Universidad de las Fuerzas Armadas “ESPE”

Innovación para la Excelencia

Departamento de Ciencias de la Computación

Ingeniería de Software

Documentación de POC

PRUEBAS DE CONCEPTO 2023

Versión: 1.0.

Trabajo de Desarrollo e Implementación de SW

Responsables: Díaz Adriana, De Veintemilla Luca, Hernández Dylan, Guevara Mathias, Iza Christopher, Masacela Brandon, Pila Johanna, Portilla Diego, Reyes Juan, Tinoco Shared, Vargas Kevin.

Tutor: Dr. Marcelo Rea PhD

Ciudad: Sangolquí

Fecha: 10 de julio de 2023

Campus universitario Sangolquí: Av. Gral. Rumiñahui s/n **Telf:** (593-02) 3 989 400
Fax: (593-02) 2334 952 / **Código postal**: 171103 / **Casillero postal:** 71 5 231 • B
Página Web: www.espe.edu.ec I Sangolquí - Ecuador

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Campus universitario Sangolquí: Av. Gral. Rumiñahui s/n **Telf:** (593-02) 3 989 400
Fax: (593-02) 2334 952 / **Código postal**: 171103 / **Casillero postal:** 71 5 231 • B
Página Web: www.espe.edu.ec I Sangolquí - Ecuador

Campus universitario Sangolquí: Av. Gral. Rumiñahui s/n **Telf:** (593-02) 3 989 400
Fax: (593-02) 2334 952 / **Código postal**: 171103 / **Casillero postal:** 71 5 231 • B
Página Web: www.espe.edu.ec I Sangolquí - Ecuador

1. Resumen

1.1. Descripción del Sistema

El sistema propuesto es un software de gestión de ciberseguridad que permite a las organizaciones identificar, evaluar y mitigar los riesgos asociados con la seguridad informática. El sistema utiliza un enfoque basado en un marco de trabajo establecido para guiar el proceso de identificación y evaluación de riesgos.

Una vez que se han identificado los riesgos, el sistema evalúa la probabilidad de ocurrencia y el impacto potencial de cada uno de ellos. Utiliza criterios establecidos y datos históricos para determinar la gravedad y la prioridad de cada riesgo. Además de su funcionalidad de identificación y evaluación de riesgos, el sistema genera informes detallados y estadísticas relevantes. Estos informes permiten a los usuarios tomar decisiones y realizar un seguimiento del progreso en la mejora de la seguridad cibernética.

1.2. Objetivo General

Desarrollar un marco de trabajo para identificar y evaluar los riesgos de ciberseguridad

1.3. Objetivos Específicos

- Definir un conjunto exhaustivo de criterios y metodologías para la identificación sistemática de los riesgos de ciberseguridad en un entorno específico.
- Establecer un proceso de evaluación riguroso que permita medir y cuantificar los riesgos identificados, considerando la probabilidad de ocurrencia y el impacto potencial en los sistemas y datos.
- Diseñar y documentar un marco de trabajo escalable y adaptable que proporciona pautas claras y prácticas para la identificación y evaluación continuas de los riesgos de ciberseguridad, asegurando una cobertura integral y actualizada en un entorno en constante evolución.

Campus universitario Sangolquí: Av. Gral. Rumiñahui s/n **Telf:** (593-02) 3 989 400
Fax: (593-02) 2334 952 / **Código postal**: 171103 / **Casillero postal:** 71 5 231 • B
Página Web: www.espe.edu.ec I Sangolquí - Ecuador

1.4. Alcance

El alcance de la investigación se centra en el desarrollo de un enfoque sistemático y estructurado para la identificación y evaluación de riesgos en ciberseguridad. Se busca proporcionar a las organizaciones un modelo de madurez y un marco de trabajo que les permita abordar eficazmente los desafíos asociados a la ciberseguridad. El estudio se enfoca en analizar los ataques cibernéticos actuales, los riesgos asociados y las mejores prácticas para proteger la información y los sistemas de las organizaciones.

2. Introducción

2.1. Antecedentes

La ciberseguridad es un tema de gran importancia en la actualidad debido al aumento de los ataques cibernéticos y la necesidad de proteger la información y los sistemas de las organizaciones. Los avances tecnológicos y la interconexión digital han ampliado las posibilidades de los ciberdelincuentes, lo que ha llevado a un incremento en la sofisticación y frecuencia de los ataques. Como resultado, las organizaciones se enfrentan a riesgos cada vez mayores, que van desde la pérdida de datos confidenciales hasta la interrupción de los servicios críticos.

2.2. Justificación

La justificación de esta investigación se basa en la necesidad de abordar la problemática de la ciberseguridad y los riesgos asociados a ella. La creciente amenaza de los ataques cibernéticos ha generado una demanda urgente de enfoques efectivos y estructurados para proteger la información y los sistemas. Es fundamental que las organizaciones cuenten con un modelo de madurez y un marco de trabajo que les permita identificar y evaluar los riesgos de manera sistemática, implementar medidas de protección adecuadas y responder de manera eficiente en caso de incidentes. Este estudio tiene como objetivo contribuir a la comunidad académica y empresarial, proporcionando directrices y mejores prácticas que ayuden a mejorar la postura de ciberseguridad de las organizaciones y mitigar los riesgos asociados a los ataques cibernéticos.

Campus universitario Sangolquí: Av. Gral. Rumiñahui s/n **Telf:** (593-02) 3 989 400
Fax: (593-02) 2334 952 / **Código postal**: 171103 / **Casillero postal:** 71 5 231 • B
Página Web: www.espe.edu.ec I Sangolquí - Ecuador

3. Requisitos

3.1. Funcionales y No Funcionales

Los requisitos para el programa de análisis de seguridad informática aborda tanto los requisitos funcionales como los no funcionales. En términos de requisitos funcionales, el programa debe ser capaz de identificar vulnerabilidades y amenazas, evaluar riesgos, priorizar riesgos y ofrecer recomendaciones de mitigación. Además, debe generar informes detallados y estadísticas relevantes. En cuanto a los requisitos no funcionales, el programa debe garantizar la seguridad de la información confidencial, ser fácil de usar, escalable, confiable y mantenerse de manera efectiva. Estos requisitos aseguran un programa eficiente y efectivo para abordar los desafíos de la seguridad cibernética.

Tabla. 1.- Descripción de Requisitos Funcionales

Requisito Funcional	Descripción
Identificación de vulnerabilidades y amenazas	El programa debe ser capaz de analizar los sistemas informáticos en busca de posibles vulnerabilidades y amenazas de seguridad.
Evaluación de riesgos	El programa debe proporcionar una evaluación precisa de los riesgos identificados, teniendo en cuenta la probabilidad de ocurrencia y el impacto potencial en los sistemas y datos.
Priorización de riesgos	El programa debe permitir la asignación de prioridades a los riesgos identificados, para que los usuarios puedan enfocarse en los riesgos más críticos y tomar medidas de mitigación adecuadas
Recomendaciones de mitigación	El programa debe ofrecer recomendaciones claras y prácticas para mitigar los riesgos identificados, proporcionando orientación sobre las mejores prácticas de seguridad y las medidas específicas a tomar
Generación de informes y estadísticas	El programa debe ser capaz de generar informes detallados y estadísticas relevantes sobre los riesgos identificados y las medidas de mitigación implementadas, para facilitar la toma de decisiones

Campus universitario Sangolquí: Av. Gral. Rumiñahui s/n **Telf:** (593-02) 3 989 400
Fax: (593-02) 2334 952 / **Código postal**: 171103 / **Casillero postal:** 71 5 231 • B
Página Web: www.espe.edu.ec I Sangolquí - Ecuador

	informadas y el seguimiento del progreso en la seguridad cibernética.

Tabla. 2.- Descripción de Requisitos No Funcionales

Requisito No Funcional	Descripción
Seguridad	El programa debe garantizar la seguridad de la información confidencial y los datos analizados, utilizando técnicas de encriptación y asegurando el acceso adecuado a través de autenticación y autorización robustas.
Usabilidad	El programa debe ser intuitivo y fácil de usar para los usuarios, con una interfaz clara y orientada al usuario que permita una interacción fluida y comprensión de los resultados y recomendaciones.
Escalabilidad	El programa debe ser capaz de manejar grandes volúmenes de datos y usuarios concurrentes sin comprometer el rendimiento y la precisión de los análisis de riesgos.
Fiabilidad	El programa debe ser confiable y estar disponible en todo momento, minimizando los tiempos de inactividad y asegurando la integridad de los datos y los resultados de los análisis
Mantenibilidad	El programa debe ser fácil de mantener y actualizar, con una arquitectura modular y bien documentada que facilite la incorporación de nuevas funcionalidades y la corrección de errores

Campus universitario Sangolquí: Av. Gral. Rumiñahui s/n **Telf:** (593-02) 3 989 400
Fax: (593-02) 2334 952 / **Código postal**: 171103 / **Casillero postal:** 71 5 231 • B
Página Web: www.espe.edu.ec I Sangolquí - Ecuador

4. Desarrollo de Base de Datos

4.1. Modelo Conceptual

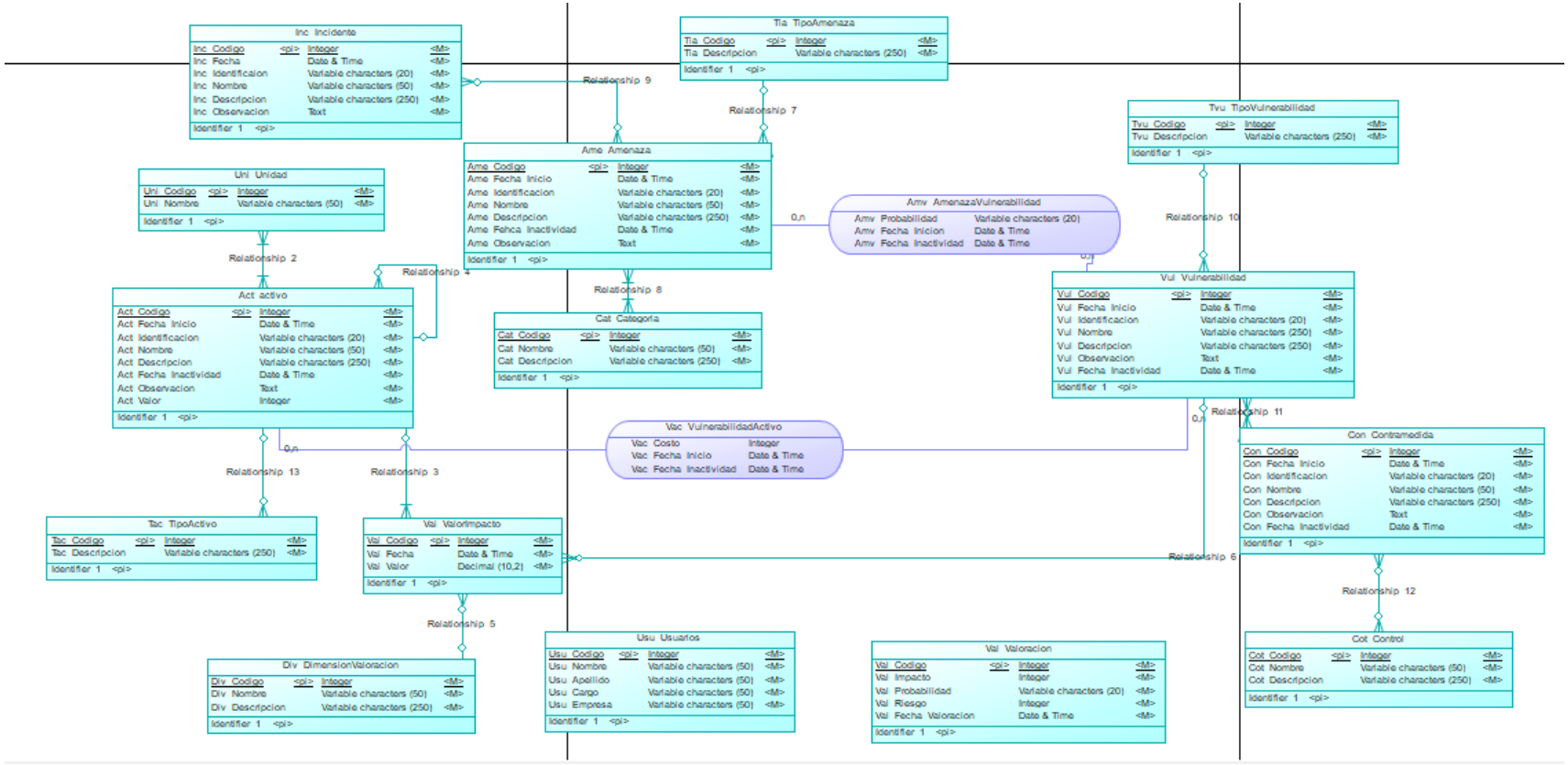

Fig. 1.- Modelo Conceptual del Sistema

4.2. Modelo Lógico

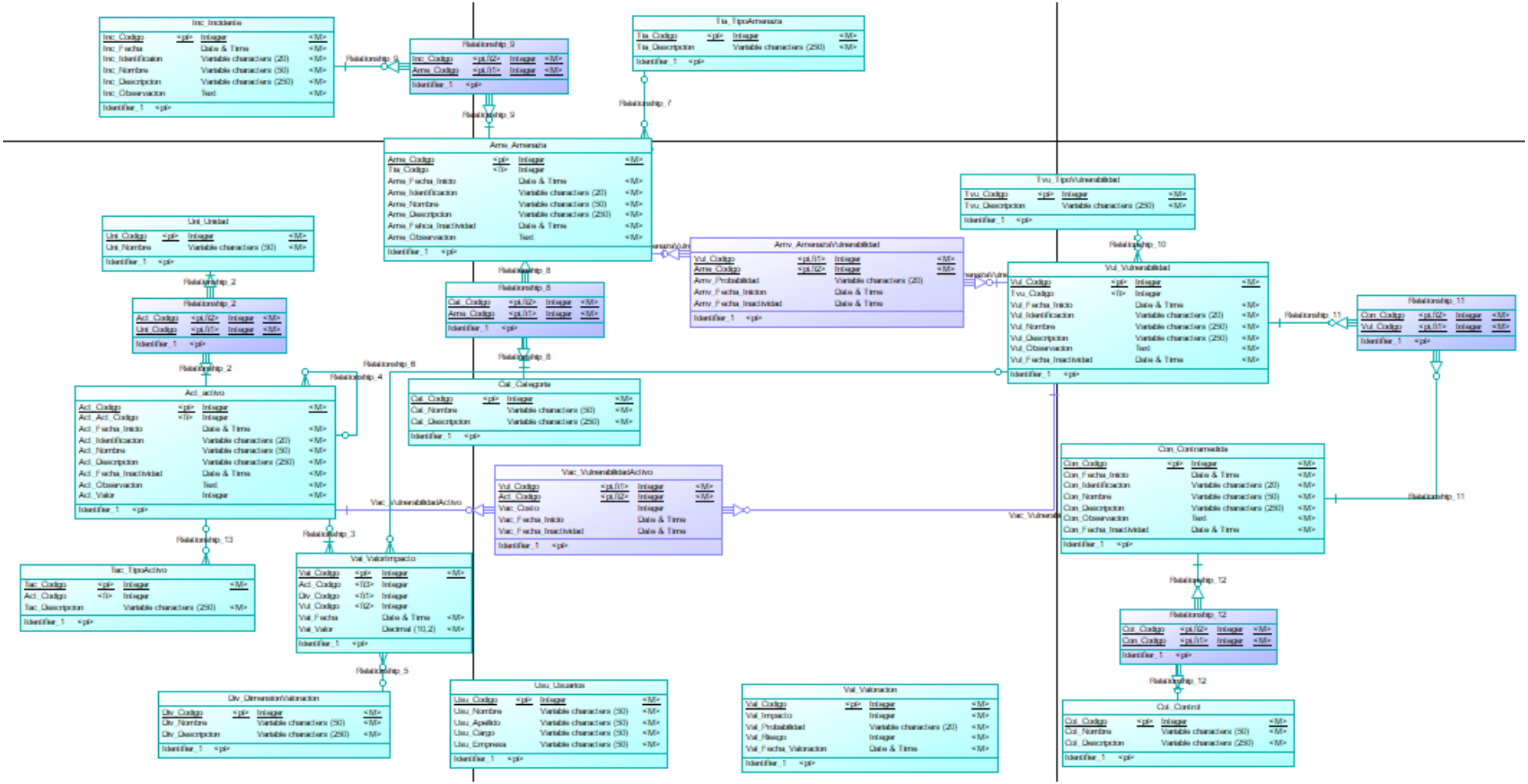

Fig. 2.- Modelo Lógico del Sistema

4.3. Modelo Físico

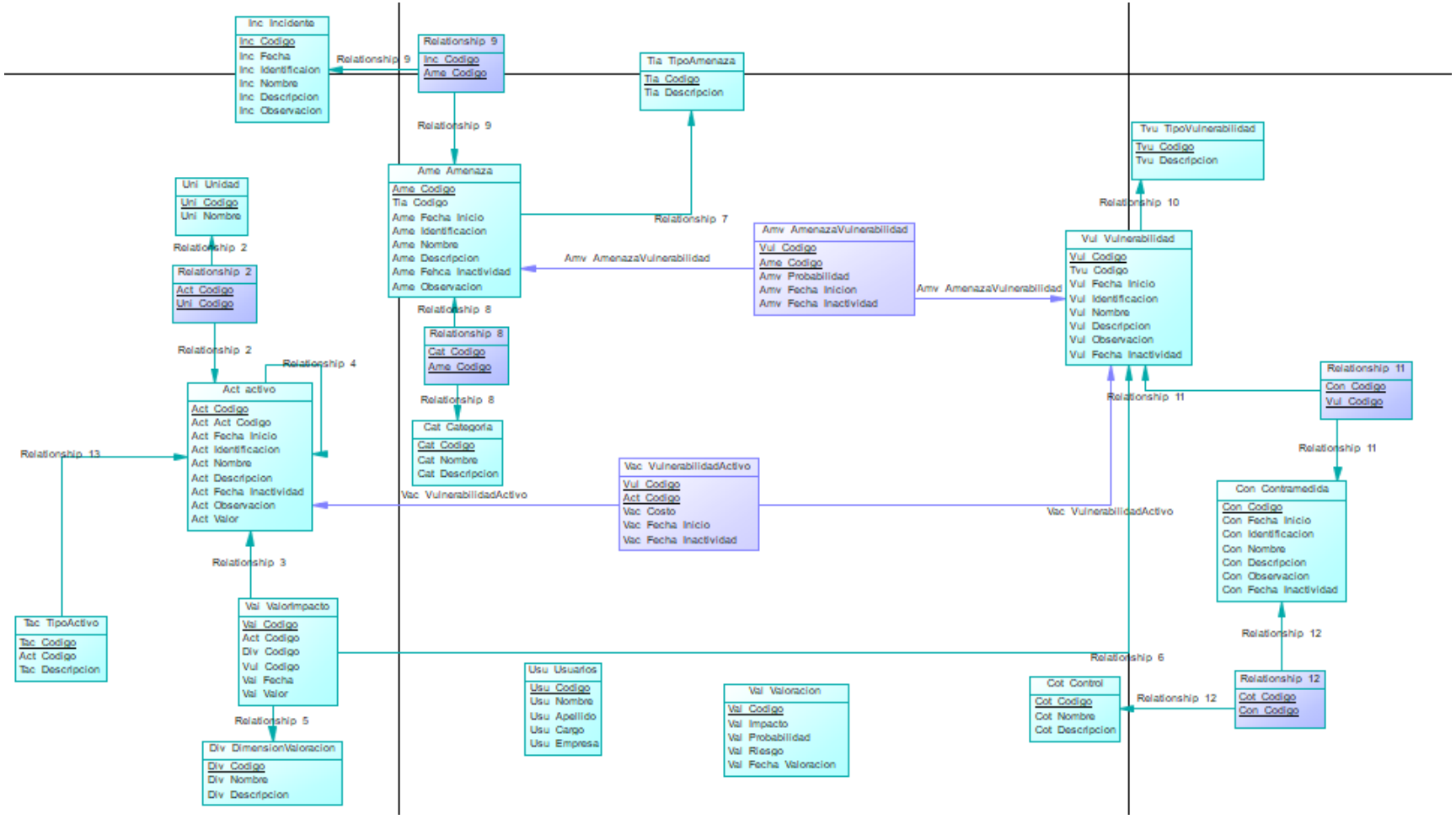

Fig. 3.- Modelo Físico del Sistema

4.4. Diccionario de Datos

Tabla. 3.- ACT_ACTIVO

ACT_CODIGO	Identificador único del activo.
ACT_ACT_CODIGO	Código del activo relacionado.
ACT_FECHA_INICIO	Fecha de inicio del activo.
ACT_IDENTIFICACION	Identificación del activo.
ACT_NOMBRE	Nombre del activo.
ACT_DESCRIPCION	Descripción del activo.
ACT_FECHA_INACTIVIDAD	Fecha de inactividad del activo.
ACT_OBSERVACION	Observación del activo.
ACT_VALOR	Valor del activo.

Tabla. 4.- AME_AMENAZA

AME_CODIGO	Identificador único de la amenaza.
TIA_CODIGO	Código del tipo de amenaza relacionado.
AME_FECHA_INICIO	Fecha de inicio de la amenaza.
AME_IDENTIFICACION	Identificación de la amenaza.
AME_NOMBRE	Nombre de la amenaza.
AME_DESCRIPCION	Descripción de la amenaza.
AME_FEHCA_INACTIVIDAD	Fecha de inactividad de la amenaza.
AME_OBSERVACION	Observación de la amenaza.

Tabla. 5.- AMV_AMENAZAVULNERABILIDAD

VUL_CODIGO	Código de la vulnerabilidad relacionada.

Campus universitario Sangolquí: Av. Gral. Rumiñahui s/n **Telf:** (593-02) 3 989 400
Fax: (593-02) 2334 952 / **Código postal**: 171103 / **Casillero postal:** 71 5 231 • B
Página Web: www.espe.edu.ec I Sangolquí - Ecuador

AME_CODIGO	Código de la amenaza relacionada.
AMV_PROBABILIDAD	Probabilidad de la amenaza y vulnerabilidad.
AMV_FECHA_INICION	Fecha de inicio de la amenaza y vulnerabilidad.
AMV_FECHA_INACTIVIDAD	Fecha de inactividad de la amenaza y vulnerabilidad.

Tabla. 6.- CAT_CATEGORIA

CAT_CODIGO	Identificador único de la categoría.
CAT_NOMBRE	Nombre de la categoría.
CAT_DESCRIPCION	Descripción de la categoría.

Tabla. 7.- CON_CONTRAMEDIDA

CON_CODIGO	Identificador único de la contramedida.
CON_FECHA_INICIO	Fecha de inicio de la contramedida.
CON_IDENTIFICACION	Identificación de la contramedida.
CON_NOMBRE	Nombre de la contramedida.
CON_DESCRIPCION	Descripción de la contramedida.
CON_OBSERVACION	Observación de la contramedida.
CON_FECHA_INACTIVIDAD	Fecha de inactividad de la contramedida.

Tabla. 8.- COT_CONTROL

COT_CODIGO	Identificador único del control.
COT_NOMBRE	Nombre del control.
COT_DESCRIPCION	Descripción del control.

Campus universitario Sangolquí: Av. Gral. Rumiñahui s/n **Telf:** (593-02) 3 989 400
Fax: (593-02) 2334 952 / **Código postal**: 171103 / **Casillero postal:** 71 5 231 • B
Página Web: www.espe.edu.ec I Sangolquí - Ecuador

Tabla. 9.- DIV_DIMENSIONVALORACION

DIV_CODIGO	Identificador único de la dimensión de valoración.
DIV_NOMBRE	Nombre de la dimensión de valoración.
DIV_DESCRIPCION	Descripción de la dimensión de valoración.

Tabla. 10.- INC_INCIDENTE

INC_CODIGO	Identificador único del incidente.
INC_FECHA	Fecha del incidente.
INC_IDENTIFICACION	Identificación del incidente.
INC_NOMBRE	Nombre del incidente.
INC_DESCRIPCION	Descripción del incidente.
INC_OBSERVACION	Observación del incidente.

Tabla. 11.- RELATIONSHIP_11

CON_CODIGO	Código de la contramedida relacionada.
VUL_CODIGO	Código de la vulnerabilidad relacionada.

Tabla. 12.- RELATIONSHIP_12

COT_CODIGO	Código del control relacionado.
CON_CODIGO	Código de la contramedida relacionada.

Tabla. 13.- RELATIONSHIP_2

ACT_CODIGO	Código del activo relacionado.

Campus universitario Sangolquí: Av. Gral. Rumiñahui s/n **Telf:** (593-02) 3 989 400
Fax: (593-02) 2334 952 / **Código postal**: 171103 / **Casillero postal:** 71 5 231 • B
Página Web: www.espe.edu.ec I Sangolquí - Ecuador

UNI_CODIGO	Código de la unidad relacionada.

Tabla. 14.- RELATIONSHIP_8

CAT_CODIGO	Código de la categoría relacionada.
AME_CODIGO	Código de la amenaza relacionada.

Tabla. 15.- RELATIONSHIP_9

INC_CODIGO	Código del incidente relacionado.
AME_CODIGO	Código de la amenaza relacionada.

Tabla. 16.- TAC_TIPOACTIVO

TAC_CODIGO	Identificador único del tipo de activo.
ACT_CODIGO	Código del activo relacionado.
TAC_DESCRIPCION	Descripción del tipo de activo.

Tabla. 17.- TIA_TIPOAMENAZA

TIA_CODIGO	Identificador único del tipo de amenaza.
TIA_DESCRIPCION	Descripción del tipo de amenaza.

Tabla. 18.- TVU_TIPOVULNERABILIDAD

TVU_CODIGO	Identificador único del tipo de vulnerabilidad.
TVU_DESCRIPCION	Descripción del tipo de vulnerabilidad.

Campus universitario Sangolquí: Av. Gral. Rumiñahui s/n **Telf:** (593-02) 3 989 400
Fax: (593-02) 2334 952 / **Código postal**: 171103 / **Casillero postal:** 71 5 231 • B
Página Web: www.espe.edu.ec I Sangolquí - Ecuador

Tabla. 19.- UNI_UNIDAD

UNI_CODIGO	Identificador único de la unidad.
UNI_NOMBRE	Nombre de la unidad.

Tabla. 20.- USU_USUARIOS

USU_CODIGO	Identificador único del usuario.
USU_NOMBRE	Nombre del usuario.
USU_APELLIDO	Apellido del usuario.
USU_CARGO	Cargo del usuario.
USU_EMPRESA	Empresa del usuario.

Tabla. 21.- VAC_VULNERABILIDADACTIVO

VUL_CODIGO	Código de la vulnerabilidad relacionada.
ACT_CODIGO	Código del activo relacionado.
VAC_COSTO	Costo de la vulnerabilidad y activo.
VAC_FECHA_INICIO	Fecha de inicio de la vulnerabilidad y activo.
VAC_FECHA_INACTIVIDAD	Fecha de inactividad de la vulnerabilidad y activo.

Tabla. 22.- VAL_VALORIMPACTO

VAI_CODIGO	Identificador único del valor de impacto.
ACT_CODIGO	Código del activo relacionado.
DIV_CODIGO	Código de la dimensión de valoración relacionada.

Campus universitario Sangolquí: Av. Gral. Rumiñahui s/n **Telf:** (593-02) 3 989 400
Fax: (593-02) 2334 952 / **Código postal**: 171103 / **Casillero postal:** 71 5 231 • B
Página Web: www.espe.edu.ec I Sangolquí - Ecuador

VUL_CODIGO	Código de la vulnerabilidad relacionada.
VAI_FECHA	Fecha del valor de impacto.
VAI_VALOR	Valor del impacto.

Tabla. 23.- VAL_VALORACION

VAL_CODIGO	Identificador único de la valoración.
VAL_IMPACTO	Impacto de la valoración.
VAL_PROBABILIDAD	Probabilidad de la valoración.
VAL_RIESGO	Riesgo de la valoración.
VAL_FECHA_VALORACION	Fecha de la valoración.

Tabla. 24.- VUL_VULNERABILIDAD

VUL_CODIGO	Identificador único de la vulnerabilidad.
TVU_CODIGO	Código del tipo de vulnerabilidad relacionado.
VUL_FECHA_INICIO	Fecha de inicio de la vulnerabilidad.
VUL_IDENTIFICACION	Identificación de la vulnerabilidad.
VUL_NOMBRE	Nombre de la vulnerabilidad.
VUL_DESCRIPCION	Descripción de la vulnerabilidad.
VUL_OBSERVACION	Observación de la vulnerabilidad.
VUL_FECHA_INACTIVIDAD	Fecha de inactividad de la vulnerabilidad.

Tabla. 25.- Relación entre tablas

ACT_ACTIVO y ACT_ACT_CODIGO	Relación uno a muchos, donde un activo puede tener varios activos relacionados.

Campus universitario Sangolquí: Av. Gral. Rumiñahui s/n **Telf:** (593-02) 3 989 400
Fax: (593-02) 2334 952 / **Código postal**: 171103 / **Casillero postal:** 71 5 231 • B
Página Web: www.espe.edu.ec I Sangolquí - Ecuador

AME_AMENAZA y TIA_CODIGO	Relación uno a muchos, donde una amenaza puede tener varios tipos de amenazas relacionados.
AMV_AMENAZAVULNERABILIDAD y AME_CODIGO	Relación uno a muchos, donde una amenaza puede tener varias amenazas y vulnerabilidades relacionadas.
AMV_AMENAZAVULNERABILIDAD y VUL_CODIGO:	Relación uno a muchos, donde una vulnerabilidad puede tener varias amenazas y vulnerabilidades relacionadas.
ACT_ACTIVO y UNI_UNIDAD	Relación muchos a muchos, donde un activo puede estar asociado a varias unidades y una unidad puede estar asociada a varios activos.
CAT_CATEGORIA y AME_AMENAZA	Relación muchos a muchos, donde una categoría puede tener varias amenazas y una amenaza puede estar asociada a varias categorías.
INC_INCIDENTE y AME_AMENAZA	Relación muchos a muchos, donde un incidente puede tener varias amenazas y una amenaza puede estar asociada a varios incidentes.
CON_CONTRAMEDIDA y VUL_VULNERABILIDAD	Relación muchos a muchos, donde una contramedida puede estar asociada a varias vulnerabilidades y una vulnerabilidad puede tener varias contramedidas relacionadas.
COT_CONTROL y CON_CONTRAMEDIDA	Relación muchos a muchos, donde un control puede tener varias contramedidas y una contramedida puede estar asociada a varios controles.
TAC_TIPOACTIVO y ACT_ACTIVO	Relación uno a muchos, donde un tipo de activo puede tener varios activos relacionados.
TIA_TIPOAMENAZA y AME_AMENAZA	Relación uno a muchos, donde un tipo de amenaza puede tener varias amenazas relacionadas.
TVU_TIPOVULNERABILIDAD y VUL_VULNERABILIDAD	Relación uno a muchos, donde un tipo de vulnerabilidad puede tener varias vulnerabilidades relacionadas.
RELATIONSHIP_11 y CON_CONTRAMEDIDA	Relación uno a muchos, donde una contramedida puede tener varias relaciones con vulnerabilidades.

Campus universitario Sangolquí: Av. Gral. Rumiñahui s/n **Telf:** (593-02) 3 989 400
Fax: (593-02) 2334 952 / **Código postal**: 171103 / **Casillero postal:** 71 5 231 • B
Página Web: www.espe.edu.ec I Sangolquí - Ecuador

RELATIONSHIP_11 y VUL_VULNERABILIDAD	Relación uno a muchos, donde una vulnerabilidad puede tener varias relaciones con contramedidas.
RELATIONSHIP_12 y COT_CONTROL	Relación uno a muchos, donde un control puede tener varias relaciones con contramedidas.
RELATIONSHIP_12 y CON_CONTRAMEDIDA	Relación uno a muchos, donde una contramedida puede tener varias relaciones con controles.
RELATIONSHIP_2 y ACT_ACTIVO	Relación uno a muchos, donde un activo puede tener varias relaciones con unidades y una unidad puede tener varias relaciones con activos.
RELATIONSHIP_8 y CAT_CATEGORIA	Relación uno a muchos, donde una categoría puede tener varias relaciones con amenazas y una amenaza puede tener varias relaciones con categorías.
RELATIONSHIP_8 y AME_AMENAZA	Relación uno a muchos, donde una amenaza puede tener varias relaciones con categorías.
RELATIONSHIP_9 y INC_INCIDENTE	Relación uno a muchos, donde un incidente puede tener varias relaciones con amenazas y una amenaza puede tener varias relaciones con incidentes.
RELATIONSHIP_9 y AME_AMENAZA	Relación uno a muchos, donde una amenaza puede tener varias relaciones con incidentes.
VAC_VULNERABILIDADACTIVO y ACT_ACTIVO	Relación uno a muchos, donde un activo puede tener varias relaciones con vulnerabilidades y una vulnerabilidad puede tener varias relaciones con activos.
VAC_VULNERABILIDADACTIVO y VUL_VULNERABILIDAD	Relación uno a muchos, donde una vulnerabilidad puede tener varias relaciones con activos.
VAI_VALORIMPACTO y ACT_ACTIVO	Relación uno a muchos, donde un activo puede tener varias relaciones con valores de impacto y un valor de impacto puede estar asociado a varios activos.
VAI_VALORIMPACTO y DIV_DIMENSIONVALORACION	Relación uno a muchos, donde una dimensión de valoración puede tener varias relaciones con valores de impacto.

Campus universitario Sangolquí: Av. Gral. Rumiñahui s/n **Telf:** (593-02) 3 989 400
Fax: (593-02) 2334 952 / **Código postal**: 171103 / **Casillero postal:** 71 5 231 • B
Página Web: www.espe.edu.ec I Sangolquí - Ecuador

VAI_VALORIMPACTO y VUL_VULNERABILIDAD	Relación uno a muchos, donde una vulnerabilidad puede tener varias relaciones con valores de impacto.
VAL_VALORACION y VAI_VALORIMPACTO:	Relación uno a muchos, donde un valor de impacto puede tener varias valoraciones.
VUL_VULNERABILIDAD y TVU_TIPOVULNERABILIDAD	Relación uno a muchos, donde un tipo de vulnerabilidad puede tener varias vulnerabilidades relacionadas.

5. Conclusión

La ciberseguridad es un tema de gran importancia en la actualidad debido al aumento de los ataques cibernéticos y la necesidad de proteger la información y los sistemas de las organizaciones. Los avances tecnológicos y la interconexión digital han ampliado las posibilidades de los ciberdelincuentes, lo que ha llevado a un incremento en la sofisticación y frecuencia de los ataques.

Existe una necesidad urgente de contar con un enfoque sistemático y estructurado para la identificación y evaluación de riesgos en ciberseguridad. Las organizaciones deben adoptar un modelo de madurez y un marco de trabajo que les permita abordar eficazmente los desafíos asociados a la ciberseguridad y proteger su información y sistemas de manera efectiva.

La implementación de medidas de protección adecuadas y la respuesta eficiente en caso de incidentes son elementos fundamentales para mitigar los riesgos de los ataques cibernéticos. Las organizaciones deben contar con políticas y procedimientos claros, así como con capacitación y concientización continua para su personal, a fin de mejorar su postura de ciberseguridad y minimizar los impactos negativos de los incidentes.

6. Recomendaciones

- Desarrollar y adoptar un modelo de madurez en ciberseguridad que permita a las organizaciones evaluar su estado actual y establecer metas para mejorar su postura de seguridad de la información.
- Implementar un marco de trabajo que proporcione directrices claras sobre las mejores prácticas en ciberseguridad, incluyendo la identificación y evaluación de riesgos, la selección y aplicación de controles de seguridad, y la gestión de incidentes.
- Mantenerse actualizado sobre las últimas tendencias y amenazas en ciberseguridad, y colaborar con expertos y organizaciones del sector para compartir información y mejores prácticas.

Campus universitario Sangolquí: Av. Gral. Rumiñahui s/n **Telf:** (593-02) 3 989 400
Fax: (593-02) 2334 952 / **Código postal**: 171103 / **Casillero postal:** 71 5 231 • B
Página Web: www.espe.edu.ec I Sangolquí - Ecuador

- Realizar evaluaciones periódicas de la postura de ciberseguridad de la organización, a través de auditorías internas o externas, con el fin de identificar áreas de mejora y tomar acciones correctivas.

Campus universitario Sangolquí: Av. Gral. Rumiñahui s/n **Telf:** (593-02) 3 989 400
Fax: (593-02) 2334 952 / **Código postal**: 171103 / **Casillero postal:** 71 5 231 • B
Página Web: www.espe.edu.ec I Sangolquí - Ecuador