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:

* Administrar: Tiene privilegios de creación, actualización y eliminación totales sobre la base de datos.
* Respaldar: Tiene privilegios para el respaldo de la estructura y la data de la base de datos.
* Actualizar: Tiene privilegios 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