# Lorena Ocampo C.

**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).

La BD es una RDBMS Relacional, ejemplo de base de datos de empleados creada en MySQL AB. Datos originales creados por Fusheng Wang y Carlo Zaniolo. Esquema actual de Giuseppe Maxia. Conversión de datos de XML a relacional por Patrick Crews

Controles aplicados

1. **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.

La descripción de la BD se puede observar en las siguientes tablas:

**Tabla 1: Administración Empleados**

|  |  |
| --- | --- |
| **dept\_emp** | **Descripción del campo** |
| emp\_no | Número de empleado |
| dept\_no | Número de departamento |
| from\_date | Fecha inicial |
| to\_date | Fecha final |

**Tabla 2: Administración Departamentos**

|  |  |
| --- | --- |
| **dept\_manager** | **Descripción del campo** |
| emp\_no | Número de empleado |
| dept\_no | Número de departamento |
| from\_date | Fecha inicial |
| to\_date | Fecha final |

**Tabla 3: Departamentos**

|  |  |
| --- | --- |
| **departments** | **Descripción del campo** |
| emp\_no | Número de empleado |
| dept\_no | Número de departamento |

**Tabla 4: Títulos**

|  |  |
| --- | --- |
| **titles** | **Descripción del campo** |
| emp\_no | Número de empleado |
| title | Título |
| from\_date | Fecha inicial |
| to\_date | Fecha final |

**Tabla 5: Empleados**

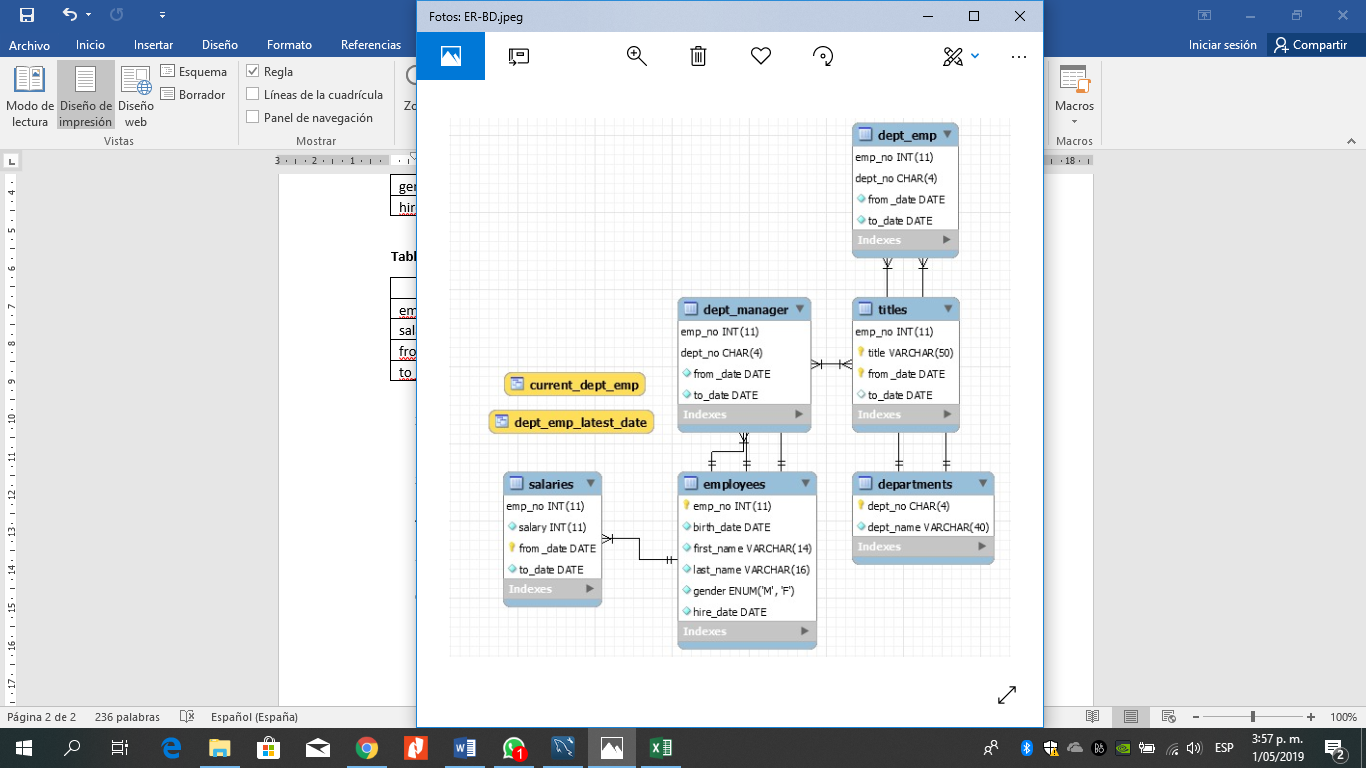
|  |  |
| --- | --- |
| **employees** | **Descripción del campo** |
| emp\_no | Número de empleado |
| birth\_date | Fecha de Nacimiento |
| first\_name | Primer Nombre |
| last\_name | Apellido |
| gender | Género |
| hire\_date | Fecha contratación |

**Tabla 6: Empleados**

|  |  |
| --- | --- |
| **salaries** | **Descripción del campo** |
| emp\_no | Número de empleado |
| salary | Salario |
| from\_date | Fecha inicial |
| to\_date | Fecha final |

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

Las comunicaciones y flujo de datos hacia la base de datos de empleados se pueden entender así:



1. **ID.AM5 Clasificación de la información (Diseño BD)**

La Clasificación de los datos de la Base de Datos se puede visualizar así:

* **Confidencial:** Serán aquellos campos a los cuales únicamente tendrán acceso los usuarios con perfiles especiales, tales como (**emp\_no, salary, titles, dept\_name, dept\_no**) cabe destacar que dentro de los anteriores, solo el campo **emp\_no,** es confidencial por sí solo, el resto, lo serán siempre y cuando estén acompañados del mencionado.
* **Uso Interno:** Serán aquellos campos a los cuales tendrán acceso los usuarios con permisos de uso en la Base de Datos. Estos campos son (**salary, titles, dept\_no, dept\_name, from\_date, to\_date, birth\_date, first\_name, last\_name, gender, hire\_date)**
* **Pùblica:**  Los datos que pueden ser accedidos por cualquiera que tenga ingreso en la Base de Datos.

1. **ID.AM6 Roles y responsabilidades que acceden o modifican la BD**
2. **ID.GV3 Identificar regulaciones y puntos específicos de cada norma**

* **1581:**

**Título II PRINCIPIOS RECTORES**

**Artículo 4°. Principios para el Tratamiento de datos personales**

1. Principio de legalidad en materia de Tratamiento de datos

f) Principio de acceso y circulación restringida

g) Principio de seguridad

h) Principio de confidencialidad

**TÍTULO III CATEGORÍAS ESPECIALES DE DATOS**

**Artículo 5°. Datos sensibles**

**Artículo 6°. Tratamiento de datos sensibles**

1. El Titular haya dado su autorización explícita a dicho Tratamiento

**TÍTULO IV DERECHOS Y CONDICIONES DE LEGALIDAD PARA EL TRATAMIENTO DE DATOS**

**Artículo 8°. Derechos de los Titulares**

1. Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento
2. Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento

e) Revocar la autorización y/o solicitar la supresión del dato cuando en el

Tratamiento no se respeten los principios, derechos y garantías

constitucionales y legales

f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de

Tratamiento

**Artículo 9°. Autorización del Titular**

**Artículo 11. Suministro de la información**

**Parágrafo**. El Responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en el presente artículo y, cuando el Titular lo solicite, entregarle copia de esta.

**Artículo 13. Personas a quienes se les puede suministrar la información**

a) A los Titulares, sus causahabientes o sus representantes legales;

b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial;

c) A los terceros autorizados por el Titular o por la ley.

**TÍTULO VI DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO Y ENCARGADOS**

**DEL TRATAMIENTO**

**Artículo 17. Deberes de los Responsables del Tratamiento**

1. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de

hábeas data;

1. Conservar la información bajo las condiciones de seguridad necesarias para

impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento

g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento

h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley;

i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;

j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley;

**Artículo 18. Deberes de los Encargados del Tratamiento**

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;

b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

g) Registrar en la base de datos las leyenda "reclamo en trámite" en la forma en que se regula en la presente ley;

h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;

j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella

**CAPÍTULO III Del Registro Nacional de Bases de Datos**

**TÍTULO VIII TRANSFERENCIA DE DATOS A TERCEROS PAÍSES**

**Artículo 26. Prohibición**

a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia;

b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública;

c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable;

d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;

e) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular;

f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

**TÍTULO IX OTRAS DISPOSICIONES**

**Artículo 27. Normas Corporativas Vinculantes**

* **PCI Nota:** Aunque esta norma es aplicable para usuarios de tarjetas de crédito. Se usarán aplicados a la información de la Base de Datos

**Proteger los datos del titular de la tarjeta**

**Requisito 3:** Proteja los datos del titular de la tarjeta que fueron almacenados. **Requisito 4:** Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas

**Mantener un programa de administración de vulnerabilidad**

**Requisito 6:** Desarrollar y mantener sistemas y aplicaciones seguros

Implementar medidas sólidas de control de acceso

**Requisito 7**: Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.

**Requisito 8**: Identificar y autenticar el acceso a los componentes del sistema. **Requisito 9:** Restringir el acceso físico a los datos del titular de la tarjeta

**Mantener una política de seguridad de información**

**Requisito 12**: Mantenga una política que aborde la seguridad de la información para todo el personal

* **GDPR**
* **SOX**

**TÍTULO VIII RESPONSABILIDAD CORPORATIVA Y FRAUDE PENAL**

**Sec. 802** Sanciones criminales por la alteración de documentos

**Sec. 806** Protección de los empleados de las compañías que se negocian

públicamente, que proporcionan evidencia de fraude

**TÍTULO XI RESPONSABILIDAD POR EL FRAUDE CORPORATIVO**

**Sec. 1102** Manipulación del registro o impedir de otra manera un procedimiento

oficial

**Sec. 1107** Represalias contra los informantes

* **ISO 271001**

**6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA IN#ORMAC.**

**6.1 Organización interna**

6.1.5 Seguridad de la información en la gestión de proyectos.

**8. GESTIÓN DE ACTIVOS.**

**8.1 Responsabilidad sobre los activos**

8.1.1 Inventario de activos

8.1.2 Propiedad de los activos

8.1.3 Uso aceptable de los activos

8.1.4 Devolución de activos

**8.2 Clasificación de la información**

8.2.1 Directrices de clasificación

8.2.2 Etiquetado & manipulado de la información

8.2.3 Manipulación de activos

**8.3 Manejo de los soportes de almacenamiento**

8.3.1 Gestión de soportes extraíbles

8.3.2 Eliminación de soportes

8.3.4 Soportes físicos en tránsito.

**9. CONTROL DE ACCESOS.**

**9.1Requisitos de negocio para el control de accesos**.

9.1.1 Política de control de accesos.

9.1.2 Control de acceso a las redes & servicios asociados.

**9.2 Gestión de acceso de usuario.**

9.2.1 Gestión de altas y bajas en el registro de usuarios.

9.2.2 Gestión de los derechos de acceso asignados a usuarios.

9.2.3 Gestión de los derechos de acceso con privilegios especiales.

9.2.4 Gestión de información confidencial de autenticación de usuarios.

9.2.5 Revisión de los derechos de acceso de los usuarios.

9.2.6 Retirada o adaptación de los derechos de acceso

**9.3 Responsabilidades del usuario.**

9.3.1 Uso de información confidencial para la autenticación.

**9.4 Control de acceso a sistemas & aplicaciones**.

9.4.1Restricción del acceso a la información.

9.4.2 Procedimientos seguros de inicio de sesión

9.4.3 Gestión de contraseñas de usuario.

9.4.4 Uso de herramientas de administración de sistemas.

9.4.5 Control de acceso al código fuente de los programas.

**10.CIFRADO.**

**10.1Controles criptográficos.**

10.1.1 Política de uso de los controles criptográficos.

10.1.2 Gestión de claves.

**12.SEGURIDAD EN LA OPERATIVA.**

**12.1 Responsabilidades & procedimientos de operación.**

12.1.1 Documentación de procedimientos de operación.

12.1.2 Gestión de cambios.

12.1.3 Gestión de capacidades.

12.1.4 Separación de entornos de desarrollo, prueba & producción.

**12.2 Protección contra código malicioso**.

12.2.1 Controles contra el código malicioso.

**12.3 Copias de seguridad.**

12.3.1 Copias de seguridad de la información.

**12.4 Registro de actividad & supervisión**.

12.4.1 Registro & gestión de eventos de actividad.

12.4.2 Protección de los registros de información.

12.4.3 Registros de actividad del administrador & operador del sistema.

12.4.4 Sincronización de relojes.

**12.5 Control del software en explotación.**

12.5.1 Instalación del software en sistemas en producción.

**12.6 Gestión de la vulnerabilidad técnica**.

12.6.1 Gestión de las vulnerabilidades técnicas.

12.6.2 Restricciones en la instalación de software.

**12.7 Consideraciones de las auditorías de los sistemas de información.**

12.7.1 Controles de auditoría de los sistemas de información.

**13.SEGURIDAD EN LAS TELECOMUNICACIONES.**

**13.1 Gestión de la seguridad en las redes.**

13.1.1 Controles de red.

13.1.2 Mecanismos de seguridad asociados a servicios en red.

13.1.3 Segregación de redes.

**13.2 Intercambio de información con partes externas.**

13.2.1 Políticas & procedimientos de intercambio de información.

13.2.2 Acuerdos de intercambio.

13.2.3 Mensajería electrónica.

13.2.4 Acuerdos de confidencialidad & secreto.

* **NIST**
* **BASEL**
* **Nerc**
* **ISA 62443**
* **FEDRAMP**
* **HIPAA/HITECH**

1. **ID.GV4 Identificar Riesgos**

|  |  |  |  |
| --- | --- | --- | --- |
| **RIESGO** | **PESO IMPACTO** | **PESO PROB.** | **RIESGO INHERENTE** |
| Privilegios excesivos e inutilizados. | 8,5 | 4 | 34 |
| Abuso de Privilegios | 8 | 2 | 16 |
| Inyección por SQL | 9,8 | 4 | 39,2 |
| Auditorías débiles | 5 | 1 | 5 |
| Exposición de los medios de almacenamiento para **backup** | 7,5 | 2 | 15 |
| Explotación de vulnerabilidades y bases de datos mal configuradas | 8,5 | 3 | 25,5 |
| Datos sensibles mal gestionados | 9 | 4 | 36 |
| Denegación de servicio (DoS) | 9,8 | 4 | 39,2 |
| Destrucción de la información / sabotaje | 9,5 | 4 | 38 |
| Limitado conocimiento y experiencia en seguridad y educación. | 8 | 3 | 24 |
| Nombre de usuario/password en blanco o bien hacer uso de uno débil | 8,5 | 4 | 34 |
| Preferencia de privilegios de usuario por privilegios de grupo | 9,5 | 4 | 38 |
| Características de bases de datos innecesariamente habilitadas | 7,5 | 4 | 30 |
| Desbordamiento de búfer | 6 | 5 | 30 |
| Bases de datos sin actualizar | 7,5 | 5 | 37,5 |
| Datos sensibles sin cifrar | 9,5 | 5 | 47,5 |