

A una cuenta de usuario se le pueden otorgar roles, lo que otorga a la cuenta los privilegios asociados con cada rol. Esto permite la asignación de conjuntos de privilegios a las cuentas y proporciona una alternativa conveniente para otorgar privilegios individuales, tanto para conceptualizar las asignaciones de privilegios deseadas como para implementarlas.

Los roles definidos en la base de datos son los siguientes:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Usuario** | **Rol** | **Privilegio** | **Recurso** | **Descripción** |
| U.consulta1 | Consulta | Grant select | BD Empleados | Este rol solo puede hacer consultas los registros dentro de la tabla de empleados de la base de datos. |
| U.consulta2 | Consulta | Grant select | BD Empleados | Este rol solo puede hacer consultas los registros dentro de la tabla de empleados de la base de datos. |
| U.crea | Creación | Grant insert | BD Empleados | Este rol puede adicionar empleados a la base de datos. |
| U.crea-actualiza | Creación  Actualizar | Grant insert, update | BD Empleados | Este rol puede actualizar los empleados de la base de datos. |
| u.admin | Creación, modificación, eliminación | Grant insert, update, delete | BD empleados | Este rol puede administrar creando, actualizando y borrando tablas sobre la base de datos. |
| U.respalda | Respaldo | Grant backup | BD Empleados | Este rol solo puede tomas respaldos de la base de datos. |

* Administrar: Tiene privilegio de creación, actualización y eliminación totales sobre la base de datos.
* Respaldar: Tiene privilegio para el respaldo de la estructura y la data de la base de datos.
* Crear: Tiene privilegio de adicionar nuevos empleados a la base de datos
* Actualizar: Tiene privilegio de adición de datos sobre las tablas de la base de datos.
* Consultar: Solo tiene privilegios de consulta sobre los datos de la base de datos.

**ID.GV-3**: Requerimientos legales y regulatorios concernientes a Ciberseguridad

A la presente base de datos le aplica la Ley 1581 de 2012 que corresponde al Régimen General de Protección de Datos Personales. Dicha ley reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.

También aplica la constitución política de Colombia de 1991 en su artículo 15.

**ID.GV-4**: Los procesos de gobierno y gestión de riesgos abordan los riesgos de Ciberseguridad

------------------------------------------------------------------------------------------------------------------------

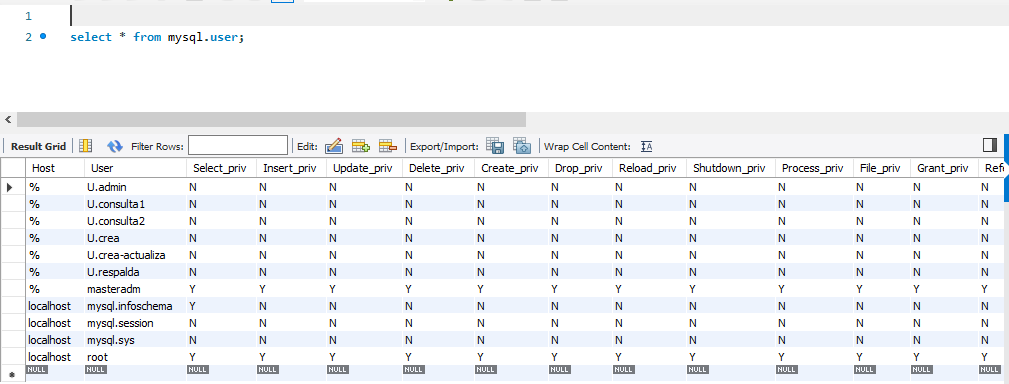
**ID.RA-4**: Se identifican los posibles impactos comerciales y las probabilidades (No aplica)

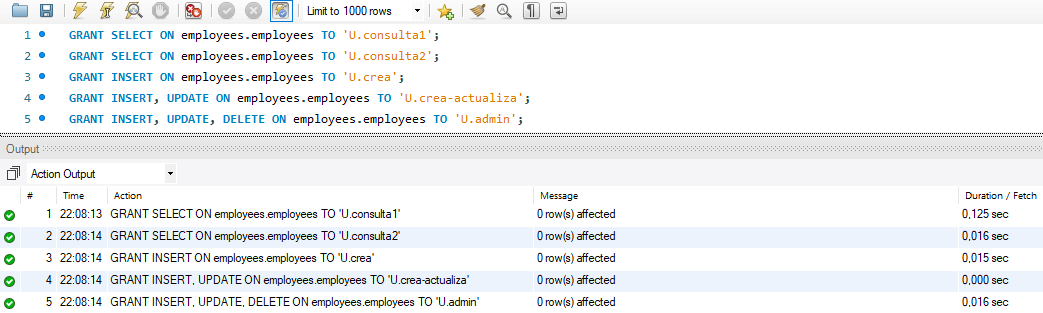
**PR.AC-1**: Las identidades y las credenciales se emiten, administran, verifican, revocan y auditan

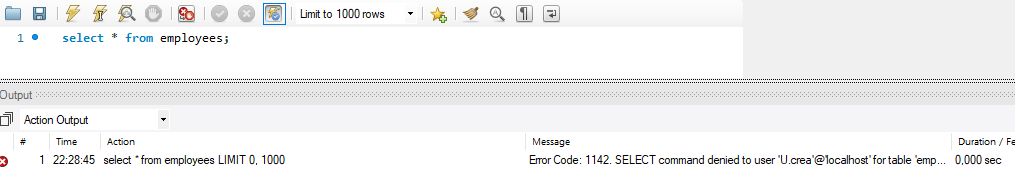
La empresa Soluciones S.A. ha desarrollado una política de gestión de identidades (P-GI-01\_Política de gestión de identidades) para toda la organización donde se describen los roles, accesos y privilegios para todas las aplicaciones y dispositivos la cual es actualizada y ajustada periódicamente. Específicamente para la base de datos de empleados, se definen los roles y privilegios descritos en la sección **4.1 PR.AC-4**.

La gestión de identidades se hace por medio de la suite de herramientas de CA Identity Suite con la que se controlan de manera automatizada las siguientes tareas:

* Gestión de identidades.
* Aprovisionamiento y eliminación del aprovisionamiento.
* Autoservicio de los usuarios.
* Generación de informes y auditorías relativos a la conformidad.
* Ayuda a establecer políticas de seguridad de identidades uniformes.
* Simplifica la conformidad.
* Automatizar procesos clave de la gestión de identidades.
* Análisis y flujos de trabajo para automatizar los procesos de control de identidades, como la limpieza de privilegios, la certificación, la segregación de funciones y la gestión de roles.







**PR.AC-4**: Se gestionan permisos de acceso y autorizaciones.

**PR.DS-1**: La data en reposo es protegida

MySQL Enterprise TDE permite el cifrado de datos en reposo al cifrar los archivos físicos de la base de datos. Los datos se cifran automáticamente, en tiempo real, antes de escribir en el almacenamiento y se descifran cuando se leen desde el almacenamiento. Como resultado, los piratas informáticos y los usuarios malintencionados no pueden leer datos confidenciales de archivos de espacio de tablas, copias de seguridad de bases de datos o discos.

MySQL Enterprise TDE utiliza una arquitectura de clave de cifrado de dos niveles, que consiste en una clave de cifrado maestra y claves de espacio de tabla que proporciona una fácil gestión y rotación de claves. Las claves del espacio de tabla se administran automáticamente entre bastidores, mientras que la clave de encriptación maestra se almacena en una solución de administración de claves centralizada como Oracle Key Vault, que impone una separación clara de las claves de los datos encriptados.

<https://medium.com/@yury.nino.roa/c%C3%B3mo-encriptar-varias-tablas-con-mysql-enterprise-transparent-data-encryption-454d26fba493>

<https://dev.mysql.com/doc/refman/5.7/en/plugin-loading.html>

**PR.DS-2**: La data en tránsito es protegida

**PR.DS-3**: Los activos se administran formalmente a lo largo de la eliminación, las transferencias y la disposición

**PR.DS-4**: Capacidad adecuada para garantizar la disponibilidad

**PR.IP-1**: Se crea y mantiene una configuración básica de los sistemas de tecnología de la información