UNIVERSIDAD NACIONAL

SANTIAGO ANTÚNEZ DE MAYOLO

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

# SISTEMA DE INFORMACIÓN DE PROTECCIÓN DE DATOS PARA MEJORAR EL CUMPLIMIENTO DEL REQUISITO 7 DEL ESTÁNDAR DE SEGURIDAD DE DATOS PARA LA INDUSTRIA DE TARJETA DE PAGO PARA UN DATAWAREHOUSE EN UNA ENTIDAD BANCARIA EN EL PERÚ, 2022

TÉSIS PARA OPTAR EL TÍTULO DE:

INGENIERO DE SISTEMAS E INFORMÁTICA

PRESENTADO POR:
Bachiller. MAGUIÑA JAVIER, CARLOS EDUARDO

ASESOR:
Dr. MEDINA VILLACORTA, ALBERTO MARTÍN

HUARAZ – PERÚ

N° Registro: T128

2022

## DEDICATORIA

*A Dios, por brindarme la vida, y cuidar de mi persona.*

*A mi madre por su constante apoyo y amor incondicional.*

*A mis hijas Danira, Annalucia por ser mi luz y mi motivo constante.*

## AGRADECIMIENTO

*A la Universidad Nacional Santiago Antúnez de Mayolo,*
*y a todos los Integrantes de la comisión Programa de Titulación*
*de Tesis Guiada (PTTG) que nos dieron su apoyo y*
*guía constante para la realización del proyecto.*
*A mi asesor por su apoyo y gran compromiso permitió*
*Pudiera completarse el objetivo planteado.*

.

# ÍNDICE GENERAL

## RESUMEN

El presente estudio tiene como objetivo mejorar el cumplimiento del requisito 7 del estándar de seguridad de datos para la industria de tarjeta de pago (PCI DSS de sus siglas en inglés) para un datawarehouse legacy en una entidad bancaria en el Perú, implementando un sistema de información de protección de datos la cual busca la automatización y establecer medidas solidas de control de acceso y mecanismos de seguridad el cual permita abordar los diferentes aspectos requeridos por el estándar. Y con ello permitirle a la entidad bancaria cerrar las brechas de seguridad existente sobre este componente legacy y contribuir de manera significativa con la mejora del cumplimiento del estándar.

La investigación que se ha desarrollado es de tipo explicativo y longitudinal, con un diseño pre-experimental, realizado con una muestra de 20 profesionales relacionados al área de seguridad y auditoria. Como técnica principal se utilizó la encuesta y como instrumento un cuestionario, considerando en su elaboración los aspectos relevantes que exige el estándar y de los cuales se pretende dar mejora con el sistema de información. Adicionalmente para medir el grado de asociación entre dos muestras relacionadas y determinar si existe diferencia entre ellas se utilizó la prueba no paramétrica de Wilcoxon; el cual fue seleccionado por la prueba de normalidad realizada a las muestras.

Se obtuvo como error calculado (0.000085) que fue menor al establecido (0.05); ello nos permitió asumir que existe diferencias significativas entre los resultados del pretest y postest al que fue sometido la variable dependiente. Por otro lado, para concluir que la diferencia identificada fue de mejoría, acompañamos el resultado con la comparación del valor de la media del postest (101.45) que fue mayor al valor del pretest (27.05), concluyendo que la implementación del sistema de información de protección de datos mejora el cumplimiento del requisito 7 del estándar PCI DSS.



**Palabras Clave:** PCI-DSS, Datawarehouse Legacy, Protección de datos, Sistema de Información, Control de acceso, Mecanismos de seguridad

**ABSTRACT**

The objective of this study is to improve compliance with requirement 7 of the data security standard for the payment card industry (PCI DSS) for a legacy data warehouse in a bank in Peru, implementing a security system data protection information which seeks the automation and establishment of solid access control measures and security mechanisms which allow addressing the different aspects that are evaluated by the standard. And with this, allow the bank to close existing security gaps on this legacy component and contribute significantly to improving compliance with the standard.

The research that has been developed is of an explanatory and longitudinal type, with a pre-experimental design, carried out with a sample of 20 professionals related to the area of security and auditing. The survey was used as the main technique and a questionnaire was used as an instrument, considering in its elaboration the relevant aspects required by the standard and of which it is intended to improve with the information system. To measure the degree of association between two related samples and determine if there is a difference between them, the Wilcoxon non-parametric test was used; which was determined by the normality test performed on the samples.

It was obtained as a calculated error (0.000085) that was less than the established one (0.05); This allowed us to assume that there are significant differences between the results of the pretest and posttest to which the dependent variable was submitted. On the other hand, to conclude that the difference identified was one of improvement, we accompany the result with the comparison of the post-test mean value (101.45) was greater than the pre-test value (27.05), concluding that the implementation of the protection information system of data improves compliance with requirement 7 of the standard.

**Keywords:** PCI-DSS, Datawarehouse Legacy, Data Protection, Information System, Access Control, Security Mechanisms.

# I. INTRODUCCIÓN

## 1.1. Planteamiento del Problema

En la actualidad, los bancos de todo el mundo están vigilando un nuevo paradigma de riesgo; una que engloba tanto amenazas físicas y cibernéticas, como el robo de identidad, el acceso a datos sensibles, la fuga de información y con ello la presencia de fraudes, las estafas y el phishing. Los bancos principalmente son víctimas de delincuentes informáticos que buscan robar información corporativa o fondos monetarios, y estos delincuentes cada vez logran hacerse más sofisticados en sus planes tanto desde un contexto externo e interno.

Según el informe publicado por (Allianz Global Corporate, 2022) las entidades financieras se enfrentan a un periodo de grandes riesgos siendo el mayor de todos aquellos relacionados a incidentes de ciberseguridad y fraude.

Por Otro lado, el informe publicado por (KPMG S.A., 2019) nos muestra ya una perspectiva global de cómo los bancos están abordando las amenazas de fraude internas y externas. Se preguntó a los encuestados sobre las tendencias en las tipologías de fraude, los desafíos que enfrentan para mitigar las amenazas, la seguridad en la era digital y cómo están estructurando sus equipos y desplegando recursos para optimizar sus esfuerzos de gestión de riesgos de fraude. A continuación, se listan algunas de las conclusiones más resaltantes:

- Más de la mitad de los encuestados en todo el mundo experimentaron aumentos tanto en el valor total como en el volumen del fraude externo. El aumento de las tipologías de fraude en todo el mundo desde 2015 hasta 2018 incluye el robo de identidad y la toma de posesión de la cuenta, los ataques cibernéticos, las tarjetas sin fraude y las estafas autorizadas de pago automático.

- Más de la mitad de los encuestados recuperan menos del 25 por ciento de las pérdidas por fraude; Demostrando que la prevención del fraude es clave. Los bancos están invirtiendo en nuevas tecnologías para prevenir el fraude.
- En cada región, los bancos encuestados consideraron que el desafío más importante en el riesgo de fraude son los ciberataques.

- Los bancos a nivel mundial están viendo una tendencia creciente en las estafas. Los estafadores están manipulando y obligando a los clientes a hacer pagos a ellos, sin pasar por los controles bancarios.
- Los clientes son clave en la prevención y detección de actividades fraudulentas en sus cuentas, especialmente para reducir las pérdidas por estafa. Se debe hacer más para educar a los clientes sobre fraudes y estafas.
- La Banca Abierta se considera un desafío importante en el riesgo de fraude de los bancos, ya que los bancos de todo el mundo se están preparando para abrir sus puertas a terceros para acceder a los datos de sus clientes.
- Los estafadores son cada vez más sofisticados y pueden cambiar y adaptar rápidamente sus enfoques. Los bancos deben ser ágiles para responder a las nuevas amenazas y adoptar nuevos enfoques y tecnologías para predecir y prevenir el fraude

En el contexto latinoamericano las empresas en la región están experimentando crecientes pérdidas por fraude, infracciones de cumplimiento y ciberataques, y se espera que la situación empeore en los próximos 12 meses, según la encuesta (KPMG , 2022). El cual también cita que el fraude, los ataques cibernéticos y los riesgos de incumplimiento regulatorio están creciendo a un ritmo alarmante. Estas problemáticas convergen en un ciclo de amenaza que repercute en pérdidas económicas para las organizaciones, amenaza su reputación y las expone a sanciones por parte de reguladores.

Por otro lado el sector financiero nacional no es ajeno a esta realidad, en los últimos años ha experimentado eventos por riesgo operacional, y específicamente fraude realizado por su propio personal como sustento de ello, en junio de 2017 el Banco de Crédito del Perú sufrió un fraude por S/ 5 millones cuando una cajera realizó un desvío de fondos según lo publicado por el (Diario Gestión, 2017); otro caso de conocimiento público, es el caso Cromwell, donde un funcionario del banco BBVA, utilizó para beneficio personal la falta de control en los programas del banco, malversando fondos a cuentas propias y de terceros (Paéz, Libón, & Hidalgo, 2003).

La participación de los bancos representa aproximadamente el 90% de los activos del sistema financiero, siendo un gran aporte para el desarrollo económico del país (SBS, 2017b), es por ello la importancia de identificar las buenas prácticas en la gestión del riesgo de fraude interno. Contar con buenas prácticas en la gestión de este riesgo es importante por

el gran impacto económico y social, asociado a la reputación y seguridad que perciben los clientes de las entidades bancarias

Por lo expuesto, actualmente la entidad objeto de estudio es un grupo financiero global fundado en 1857 con una visión centrada en el cliente. Tiene una posición de liderazgo en el mercado español, es la mayor institución financiera de México y cuenta con franquicias líder en América del Sur y en Nuestro país se ha transformado en una empresa de referencia en el país no solo por sus resultados económicos, sino también por sus altos índices de reputación que lo constituyen en una entidad de confianza para todos los peruanos (en razón de ello debido a la política de confidencialidad, privacidad se omite en el estudio la mención del nombre comercial) . De igual manera cabe resaltar el banco se suma al intenso proceso de digitalización de los servicios y productos que contribuyen decididamente a convertir en realidad el propósito que impulsa las voluntades de los miles personas que laboran en esta institución: poner al alcance de todos los peruanos las oportunidades de esta nueva era.

Es así que dentro de todos los procesos y sistemas con los que cuentan se ha podido identificar la existencia de una problemática que conlleva a la presencia de un riesgo de fuga de datos, específicamente identificado en el único datawarehouse local legacy que dispone el Banco (teniendo como motor de base de dato un Oracle 11g). Que por su condición "legacy" o sistema heredado, nació sin un con un sistema de control ya que el contexto en el que nació era ya hace más de 10 años, y que en la actualidad al ser un sistema legacy ya no se agregan nuevos procesos o modelos de Información, No contando así con disposición de presupuesto de inversión para upgrades o mejoras en la implementación de aplicaciones de seguridad esto debido a que el Banco se encuentra como política corporativa en proceso de migración de toda la informacional en una única plataforma global de Big data propia de la Compañía.

Si bien la condición de riesgo de este sistema legacy es aminorado en gran medida por las acciones que comprende el cumplimiento de la Política General de Seguridad de la Información y Ciberseguridad de la compañía y en el estricto cumplimiento de las regulaciones Nacionales tales como Ley Nº 29733 - Ley de protección de datos personales, Resolución SBS N° 504-2021: Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, Resolución SMV Nº 027-2016-SMV/01:Reglamento de Gestión del Riesgo Operacional, Resolución SBS N° 6523-2013: Reglamento de Tarjetas de Crédito y Débito y en especial el cumplimiento del estándar Internacional PCI-

DSS (Payment Card Industry-Data Security Standard) del cual en el proceso de cumplimiento y análisis de los requisitos que exige el mismo, se ha podido identificar una brecha de seguridad.

En tal sentido surge como necesidad primordial eliminar la brecha de seguridad identificada y así aminorar el riesgo de la concreción de fraudes por fugas de información e incidentes de ciberseguridad que puedan acarrear la presencia de la Brecha, generando así un gran impacto a nivel de cumplimiento regulatorio, siendo no solo para el banco uno de los mayores compromisos, sino también como para toda la industria de servicios financieros, y para las regulaciones crecientes en torno a la ciberseguridad y el entorno tecnológico que vivimos, aquel que se encuentra en constante evolución. toman un gran alcance en el sector financiero y que derivan en su gran medida en mayores multas, litigios y más por sobre todo un impacto negativo de imagen.

Es por ello que el banco y en general las empresas de los servicios financieros al trabajar con información altamente sensible que incluye datos personales y registros financieros, son de alto interés para un ciber-atacante. Y para asegurar que estos datos sensibles se protejan de forma apropiada, surge la necesidad de Diseñar e implementar un sistema de información que nos permita controlar el acceso a datos sensibles de todos los usuarios (internos y proveedores) que consumen la informacional almacenada, esto teniendo como base el establecimiento de políticas de control de acceso configurables, complementando así a los roles de Seguridad que dispone actualmente la Base de datos. De igual forma adicionar mecanismos de control de granularidad sobre lo que puede y debe ver una persona en base a mecanismos lógicos de ofuscamiento o enmascaramiento de los datos en tiempo de ejecución. Salvaguardando así la seguridad de los Datos tomando en cuenta las diferentes fases que esta conlleva. Permitiéndonos así disponer de un rastro de que, quienes y de qué forma se están usando los datos.

El sistema de información que se implementó, indudablemente aportará enormemente al cierre de la brecha de seguridad identificada en este Datawarehouse legacy. Y que a su vez permitan el cumplimiento del del estándar de seguridad de datos para la industria de tarjeta de pago (en adelante PCI-DSS por sus siglas en inglés Payment Card Industry Data Security Standard) y en especial énfasis en el del requisito 7 que requiere la implementación de medidas solidas de control de acceso a los datos relacionados a titulares y tarjetas de medio

de pago, cumpliendo de igual forma con las regulaciones Nacionales e internacionales en el marco del tratamiento de los datos Personales.

## 1.2. Formulación del Problema

### 1.2.1. Problema General

¿En qué medida la implementación de un sistema de información de protección de datos mejora el cumplimiento del requisito 7 del estándar de seguridad de datos para la industria de tarjeta de pago para un datawarehouse en una entidad bancaria en el Perú?

### 1.2.2. Problemas Específicos

- ¿En qué medida la implementación de un sistema de información de protección de datos mejora el control de acceso de un datawarehouse en una entidad bancaria en el Perú?
- ¿En qué medida la implementación de un sistema de información de protección de datos mejora el mecanismo de seguridad de un datawarehouse en una entidad bancaria en el Perú?

## 1.3. Objetivos de la Investigación

### 1.3.1. Objetivos General

Mejorar el cumplimiento del requisito 7 del estándar de seguridad de datos para la industria de tarjeta de pago para un datawarehouse mediante la implementación de un sistema de información de protección de datos en una entidad bancaria en el Perú.

### 1.3.2. Objetivos Específicos

- Mejorar el control de acceso con la implementación de un sistema de información de protección de datos para un datawarehouse en una entidad bancaria en el Perú.

- Mejorar el mecanismo de seguridad con la implementación de un sistema de información de protección de datos para un datawarehouse en una entidad bancaria en el Perú.

## 1.4. Justificación

### 1.4.1. Justificación Operativa

El banco dentro de su operativa y al trabajar con información altamente sensible que incluye datos personales y registros financieros, tiene la necesidad de asegurar que estos datos sensibles se protejan de forma apropiada, surge por ello la necesidad de Diseñar e implementar un sistema de información que permita controlar el acceso a datos sensibles que son almacenados y que son disponibilizados a los usuarios y áreas de negocio (internos y proveedores) de forma oportuna en el marco del cumplimiento del estándar internacional PCI-DSS.

### 1.4.2. Justificación Económica

El proyecto es considerado económicamente viable dado que todos los costos que se desprenden de las actividades de análisis, diseño, construcción e implementación serán asumidos íntegramente por el tesista ya que este sistema no generara ningún compromiso de gasto sobre licencias, ya que está diseñado sobre el uso de plataformas licenciadas ya homologadas y estandarizadas por el banco, tomando como base la arquitectura computacional que dispone; sin incurrir en la compra de equipos que implementen servicios para la solución que se plantea.

### 1.4.3. Justificación Social

El presente proyecto permite, de igual manera elevar la protección de la información sensible de los clientes, conllevando así la reducción de la fuga de información que puedan generar algún riesgo de perpetración de fraude y afectación a los clientes del banco.

### 1.4.4. Justificación Legal

El Presente Proyecto está amparado en la normativa nacional adoptados por el banco, tanto en la protección de la información en la salvaguarda de la confidencialidad de la información, las cuales son:

- Ley Nª 29733 - Ley de protección de datos personales, Resolución SBS N° 504-2021.
- Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad
- Resolución SBS N° 6523-2013: Reglamento de Tarjetas de Crédito y Débito

### 1.4.5. Justificación Tecnológica

El presente proyecto también se considera como innovador, permitiendo servir como un referente a nivel institucional en las diferentes áreas de negocio del Banco, en función al despliegue de controles de controles de aseguramiento del control de acceso a Datos sensibles en ambientes Legacy, permitiendo así el cumplimiento de estándares, tales como:

- Decreto Legislativo N° 1412 - Ley de gobierno digital
- Reglamento General de Protección de Datos (RGPD) de la Unión europea.
- Estándar internacional PCI-DSS.

# II. MARCO TEÓRICO

## 2.1 Antecedentes de la Investigación

Para abordar los antecedentes que sirvieron de base a la investigación en referencia, se procedió a la revisión de algunos estudios relacionados con el problema, los cuales incorporaron elementos de relevancia.

### 2.1.1. Antecedentes Nacionales

Navarro (2019) En su investigación presenta una metodología de implementación del estándar PCI-DSS en el diseño de red en una entidad bancariala cual permitio la implementación de medidas correctivas en su diseño y arquitectura de red con la finalidad de reducir el entorno sobre el que las auditorías de las compañías de tarjetas de pago evalúan el cumplimiento de la norma. El diseño y arquitectura de red se desarrolla a partir de la protección perimetral de la red con la implementación de firewalls, sistemas de detección y prevención de intrusos y la segmentación de la red interna actual separando los sistemas que deben de cumplir con los requisitos de la norma de las demás redes. Asimismo, muestra los requisitos de configuración que deben de cumplir cada uno de los componentes necesarios en el diseño.

Cuadros (2019) Trata sobre la implementación de un SIEM (Security Information and Event Management) que significa Sistema de gestión eventos e información de seguridad en la empresa Globokas Perú, la cual estaba en un proceso de auditoría para poder obtener la certificación de cumplimiento de la norma PCI DSS v3.2. para lo cual utilizó una herramienta informática llamada USM AlienVault la cual, según sus muchos beneficios, costo de la implementación y licencia en comparación de otras herramientas pagadas del mercado de los SIEMs. Se estableció que esta herramienta ayudo al cumplimiento de los requisitos 10 y 11 de la norma PCI DSS, el cual nos indica que se debe de almacenar los registros de auditoria de todos los componentes tecnológicos de la empresa tales como servidores, equipos de comunicación (firewall y routers) así como también se debe de realizar análisis de vulnerabilidades a los equipos tecnológicos descritos.

Lavado (2019) En tuvo como propósito la implementación de un software SIEM (Log360) para el cumplimiento del requisito 10 del estándar PCI DSS, teniendo en consideración que para el desarrollo del proyecto se utilizó una variación de la metodología PDCA adaptada a las necesidades de la organización y aprobada por la unidad de cumplimiento normativo del banco. Se utilizó un cuestionario elaborado por el ente que desarrolló la normativa en estudio, a fin de identificar la situación actual de la entidad financiera y, con dicha información, se realizó un análisis de brechas, utilizando la metodología GAP de análisis para determinar los puntos a mejorar. Se usó herramientas de gestión de proyectos para la elaboración del plan de trabajo y para el rastreo de la realización de los procesos durante la implementación del control de seguridad. Por último, debido al proceso de mejora continua, se verificó nuevamente el nivel de cumplimiento del objetivo. Como resultado, la entidad financiera automatizó el proceso de auditoría de registros de eventos de los componentes que transmiten, procesan y almacenan data confidencial durante una transacción de pago; además, tiene visibilidad de lo que sucede en la red, por lo que está en la capacidad de detectar amenazas y anomalías en el comportamiento de usuarios utilizando tecnologías emergentes, como la inteligencia artificial.

Cuadros, Huacac (2018) En su investigación Asignación y control de roles de los usuarios para mejorar la seguridad de acceso a los sistemas de una entidad bancaria tuvo como fin implementar un sistema de gestión de identidades y roles que permita mejorar la administración de permisos a usuarios y la gestión de asignación de roles a fin de mitigar riesgos potenciales de vulnerabilidades en la entidad bancaria, reduciendo tiempos y costos en la asignación de roles e implementar notificaciones automáticas de los permisos modificados a los usuarios.

### 2.1.1. Antecedentes Internacionales

Orellana y Tamallo (2020) Elaboración de una propuesta de mejora de la seguridad de la información en una institución financiera basada en la norma PCI DSS, proponen la mejora de la seguridad de la información en una institución financiera basada en controles que indica la norma PCI DSS, se

plantea un estudio de las mejores prácticas del manejo información dentro de una institución financiera, involucrando a todas las personas que participan en el ciclo de mejora de la Seguridad de la Información, pero en esta propuesta de mejora como tema principal se va a conocer la norma PCI DSS en la cual participan personas, procesos y sistemas que almacenen, transmitan o procesar los datos de tarjetahabiente de todos los clientes de alguna institución financiera.

Benenaula y Ortega (2016) en su estudio Auditoría de sistemas al cumplimiento de los requerimientos 7, 8, 9 de la norma PCI DSS aplicada a Coral Hipermercado, teniendo en consideración la demanda que mantienen y el nivel de transacciones que realizan en ventas diariamente, y en el uso de sus diversas formas de pago entre ellas las tarjetas de pago, genera la necesidad de salvaguardar la seguridad de los datos ante actos maliciosos, han visto necesaria la implementación obligatoria de la Normativa PCI DSS. De esta manera a través de su investigación se obtuvo conocimiento de que la empresa Coral Hipermercado GO no ha realizado anteriormente una auditoria de la Normativa PCI DSS, por lo que la implementación de la Normativa podría no ser completa o apropiada, las políticas de la empresa pueden no contener los procesos y procedimientos que se deben llevar a cabo, haciendo que la seguridad de accesos a los datos de los titulares de tarjetas se vean vulnerables, de igual manera el manejo de las autenticaciones y la infraestructura de la seguridad física, misma que permite el resguardo de los equipos y por ende de la información.

Polo y Chaparro (2020) Guías para la construcción de la política de seguridad de la información y mejorar el nivel de concientización, basado en los requisitos 12.1 y 12.6 de la norma PCI DSS en empresas del gremio de los call center, realizó una investigación mediante la realización de una encuesta aplicada a 20 empresas de Call Center1, con la cual reafirma la importancia de la política de seguridad de la información como uno de los pilares para la protección de datos y seguridad de los activos de la organización, conforme a los requisitos que actualmente son sugeridos por una serie de normas que regulan y protegen los datos de los usuarios como son PCIDSS, adicionalmente se pretendió orientar y generar conciencia en las empresas de Call center en la importancia de tener una política de seguridad de la información en la empresa, lo cual permite la

protección de los datos de sus clientes en cuanto a la disponibilidad, integridad y confidencialidad de estos, ya que genera beneficios como toma de conciencia de la seguridad de la información por parte de todo el personal de la organización, proveedores y terceros, incentiva el uso adecuado de la información, uso correcto de activos y la mitigación de ataques producidos por ingeniería social ya que estos marcan una tendencia para este año con un 13.5% de los caso reportados.

## 2.2. Bases Teóricas

### 2.2.1. Sistema de Información

Sistema de Información según Peña, Dangel (2008) es "Un conjunto de elementos interrelacionados con el propósito de prestar atención a los requisitos de información de una organización, para contribuir y sumar el nivel de conocimientos que permitan un mejor apoyo a la toma de decisiones y desarrollo de acciones" pág. 20.

Los elementos que interactúan entre sí son:

- El equipo computacional. Se refiere al hardware, el cual se necesita para poder operar los sistemas de información.
- El recurso humano. Lo conforman las personas que están relacionadas con el sistema.
- Los datos. Son la fuente que es introducida en el sistema la cual será procesada para retornar un resultado.
- Los programas. Se refiere al software que va a recibir la información suministrada, la procesa y devolverá un resultado.
- Las telecomunicaciones. Lo conforman el hardware y software quienes contribuyen con la transmisión de la información de forma digital.
- Procedimientos. Todo procedimiento se encuentra incluido dentro de las reglas y políticas bajo las cuales se va a operar en el aspecto funcional del proceso.

Un sistema de información realiza cuatro actividades básicas:

- Entrada: Se toman los datos.

- Almacenamiento: por hardware o archivos físicos para conservar la información.
- Procesamiento: permite la transformación de los datos fuente en información que puede ser utilizada para la toma de decisiones
- Salida: es la capacidad del sistema para producir la información procesada o sacar los datos de entrada al exterior.

**Tipos de sistemas de información**

Según Castellanos (2011) los sistemas de información pueden clasificarse en:

- Sistemas Transaccionales: automatizan tareas operativas de la organización.
- Sistemas de Apoyo de las Decisiones: brindan información que sirve de apoyo a los mandos intermedios y a la alta administración en el proceso de toma de decisiones.
- Sistemas Estratégicos: generan ventajas que los competidores no posean, tales como ventajas en costos y servicios diferenciados con clientes y proveedores.
- Sistema Planificación de Recursos (ERP – Enterprise Resource Planning): integran la información y los procesos de una organización en un solo sistema (Pág 8)

### 2.2.2. Seguridad de la información

La norma ISO/IEC 27001 define a la seguridad de la información como aquel conjunto de medidas preventivas y reactivas que acoge una organización o sistema tecnológico para permitir el resguardo y protección la información teniendo considerando como base los siguientes principios:

- Confidencialidad. Es la propiedad que asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.
- Disponibilidad. Es la característica de la información de encontrarse a disposición de quienes deben acceder a ella en el momento que así lo requieran.

- Integridad. Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.

Recapitulando lo anterior, el concepto de seguridad de la información contempla 3 elementos importantes para identificar la información a proteger:

- **Crítica:** Esto quiere decir que la información es indispensable para el funcionamiento y operación de la institución o empresa.
- **Valiosa:** Como lo mencionamos, son activos indispensables de las instituciones, por lo tanto, deben ser resguardadas y protegidas para evitar poner en riesgo el futuro de la organización.
- **Sensible:** Esto significa que solo debe ser conocida por las personas autorizadas por la organización.

Como complemento a lo anterior, existen dos conceptos que es importante a considerar para comprender el tema:

- **Riesgo:** Es la materialización de las vulnerabilidades que están identificadas en la institución y que resulta de la combinación de la probabilidad que suceda un evento no deseable y su impacto negativo a la organización.
- **Seguridad:** Es la forma en que la institución se protege de los riesgos.

### 2.2.3. Seguridad de Datos

(Power Data, 2022) Se refiere a medidas de protección de la privacidad digital que se aplican para limitar el acceso no autorizado a los datos, los cuales pueden encontrarse en ordenadores, bases de datos, sitios web, etc. La seguridad de datos también protege los datos de una posible mala manipulación.

Seguridad de datos incluye conceptos como encriptación de datos, tokenización y prácticas de gestión de claves que ayudan a proteger los datos en todas las aplicaciones y plataformas de una organización.

**Tipos de medidas y técnicas de seguridad de datos**

No existe una única técnica que pueda resolver todos los problemas de seguridad de datos, pero existen varias soluciones que, combinadas, pueden fortalecer la protección de datos de una organización.

- **El cifrado,** utiliza un algoritmo para codificar los datos en un formato ilegible, de modo que solo los usuarios autorizados puedan leerlos. Este algoritmo se denomina clave de cifrado. Las soluciones de seguridad de datos utilizan el cifrado para proteger los datos, por lo que, en caso de una infracción, el atacante no puede leerlos.
- **El borrado de datos**, es más seguro que el borrado de datos, ya que utiliza un algoritmo para sobrescribir los datos en cualquier dispositivo de almacenamiento. Luego, los datos son irrecuperables.
- **El enmascaramiento de datos**, oculta los datos mediante la creación de una versión falsa pero realista de los datos de su organización. Esta técnica tiene como objetivo proteger los datos confidenciales mientras se utiliza una alternativa funcional o una versión ficticia. El enmascaramiento de datos mantiene el formato, pero cambia los valores de los datos al mezclarlos, sustituir caracteres o usar el cifrado de datos.
- **La resiliencia de datos** implica la implementación de varias prácticas para garantizar la integridad de los datos en caso de desastre o falla. El desastre puede variar desde una falla de hardware hasta un corte de energía y ataques cibernéticos. Las prácticas comunes incluyen copias de seguridad de datos programadas con frecuencia, redundancia y copias de seguridad en la nube.
- **El control de acceso** incluye limitar el acceso físico y digital a recursos y datos críticos. Por lo general, implica proteger dispositivos con credenciales de inicio de sesión. Del mismo modo, las medidas de autenticación identifican a los usuarios antes de que puedan acceder al sistema o a los datos a través de tokens de seguridad, datos biométricos, contraseñas, números de identificación u otras medidas.

### 2.2.4. Sistema de Control de Acceso

(Microsoft, 2022) El control de acceso es un componente fundamental de la seguridad de los datos que dicta quién tiene permiso para acceder a y usar información y recursos de la empresa. Mediante la autenticación y autorización, las políticas de control de acceso se aseguran de que los usuarios sean quienes dicen ser y tengan acceso apropiado a los datos de empresa. También se puede aplicar el control de acceso para limitar el acceso físico a los campus, edificios, habitaciones y centros de datos.

Existen cuatro tipos de control de acceso principales. Las organizaciones suelen elegir el método que tiene más sentido según sus requisitos de seguridad y cumplimiento normativo únicos. Los cuatro modelos de control de acceso son:

- **Control de acceso discrecional (DAC):** en este método, el propietario o administrador del recurso, los datos o el sistema protegido establece las políticas de a quién se permite acceso.
- **Control de acceso obligatorio (MAC):** en este modelo no discrecional, se garantiza a las personas el acceso basándose en una autorización de información. Una autoridad central regula los derechos de acceso basándose en distintos niveles de seguridad. Este modelo es común en entornos gubernamentales y militares.
- **Control de acceso basado en funciones (RBAC):** RBAC concede acceso basándose en funciones empresariales definidas, en vez de la identidad del usuario individual. El objetivo es proporcionar a los usuarios acceso solo a datos que se hayan considerado necesarios para sus funciones en la organización. Este método de amplio uso se basa en una combinación compleja de asignaciones de funciones, autorizaciones y permisos.
- **Control de acceso basado en atributos (ABAC):** en este método dinámico, el acceso se basa en un grupo de atributos y entornos medioambientales, como la hora del día y la ubicación, asignado tanto a usuarios como a recursos.

**Importancia del Control de Acceso**

El control de acceso impide que la información confidencial, que incluye los datos de los clientes, información identificable personalmente y propiedad intelectual, caiga en malas manos. Es un componente clave del moderno marco de seguridad de confianza cero, que utiliza varios mecanismos para verificar continuamente el acceso a la red de la empresa. Sin políticas sólidas de control de acceso, las organizaciones se arriesgan a una fuga de datos tanto por fuentes internas como externas.

### 2.2.5. Datawarehouse Legacy

(Power Data, 2022) Una data warehouse es un repositorio unificado para todos los datos que recogen los diversos sistemas de una empresa, que permite a los ejecutivos de negocios organizar, comprender y utilizar sus datos para tomar decisiones estratégicas. El repositorio puede ser físico o lógico y hace hincapié en la captura de datos de diversas fuentes sobre todo para fines analíticos y de acceso.

Normalmente, una data warehouse se aloja en un servidor corporativo o cada vez más, en la nube. Los datos de diferentes aplicaciones de procesamiento de transacciones Online (OLTP) y otras fuentes se extraen selectivamente para su uso por aplicaciones analíticas y de consultas por usuarios.

Históricamente, los datawarehouse se habían formado utilizando datos repetitivos estructurados que eran filtrados antes de entrar en la data warehouse. Sin embargo, en los últimos años, la data warehouse ha evolucionado debido a información contextual que ahora se puede adjuntar a los datos no estructurados y que también puede ser almacenada.

**Estructuras de un Data Warehouse**

La arquitectura de una data warehouse puede ser dividida en tres estructuras simplificadas: básica, básica con un área de ensayo y básica con área de ensayo y datamarts.

- **Con una estructura básica**, sistemas operativos y archivos planos proporcionan datos en bruto que se almacenan junto con metadatos. Los usuarios finales pueden acceder a ellos para su análisis, generación de informes y minería.
- **Al añadir un área de ensayo** que se puede colocar entre las fuentes de datos y el almacén, ésta proporciona un lugar donde los datos se pueden limpiar antes de entrar en el almacén. Es posible personalizar la arquitectura del almacén para diferentes grupos dentro de la organización.
- **Se puede hacer agregando datamarts**, que son sistemas diseñados para una línea de negocio en particular. Se pueden tener datamarts separados para ventas, inventario y compras, por ejemplo, y los usuarios finales pueden acceder a datos de uno o de toda la datamarts del departamento.

### 2.2.6. Estándar PCI DSS

(Acosta, 2022) El Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (Payment Card Industry Data Security Standard – PCI DSS) es un estándar de seguridad publicado por el PCI SSC y orientado a la definición de controles para la protección de los datos del titular de la tarjeta y/o datos confidenciales de autenticación durante su procesamiento, almacenamiento y/o transmisión.

Antes de la publicación de la primera versión del estándar PCI DSS, cada una de las marcas de tarjetas de pago que actualmente hacen parte del PCI SSC contaban con un programa propio de seguridad para la protección de los datos del titular de tarjeta:

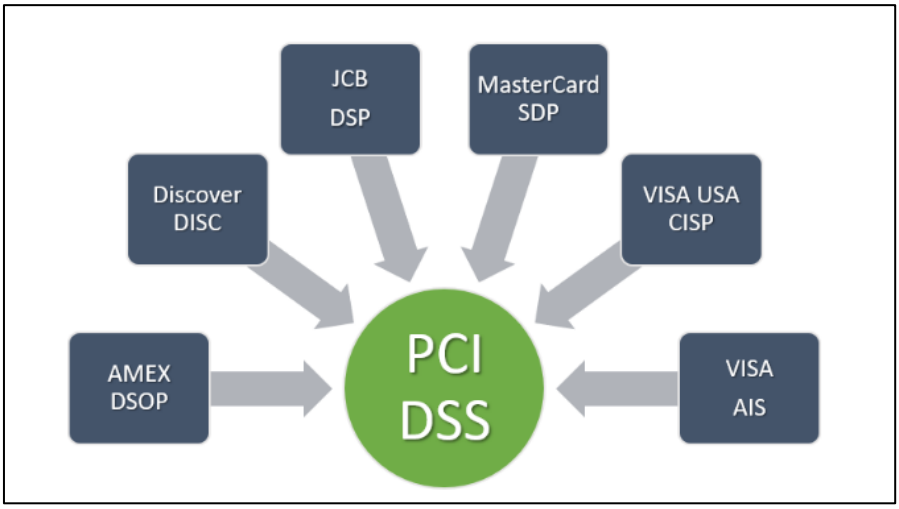
- American Express – **Data Security Operating Policy** (DSOP)
- Discover – **Discover Information Security Compliance** (DISC)
- JCB International – **Data Security Program** (DSP)
- MasterCard – **Site Data Protection** (SDP)
- Visa USA – **Cardholder Information Security Program** (CISP)
- Visa International – **Account Information Security Program** (AIS)

Cada uno de estos programas definía los controles de seguridad a implementar, las entidades que debían cumplir con dichos controles, los procesos de reporte de cumplimiento y las sanciones y multas en caso de incumplimiento. No obstante, esto implicaba que, si una entidad almacenaba, procesaba y/o transmitía datos de tarjetas

pertenecientes a cualquiera de estas marcas entonces tenía que cumplir con su programa de seguridad relacionado, lo cual creaba duplicidades, incongruencias y solapamientos en la implementación de controles, sin contar la carga burocrática que conllevaba la gestión y reporte.

**Figura 1**

*Unión de los programas de cada una de las marcas en el PCI DSS*




**Nota:** Gráfico Obtenido de www.pcihispano.com

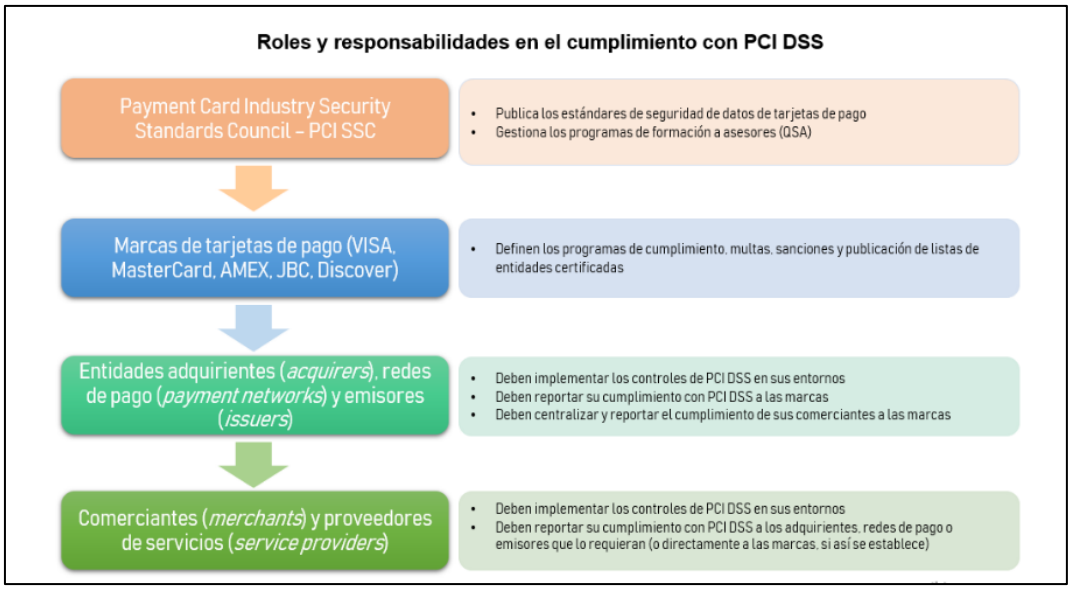
Todo esto llevó a que las marcas de pago definieran un estándar único que cumpliera con los requerimientos y expectativas de seguridad de forma transversal, evitando los problemas citados anteriormente y facilitando una adopción masiva en las entidades afectadas. Por ello, el 14 de diciembre de 2004 se publicó la versión 1.0 del Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (*Payment Card Industry Data Security Standard* – PCI DSS).

Sin embargo, es importante aclarar que con la publicación del estándar PCI DSS los programas de seguridad de las marcas de pago no desaparecieron, ya que la responsabilidad en la definición de las entidades que tienen que cumplir con el estándar, la gestión de los reportes de cumplimiento, la publicación de las listas de entidades certificadas, las acciones en caso de compromiso de datos de tarjetas y los criterios de multas y sanciones siguen siendo administrados por cada marca de forma independiente a través de dichos programas.

De acuerdo con lo descrito anteriormente, los roles y responsabilidades en el cumplimiento del estándar PCI DSS se pueden esquematizar de la siguiente manera:

**Figura 2**

*Descripción de los roles y responsabilidades en el cumplimiento de PCI DSS*




**Nota:** Recuperado www.pcihispano.com

## Aplicabilidad

El estándar PCI DSS está orientado a la protección de los datos del titular de la tarjeta y/o datos confidenciales de autenticación, de acuerdo con la siguiente tabla:

**Figura 3**

*Tipo de datos en una tarjeta de pago*


**Nota**: Fuente de extracción www.pcihispano.com

## Descripción de los controles de seguridad del estándar PCI DSS

El estándar PCI DSS cuenta con más de 250 controles de seguridad física, lógica y administrativa esquematizados en 6 grupos principales que a su vez se subdividen en 12 requerimientos, de la siguiente manera:

**Figura 4**

*Esquema de los requisitos de seguridad del estándar PCI DSS*


**Nota**: Grafico estraido de www.pcihispano.com

Finalmente, el estándar permite el uso de controles alternativos para el cumplimiento de un requerimiento original del estándar cuando existe una justificación de negocio o administrativa que lo requiera. Este tipo de controles se denominan «controles compensatorios» (*Compensating Controls*).

## Entidades que requieren cumplimiento con el estándar

El estándar PCI DSS se aplica a todas las entidades que participan en los procesos de almacenamiento, procesamiento y/o transmisión de datos del titular de la tarjeta y/o datos confidenciales de autenticación de las tarjetas de pago, entre las que se incluyen:

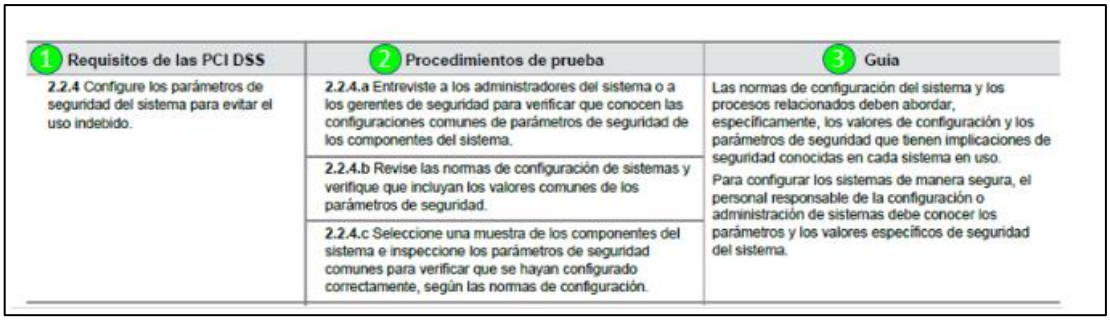
- Comerciantes (*merchants*)
- Procesadores
- Adquirentes (*acquirers*)
- Entidades emisoras (*issuers*)
- Proveedores de servicios de pagos (*service providers*) como pasarelas de pago, centros autorizadores, etc.

**Criterios de evaluación de PCI DSS**

Una de las ventajas del estándar PCI DSS es que el mismo documento del estándar incluye tanto el requisito a cumplir como los procedimientos de prueba para su evaluación y una guía con explicaciones adicionales:

**Figura 5**

*Requisitos, procedimientos de prueba y guías en el estándar PCI DSS*



| 1 Requisitos de las PCI DSS | 2 Procedimientos de prueba | 3 Guía |
|---|---|---|
| **2.2.4** Configure los parámetros de seguridad del sistema para evitar el uso indebido. | **2.2.4.a** Entreviste a los administradores del sistema o a los gerentes de seguridad para verificar que conocen las configuraciones comunes de parámetros de seguridad de los componentes del sistema. | Las normas de configuración del sistema y los procesos relacionados deben abordar, específicamente, los valores de configuración y los parámetros de seguridad que tienen implicaciones de seguridad conocidas en cada sistema en uso.<br>Para configurar los sistemas de manera segura, el personal responsable de la configuración o administración de sistemas debe conocer los parámetros y los valores específicos de seguridad del sistema. |
| | **2.2.4.b** Revise las normas de configuración de sistemas y verifique que incluyan los valores comunes de los parámetros de seguridad. | |
| | **2.2.4.c** Seleccione una muestra de los componentes del sistema e inspeccione los parámetros de seguridad comunes para verificar que se hayan configurado correctamente, según las normas de configuración. | |

**Nota**: Fuente www.pcihispano.com

- **Requisitos de PCI DSS**: Esta columna define los requisitos de las normas de seguridad de datos. El cumplimiento con PCI DSS se validará en comparación con estos requisitos.
- **Procedimientos de pruebas**: Esta columna muestra los procesos que se deben seguir a efectos de validar que los requisitos de PCI DSS se hayan implementado y cumplido. Dentro de estos procedimientos de prueba se encuentran:
    - Realización de entrevistas
    - Revisión de documentación y diagramas
    - Verificación de configuraciones técnicas

- Observación de procesos, acciones y estados

- **Guía**: Esta columna describe la meta o el objetivo de seguridad de cada requisito de PCI DSS. Esta columna es solo una guía y tiene como objetivo ayudar a comprender el objetivo de cada requisito. La guía de esta columna no reemplaza ni extiende los requisitos de PCI DSS ni los procedimientos de pruebas.

### 2.2.7. Oracle Virtual Private Database para el Control de acceso a datos (VPD)

Según (ORACLE , 2022), nos indica que el Oracle Virtual Private Database le (VPD) permite crear políticas de seguridad para controlar el acceso a la base de datos a nivel de fila y columna. Esencialmente, Oracle Virtual Private Database agrega una clausula WHERE dinámica a una declaración SQL que se emite contra la tabla, vista o sinónimo a la que se aplicó una política de seguridad de Oracle Virtual Private Database.

La VPD aplica la seguridad, a un nivel fino de granularidad, directamente en las tablas, vistas o sinónimos de la base de datos. Debido a que adjunta políticas de seguridad directamente a estos objetos de la base de datos y las políticas se aplican automáticamente cada vez que un usuario accede a los datos, no hay forma de eludir la seguridad.

Cuando un usuario accede directa o indirectamente a una tabla, vista o sinónimo que está protegido con una política de Oracle Virtual Private Database, Oracle Database modifica dinámicamente la declaración SQL del usuario. Esta modificación crea una condición WHERE (llamada predicado) devuelta por una función que implementa la política de seguridad. Oracle Database modifica la declaración de forma dinámica y transparente para el usuario, utilizando cualquier condición que una función pueda expresar o devolver. Puede aplicar las políticas de Oracle Virtual Private Database a declaraciones SELECT, INSERT, UPDATE, INDEX y DELETE

**Beneficios de usar las políticas de la base de datos privada virtual de Oracle**

Las políticas de Oracle Virtual Private Database brindan los siguientes beneficios:

- Basar las políticas de seguridad en objetos de base de datos en lugar de aplicaciones, Adjuntar políticas de seguridad de Oracle Virtual Private Database a las tablas, vistas o sinónimos de la base de datos, en lugar de implementar controles de acceso en todas sus aplicaciones, brinda los siguientes beneficios:

    - **Seguridad.** Asociar una política con una tabla de base de datos, una vista o un sinónimo puede resolver un problema de seguridad de la aplicación potencialmente grave. Supongamos que un usuario está autorizado para usar una aplicación y luego, aprovechando los privilegios asociados con esa aplicación, modifica incorrectamente la base de datos utilizando una herramienta de consulta ad hoc, como SQL*Plus. Al adjuntar políticas de seguridad directamente a las tablas, vistas o sinónimos, el control de acceso detallado garantiza que se aplique la misma seguridad, independientemente de cómo acceda un usuario a los datos.

    - **Sencillez.** La política de seguridad se agrega a una tabla, vista o sinónimo solo una vez, en lugar de agregarla repetidamente a cada una de sus aplicaciones basadas en tablas, vistas o sinónimos.

    - **Flexibilidad.** Puede tener una política de seguridad para las declaraciones SELECT, otra para las declaraciones INSERT y otras más para las declaraciones UPDATE y DELETE. Por ejemplo, es posible que desee permitir que los empleados de recursos humanos tengan privilegios SELECT para todos los registros de empleados en su división, pero que actualicen solo los salarios de aquellos empleados en su división cuyos apellidos comiencen con F. Además, puede crear varias políticas para cada tabla, vista o sinónimo.

- Controlar cómo la base de datos Oracle evalúa las funciones de la política, La ejecución de funciones de política varias veces puede afectar el rendimiento. Puede controlar el rendimiento de las funciones de política configurando cómo Oracle Database almacena en caché los predicados de Oracle Virtual Private Database. Las siguientes opciones están disponibles:

    - Evalúe la política una vez para cada consulta (políticas estáticas).
    - Evalúe la política solo cuando cambie el contexto de una aplicación dentro de la función de la política (políticas sensibles al contexto).
    - Evaluar la política cada vez que se ejecuta (políticas dinámicas).

## 2.3. Definición de Términos

- **Virtual Private Database (VPD):** Base de datos Privada Virtual.

- **GDPR / RGPD:** El Reglamento General de Protección de Datos es el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, publicado por el Parlamento Europeo y Consejo de la Unión Europea el 27 de abril de 2016.

- **Seguridad de la información:** tiene como objeto garantizar la disponibilidad, integridad y confidencialidad, el buen uso de la información en una organización de cualquier sector.

- **Disponibilidad:** Se refiere a que la información esté disponible y accesible para el personal autorizado cuando esta lo requiera.

- **Integridad:** Se refiere a que la información no pueda ser modificada, alterada o eliminada en alguna de sus partes, debe preservarse sin cambio alguno, los cambios solo se harán aquellos que sean autorizados.

- **Confidencialidad:** Se refiere a que la información solo debe ser accedida por el personal autorizado.

- **Política de Seguridad:** Es un documento que contiene un conjunto de reglas para el mantenimiento de cierto nivel de seguridad y denota el compromiso que tiene la dirección con la seguridad de la información.

- **Riesgo:** Probabilidad de que ocurra un evento que afecte en menor o mayor medida a la organización en cuanto su seguridad con el entorno.

- **Amenaza:** Causa potencial de que ocurra un incidete no deseado que pueda causar daño a un sistema u organización.

- **Vulnerabilidad:** Grado de debilidad o exposición de un sujeto, objeto o sistema; y en cuanto a seguridad de la información son aquellas fallas o deficiencias que posee un sistema o entorno que pueden ser aprovechadas por delincuentes para ejecutar sus ataques.

- **Activo:** Algo que posee valor para la organización, estos pueden ser tangibles e intangibles.

- **Protección de Datos:** 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. (Ley de Protección de Datos Personales – 1581)

- **Datos Personales:** Se refiere a toda información asociada o que pertenece a una persona y que permiten su identificación.

- **Ataques Cibernéticos:** Cualquier maniobra con el objetivo de es apropiarse de la información de una la empresa o persona, es de recordar que cualquier empresa que almacene, manipule o transmita datos se encuentra expuesta a un ciberataque.

- **Control de acceso:** El control de acceso es un elemento esencial de la seguridad que determina quién tiene permiso para acceder a determinados datos

- **Mecanismo de Seguridad:** Herramientas técnicas y métodos técnicos que se utilizan para implementar los servicios de seguridad

- **Datawarehouse Legacy:** Es una colección de datos que se utiliza para almacenar datos de los procesos operativos y de toma de decisiones. Estos datos se organizan por áreas temáticas y se actualizan a partir de los sistemas de información operativa.

- **PCI DSS:** Payment Card Industry Data Security Standard (Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago).

## 2.4. Hipótesis

### 2.4.1. Hipótesis General

**HG:** La implementación de un sistema de información de protección de datos mejorará el cumplimiento del requisito 7 del estándar de seguridad de datos para la industria de tarjeta de pago para un datawarehouse en una entidad bancaria en el Perú

### 2.4.2. Hipótesis Específicas

**HE1:** La implementación de un sistema de información de protección de datos mejorará el control de acceso en un datawarehouse de una entidad bancaria en el Perú

**HE2:** La implementación de un sistema de información de protección de datos mejorará el mecanismo de seguridad en un datawarehouse de una entidad bancaria en el Perú.

## 2.5. Variables

### 2.5.1. Variable Independiente

- Sistema de información de protección de datos.

### 2.5.2. Variable Dependiente

- Cumplimiento del requisito 7 del estándar.

### 2.5.3. Operacionalización de Variable

Acontinuación mostramos el cuadro de referencia de las dimensiones e indicadores referidos a la variable dependiente.

**Tabla 1**

*Cuadro de operacionalización de variable dependiente: cumplimiento del requisito 7 del estándar*

| HIPÓTESIS | VARIABLE | DIMENSIONES | INDICADORES | Escala de Medición | Niveles y rangos |
|---|---|---|---|---|---|
| "La implementacion de un sistema de información de protección de datos mejorará el cumplimiento del requisito 7 del estándar de seguridad de datos para la industria de tarjeta de pago para un datawarehouse en una entidad bancaria en el Perú" | Cumplimiento del requisito 7 del estándar | **Dimension 1** Control de acceso<br><br>**Dimension 2** Mecanismo de Seguridad | Limite de acceso a Componentes.<br>Derechos de Acceso.<br>Funcionalidad y gestión.<br><br>Politicas.<br>Procedimientos.<br>Enmascaramiento Datos. | **Escala de Likert**<br>(1) Totalmente en desacuerdo<br>(2) En desacuerdo<br>(3) Ni deacuerdo ni en desacuerdo<br>(4) De acuerdo<br>(5) Totalmente deacuerdo | **Variable**<br>Bajo (0-35)<br>Medio(36-70)<br>Alto(71-105)<br><br>**Dimensión 1**<br>Bajo (0-28)<br>Medio(29-57)<br>Alto(58-85)<br><br>**Dimensión 2**<br>Bajo (0-6)<br>Medio(7-13)<br>Alto(14-20) |

# III. METODOLOGÍA

## 2.1. Tipo de estudio

### 2.1.1. De acuerdo a la orientación

De acuerdo a la orientación el proyecto es considerado como una investigación **aplicada**, ya que se pretende generar una propuesta de solución tecnológica para resolver de manera mediata la problemática que afronta.

### 2.1.2. De acuerdo a la técnica de contrastación

De acuerdo a la técnica de contrastación el proyecto de investigación es considerado de tipo **explicativo**, ya que los datos se obtendrán mediante la observación los cuales serán condicionados por el investigador.

## 2.2. El diseño de Investigación

El diseño de la investigación es pre experimental. La representación gráfica es la siguiente:

$G_1$ : $O_1 X O_2$

Donde :

$G_1$ : Grupo Experimental
X : Tratamiento con el Sistema
$O_1$ : Test antes del experimento
$O_2$ : Test despues del experimento

Este diseño con grupo pre-experimental permitió la comparación de resultados pretest y postest, con un alto nivel de probabilidad, que el sistema de información de protección de datos (variable independiente) contribuye en la mejora del cumplimiento del requisito 7 del estándar de seguridad de datos para la industria de tarjeta de pago para un datawarehouse.

## 2.3. Descripción de la unidad de análisis población y muestra

### 2.3.1. Población

La población del estudio estuvo conformada por la totalidad del personal que labora en el área de Seguridad de la información, los cuales son los ecargados de certificar y evaluar, la cual lo constituye en número a la fecha de 20 personas (Auditores, Analistas y tech leads), con esta población se va a determinar la muestra necesaria.

### 2.3.2. Muestra

La muestra se consideró a todo el Personal experto del área de Seguridad de la informacion el cual constó de 20 personas.

La muestra se obtiene mediante una selección intencional, debido al tamaño de la población.

## 2.4. Técnicas de instrumentos de recolección de datos

Para la recolección de la información necesaria para resolver el problema planteado se utilizó dos instrumentos, las cuales son las siguientes: la encuesta, la entrevista y la observación.

- Encuesta: Las entrevistas se realizaron a profesionales de seguridad de la información que validan el cumplimiento normativo.

  Se elaboró la encuesta utilizando la escala de Likert, cuyas alternativas fueron las siguientes:

  a. Totalmente en desacuerdo.

  b. En desacuerdo.

  c. Ni de acuerdo ni en desacuerdo.

  d. De acuerdo.

  e. Totalmente de acuerdo

- Observación: Mediante la observación podemos ver el comportamiento de sistema de protección de Datos, además nos ayudó a entender su funcionamiento y capacidad.

## 2.5. Técnica de análisis y prueba de hipotesis

El análisis de la información recolectada estuvo orientada a comprobar la hipótesis general, para lo cual se ordena, clasifica y presenta los resultados de la investigación en cuadros estadisticas elaboradas sistematizados con el propósito de hacerlos comprensibles.

Se utilizaron las siguientes técnicas de procesamiento:

- Estadística: Los datos recogidos permitieron la construcción de cuadros estadísticos con su respectiva interpretación.
- Ordenamiento y clasificación:
    - Registro manual
    - Registro en Excel:

Así también, se aplicaron las siguientes técnicas de análisis:

- Formulación de cuadros de indicadores.
- Tabulación de datos de la encuesta. Luego de efectuado la encuesta se realizó en excel la tabulación respectiva y el análisis porcentual de las respuestas.

Adicionalmente como diseño especifico se han anotado en secuencia lógica, los pasos necesarios para probar la hipótesis, en concordancia con la estrategia global diseñada:

- Para Corroborar o refutar la hipótesis planteada, con la información pre y post test y para lo cual se ha realizado la prueba estadística Wilcoxon, para analizar e interpretar los resultados, para lo que se realizó los siguientes pasos:

**Paso 1:** Se plantean las Hipótesis Nula (Ho) e Hipótesis Alternativa (Hi), la segunda indica lo que se quiere demostrar y la primera lo contrario.

**Paso 2:** Se define el Nivel de Significancia, donde se estable un rango que indicara cuan aceptable es la hipótesis alternativa.

**$\alpha$ = 0.05 Confiable**

**Paso 3:** Se ha de calcular la media.

**Paso 4:** Se ha de rechazar o aceptar la hipótesis alternativa.

- Si la probabilidad obtenida P(Significancia)≤ α, se rechaza $\boldsymbol{H0}$ y se acepta $\boldsymbol{H1}$
- Si la probabilidad obtenida P(Significancia)> α, NO se rechaza $\boldsymbol{H0}$ y se acepta $\boldsymbol{H0}$

De esta forma se valida la mejora entre medias demostrando que se logró mejorar o no lo planteado en este projecto.

# IV. RESULTADOS DE LA INVESTIGACIÓN

## 4.1. Descripción del trabajo de campo

En este punto, se detalla los componentes que han sido desarrollados para este proyecto, con el objetivo de comprender los aspectos que se consideraron, así como también, conocer todos los procesos que forman la base de la solución.

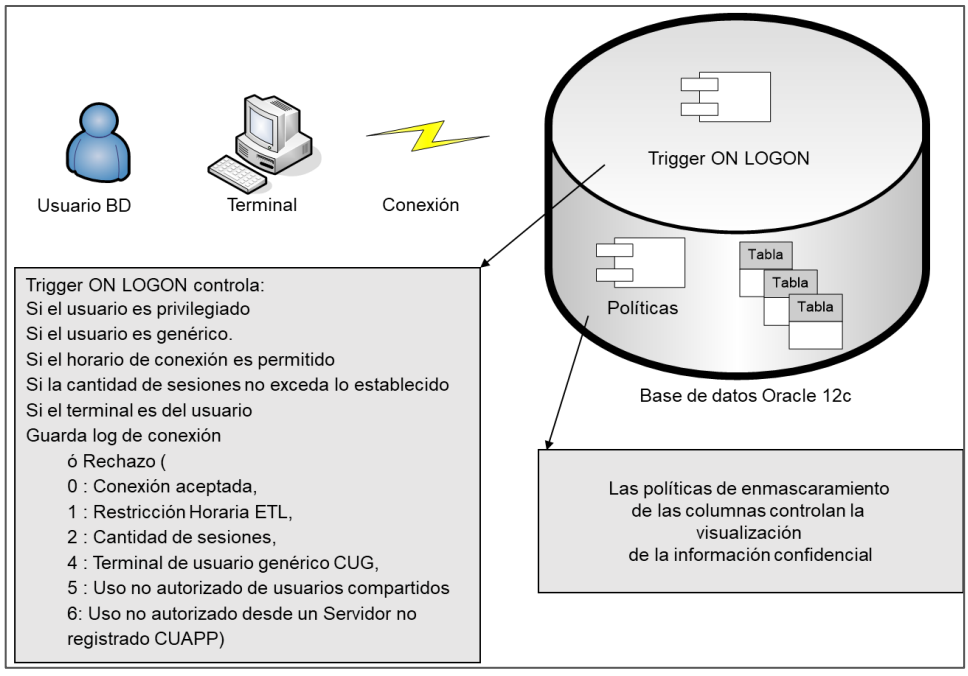
### 4.1.1. Arquitectura de la solución

Para la solución requerida en el proyecto, se ha establecido la implementación de los controles:

- Control de horario de conexiones
- Control de cantidad de sesiones
- Control de sitio de trabajo (terminales)
- Enmascaramiento de la información confidencial
- Auditoría de sesiones (logon, logoff)
- Custodia de usuarios genéricos.

**Figura 6**

*Diagrama de la arquitectura implementada del sistema de protección de Datos*



Como se muestra en la Figura 7, la solución se estructuró con un conjuto de Paquetes y Objetos de base de datos donde se implementaron las reglas de negocio establecidas para todos los controles desarrollados para lo cual se detallan asi como los elementos que conforman la solución.

### 4.1.2. Descripción de la solución

Toda configuración de la solución implementada se tiene que efectuar mediante el paquete DML_VPD_ADMIN la cual cumple la función de administración. De Igual forma el paquete DML_VPD_ADMIN contiene las funciones y procedimientos necesarios para la configuración y el mantenimiento de VPD implementada.

**Figura 7**

*Cuadro de Componentes de Base de Datos de la Solución*

| | | |
|---|---|---|
| **PACKAGE** | ADMIN.DML_VPD_ADMIN | Sirve para configurar el uso correcto de VPD (CLIENT_IDENTIFIER, TERMINAL, columnas enmascaradas, restricciones de las sesiones). |
| **PACKAGE** | ADMIN.DML_VPD | Sirve para controlar las restricciones por sesión y las políticas de enmascaramiento. |
| **TRIGGER** | SYS.TRIGGER_LOGON | Configura el CLIENT_IDENTIFIER y controla la conexión de las sesiones. En el caso de que se incumpla alguna restricción la conexión se rechaza. |

**Figura 8**

*Elementos de Paquetes Implementados.*

| | | |
|---|---|---|
|  | Client Identifier | Es el grupo identificador o conjunto de privilegios DAC que se pueden otorgar solo a un usuario y asociar varios o ningún concepto. De esa forma se simplifica el trabajo de la Gestion de Acceso al DAC. |
|  | Concepto | Es la agrupación de todas las columnas de tablas o Vista del DWH con una misma definición . Crea una unidad agrupando columnas con el mismo significado. |
|  | Política de Enmascaramiento por columna | Es la creación de claves dinámicas a cada columna de la tabla o vista, controlan la visualización de la información confidencial y está asociada solo a un concepto. |
|  | Usuario de Base de Datos | Es todo aquel que tenga contacto con el sistema de bases de datos |
|  | Exclusión de Políticas | Son las excepciones que se le aplica a cada usuario para que pueda visualizar una o varias (Columna/Concepto) |

**Figura 09**

*Funcionamiento del Sistema de Protección Implementado*

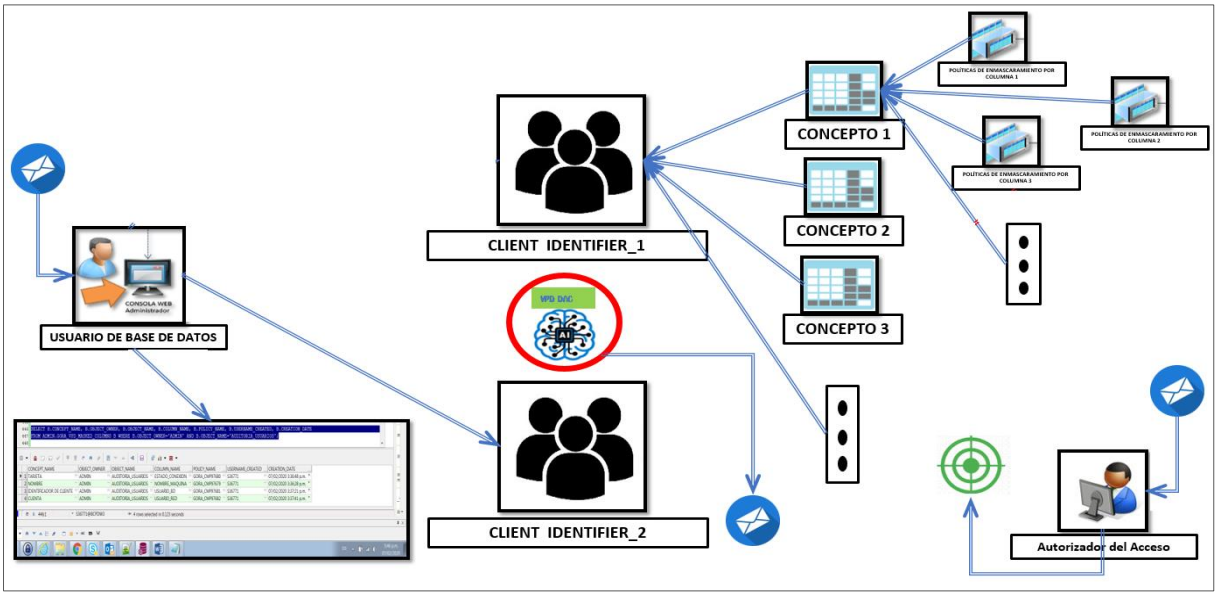



**Figura 10**

*Módulo de Custodio de Usuario Genérico*

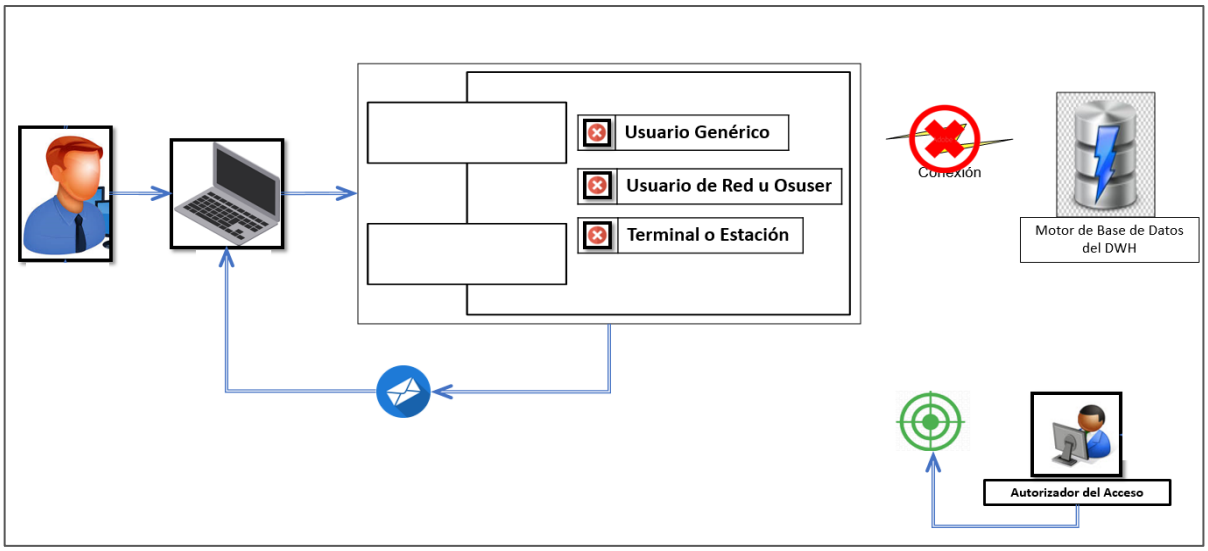
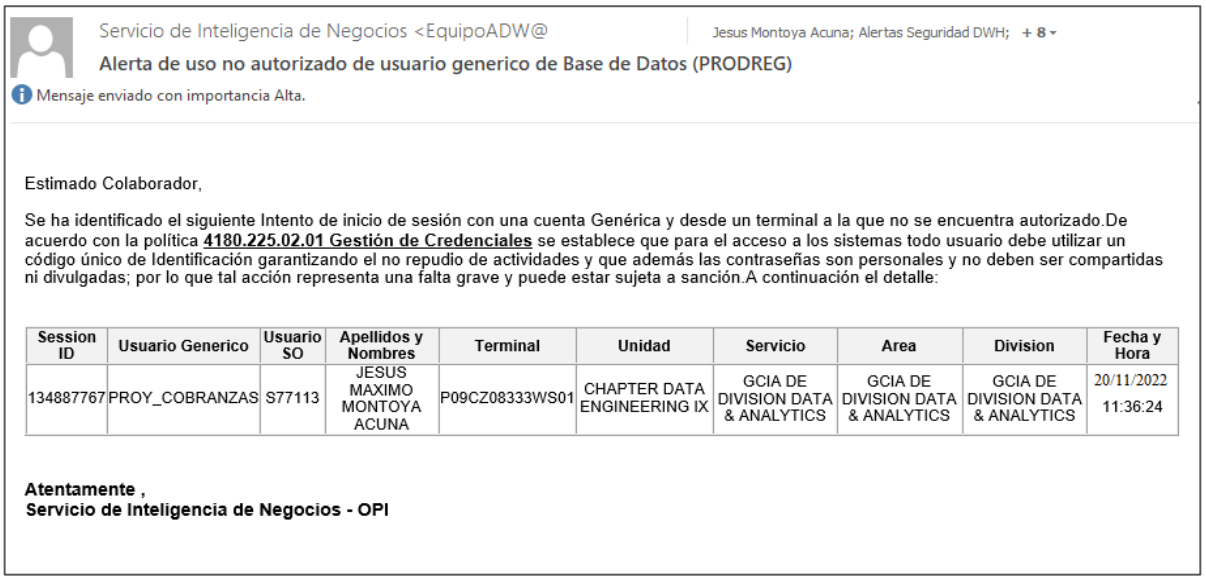


**Figura 11**

*Alerta de la política de Control del Custodio de Usuario Genérico*



Servicio de Inteligencia de Negocios <EquipoADW@ Jesus Montoya Acuna; Alertas Seguridad DWH; + 8

Alerta de uso no autorizado de usuario generico de Base de Datos (PRODREG)

Mensaje enviado con importancia Alta.

Estimado Colaborador,

Se ha identificado el siguiente Intento de inicio de sesión con una cuenta Genérica y desde un terminal a la que no se encuentra autorizado.De acuerdo con la política **4180.225.02.01 Gestión de Credenciales** se establece que para el acceso a los sistemas todo usuario debe utilizar un código único de Identificación garantizando el no repudio de actividades y que además las contraseñas son personales y no deben ser compartidas ni divulgadas; por lo que tal acción representa una falta grave y puede estar sujeta a sanción.A continuación el detalle:

| Session ID | Usuario Generico | Usuario SO | Apellidos y Nombres | Terminal | Unidad | Servicio | Area | Division | Fecha y Hora |
|---|---|---|---|---|---|---|---|---|---|
| 134887767 | PROY_COBRANZAS | S77113 | JESUS MAXIMO MONTOYA ACUNA | P09CZ08333WS01 | CHAPTER DATA ENGINEERING IX | GCIA DE DIVISION DATA & ANALYTICS | GCIA DE DIVISION DATA & ANALYTICS | GCIA DE DIVISION DATA & ANALYTICS | 20/11/2022 11:36:24 |

**Atentamente ,**
**Servicio de Inteligencia de Negocios - OPI**

**Figura 12**

*Alerta del Control Custodio de Usuario Genérico*

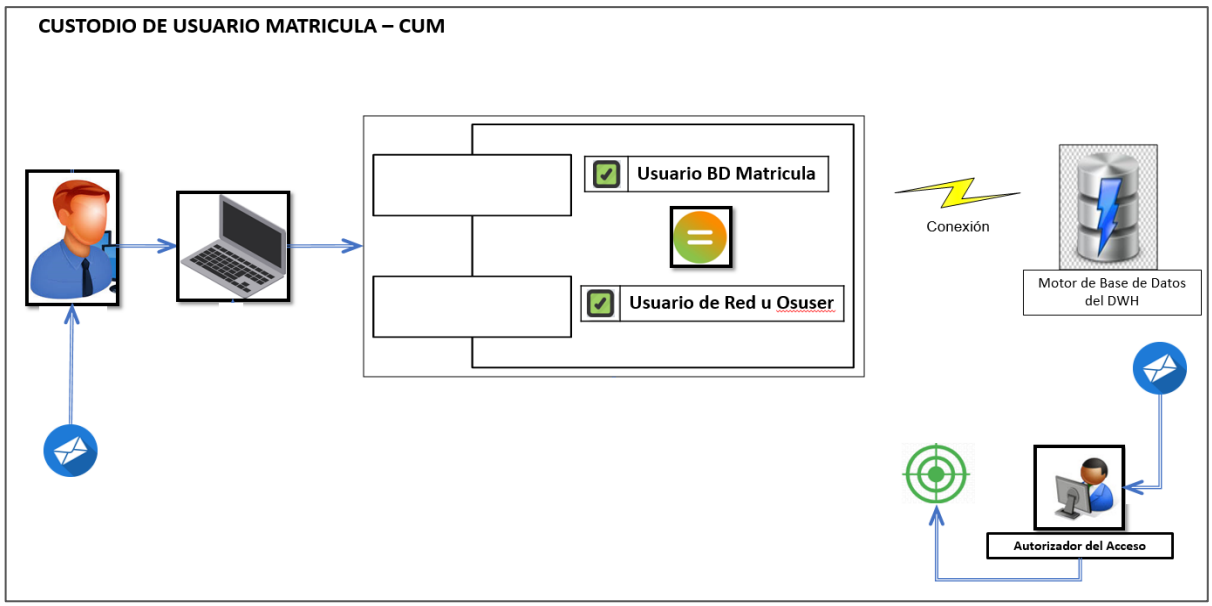


**Figura 13**

*Alerta del Control de la política de Custodio de Usuario Matricula*

Servicio de Inteligencia de Negocios <EquipoADW

Giancarlo Herrera Menendez; Dayanna Tito Solis; Mariana Muñoz Drinot; Alertas Seguridad DWH; + 10

**Alerta de uso no autorizado de usuarios compartidos en Base Datos Oracle (PRODREG)**

Mensaje enviado con importancia Alta.

Estimado(a) Dayanna Madeley Tito Solis:

Se ha identificado que el día 20-Nov-2022 a las 12:40:19 has intentado acceder a la Base de Datos Oracle Producción DWH(BCPDW3) con la cuenta de GIANCARLO ENRIQUE HERRERA MENENDEZ, la cual no te pertenece.
Esta acción está incumpliendo con la política **4180.225.02.01 Gestión de Credenciales**, la cual establece que para el acceso a los sistemas todo usuario debe utilizar un código único de identificación -garantizando el no repudio de actividades- y que, además, las contraseñas son personales y no deben ser compartidas ni divulgadas; por lo que esto representa una falta grave y está sujeto a sanciones.

Estimado(a) Giancarlo Enrique Herrera Menendez:

Se ha identificado que tu cuenta de Base de Datos Oracle Producción ha tratado de ser utilizada por DAYANNA MADELEY TITO SOLIS.
Como acción inmediata es necesartio que realices el cambio de clave de tu cuenta vulnerada de Base de Datos (mediante la web de HelpDesk) y no vuelvas a compartir la credencial.

A continuación, el detalle:

| Tipo Cuenta | Usuario Matricula | Apellidos y Nombres | Unidad | Servicio | Area | Division |
|---|---|---|---|---|---|---|
| CUENTA DE BD VULNERADA | S15203 | GIANCARLO ENRIQUE HERRERA MENENDEZ | SUBGCIA DE PLANEAMIENTO, INF Y AN?LISIS | GCIA. ?REA ESTRATEGIA Y DESEMPE?O DE SDP | GERENCIA DE DIVISI?N SOLUCIONES DE PAGO | GERENCIA DE DIVISI?N SOLUCIONES DE PAGO |
| USUARIO QUE INTENTA ACCEDER | S74358 | DAYANNA MADELEY TITO SOLIS | SUBGCIA DE PLANEAMIENTO, INF Y AN?LISIS | GCIA. ?REA ESTRATEGIA Y DESEMPE?O DE SDP | GERENCIA DE DIVISI?N SOLUCIONES DE PAGO | GERENCIA DE DIVISI?N SOLUCIONES DE PAGO |

En caso la alerta sea generada por un proceso de un servidor o por un aplicativo, deben contactarse con el equipo de Seguridad al buzón seganaplicacion@ y seguir el flujo de atención que se informa en la presentación AlertaUsuarioCompartido.ppt.

Información adicional: Nombre del equipo utilizado (P09MV84105LPT01) y Código de Sesión(134904488).

**Atentamente ,**
**Servicio de Inteligencia de Negocios - OPI**

## 4.2. Presentación resultado y prueba de hipótesis

### 4.2.1. Análisis descriptivo

**Resultados descriptivos para la variable dependiente: Cumplimiento del requisito 7 del estándar**

**Tabla 2**

*Frecuencias de la variable dependiente: Cumplimiento del requisito 7 del estándar*

| Nivel | Pretest | | Postest | |
|---|---|---|---|---|
| | Frecuencia | Porcentaje | Frecuencia | Porcentaje |
| Bajo | 19 | 95.00% | 0 | 0.00% |
| Medio | 1 | 5.00% | 0 | 0.00% |
| Alto | 0 | 0.00% | 20 | 100.00% |

De acuerdo a tabla 2 se puede apreciar lo siguiente:

- En el caso de pretest el 100% de los encuestados indico un nivel bajo respecto al cumplimiento del requisito 7 del estándar, mientras que el 0% indicaron un nivel los niveles medio y alto respectivamente.

- En el caso del posttest el 100% de los encuestados indico un nivel alto.

**Resultados descriptivos para la dimensón: Control de Acceso**

**Tabla 3**

*Tabla de Frecuencias de la dimensión: Control de acceso*

| Nivel | Pretest | | Postest | |
|---|---|---|---|---|
| | Frecuencia | Porcentaje | Frecuencia | Porcentaje |
| Bajo | 20 | 100.00% | 0 | 0.00% |
| Medio | 0 | 0.00% | 0 | 0.00% |
| Alto | 0 | 0.00% | 20 | 100.00% |

De acuerdo a tabla 3 se puede apreciar lo siguiente:

- En el caso de pretest el 100% de los encuestados indico un nivel bajo respecto a la dimensión Control de acceso, mientras que el 0% indicaron un nivel los niveles medio y alto respectivamente.

- En el caso del posttest el 100% de los encuestados indico un nivel alto.

**Resultados descriptivos para dimensón: Mecanismo de Seguridad**

**Tabla 4**

*Tabla de Frecuencias de la dimensión: Mecanismo de seguridad*

| Nivel | Pretest | | Postest | |
|---|---|---|---|---|
| | Frecuencia | Porcentaje | Frecuencia | Porcentaje |
| Bajo | 17 | 30.00% | 0 | 0.00% |
| Medio | 3 | 70.00% | 0 | 0.00% |
| Alto | 0 | 0.00% | 20 | 100.00% |

De acuerdo a tabla 4 se puede apreciar lo siguiente:

- En el caso de pretest el 15% de los encuestados indico un nivel bajo respecto a la dimensión mecanismos de seguridad, mientras que el 85% indico un nivel medio y un 0% para el nivel alto.

- En el caso del posttest el 100% de los encuestados indico un nivel alto.

### 4.2.2. Analisis infenrencial

Para la selección de la prueba estadística a realizar, se realizaron pruebas de normalidad, siendo seleccionado la prueba Shapiro-Wilk, debido a que la muestra estuvo formada por 20 personas. Para esta prueba se considero un error inferior al 5%(0.05) par asumir distribuciones significativamente normales. Los resultados fueron los siguientes.

**Resultados de la prueba de hipótesis especificia 1**

**HE0:** La implementacion de un sistema de información de protección de datos no mejora el control de acceso en un datawarehouse de una entidad bancaria en el Perú.

**HE1:** La implementacion de un sistema de información de protección de datos mejora el control de acceso en un datawarehouse de una entidad bancaria en el Perú.

**Tabla 5**

*Resultado de la prueba de Wilcoxon para dimensión Control de Acceso*

| Valor p calculado | Medias Calculadas | |
|---|---|---|
| | Pretest | Postest |
| 0.000086 | 21.65 | 82.5 |

Como se aprecia en la Tabla 5 el el valor p calculado (0.000086) fue menor al establecido (0.05); ello permite asumir diferencias significativas entre los resultados del pretest y postest. Por otro lado, el valor de la media del postest (82.5) fue mayor al valor del pretest (21.65) ello permitió determinar que los resultados del postest fueron significativamente mejores que los del pretest. Por tanto, se puede afirmar que la implementación de un sistema de información de protección de datos mejoró de forma significativa el control de acceso del datawarehouse de una entidad bancaria en el Perú.

**Resultados de la prueba de hipótesis especificia 2**

**HE0:** La implementación de un sistema de información de protección de datos no mejora el mecanismo de seguridad en un datawarehouse de una entidad bancaria en el Perú.

**HE1:** La implementación de un sistema de información de protección de datos mejora el mecanismo de seguridad en un datawarehouse de una entidad bancaria en el Perú.

**Tabla 6**

*Resultado de la prueba de Wilcoxon para dimensión mecanismo de seguridad*

| Valor p calculado | Medias Calculadas | |
|---|---|---|
| | Pretest | Postest |
| 0.000079 | 5.6 | 18.95 |

Como se aprecia en la Tabla 6 el valor p calculado (0.000079) fue menor al establecido (0.05); ello permitió asumir diferencias significativas entre los resultados del pretest y postest. Por otro lado, el valor de la media del postest (18.95) fue mayor al valor del pretest (5.6) ello permitió determinar que los resultados del postest fueron significativamente mejores que los del pretest. Por tanto, se puede afirmar que la implementación de un sistema de información de protección de datos mejora el mecanismo de seguridad en un datawarehouse de una entidad bancaria en el Perú.

**Resultados de la prueba de hipótesis general**

**HG0:** La implementación de un sistema de información de protección de datos no mejora el cumplimiento del requisito 7 del estándar de seguridad de datos para la industria de tarjeta de pago para un datawarehouse en una entidad bancaria en el Perú.
**HG1:** La implementación de un sistema de información de protección de datos mejora el cumplimiento del requisito 7 del estándar de seguridad de datos para la industria de tarjeta de pago para un datawarehouse en una entidad bancaria en el Perú.

**Tabla 7**

*Resultado de la prueba de Wilcoxon para la variable dependiente*

| Valor p calculado | Medias Calculadas | |
|---|---|---|
| | Pretest | Postest |
| 0.000085 | 27.05 | 101.45 |

Como se aprecia en la Tabla 7 el valor p calculado (0.000085) fue menor al establecido (0.05); ello permitió asumir diferencias significativas entre los resultados del pretest y postest. Por otro lado, el valor de la media del postest (101.45) fue mayor al valor del pretest (27.05) ello permitió determinar que los resultados del postest fueron significativamente mejores que los del pretest. Por tanto, se puede acepta la hipótesis alterna que asume que la implementación de un sistema de información de protección de datos mejora el cumplimiento del requisito 7 del estándar de seguridad de datos para la industria de tarjeta de pago para un datawarehouse en una entidad bancaria en el Perú.

### 4.3. Discusión de resultados

Según los resultados obtenidos en la investigación se realiza un análisis comparativo con algunos resultados obtenidos en otras investigaciones similares a esta investigación considerando cada una la relación con las dimensiones planteadas.

El primer lugar analizamos la dimensión control de acceso según Cuadros, Huacac (2018) concluye que implementar un sistema de gestión de identidades y roles que permita mejorar la administración de permisos a usuarios a fin de mitigar riesgos potenciales de vulnerabilidades en la entidad bancaria y mejorar la seguridad de acceso a los sistemas de una entidad bancaria la cual es acorde a los resultados que se han obtenido en nuestro estudio.

De igual manera Cuadros (2019), concluye que la implementación de un SIEM (Sistema de gestión eventos e información de seguridad), ayuda al cumplimiento de los requisitos 10 y 11 de la norma PCI DSS lo cual nos indica que se debe de almacenar los registros de auditoria de todos los componentes tecnológicos de la empresa tales como servidores, concordando con las medidas que implementan nuestro sistema en el tema de control de acceso.

En referencia a la dimensión mecanismos de seguridad según Orellana y Tamallo (2020) proponen una mejora de la seguridad de la información en una institución financiera basada en controles y mecanismos que indica la norma PCI DSS, se plantea un estudio de las mejores prácticas del manejo información dentro de una institución financiera, establecimiento de políticas y procedimientos; lo cual concuerda con la implementación realizada en el establecimiento de políticas y procedimientos han permitido cubrir los requsitos que establece el estándar.

# V. CONCLUSIONES

1. En esta tesis se mejoró el cumplimiento del requisito 7 del estándar de seguridad de datos para la industria de tarjeta de pago para un datawarehouse mediante la implementación de un sistema de información de protección de datos en una entidad bancaria en el Perú considerando que toda empresa que requiera almacenar información relaciona con método de pagos, debe cumplir con las normas de seguridad PCI DSS y poder generar confidencialidad e integridad en los datos de los clientes.

2. En esta tesis de igual forma se mejoró el control de acceso con la implementación de un sistema de información de protección de datos para un datawarehouse de una entidad bancaria en el Perú, considerando que el establecimiento de controles en base de datos legacy y el aseguramiento del enmascaramiento de la información, se torna muy importante en la línea del cumplimiento normativo nacional e internacional, que contribuyen enormemente a las empresas tanto en la reducción de riesgos que involucren perdidas monetarias como de imagen institucional.

3. En esta Tesis se mejoró el mecanismo de seguridad con la implementación de un sistema de información de protección de datos para un datawarehouse en una entidad bancaria en el Perú, permitiendo generar y establecer políticas y procedimientos de control de acceso y protección de datos de gran aporte al cumplimiento de los requisitos del estándar.

## VI. RECOMENDACIONES

En la actualidad todas las empresas tienen la necesidad y diríamos obligación de tomar medidas en los controles de accesos a la información sensible de los usuarios, en ese sentido se debe crear normas y procedimientos que regulen la visualización y manipulación de la misma. Considerando que todo control de acceso debe alcanzar tanto a todas las plataformas productivas como en nuestro caso de estudio un datawarehouse legacy.

Se recomienda que los sistemas o aplicaciones utilizados en la implementación, deben encontrarse actualizados a su última versión o tenga los parches de seguridad más recientes. Para el caso de aplicaciones desarrolladas internamente estas deberán actualizarse y revisarse en los casos de upgrade de la base de datos, para así reducir el riesgo de que algunas Funcionalidades no funcionen.

Se recomienda almacenar la menor cantidad de datos confidenciales del usuario y crear políticas de retención y disponibilidad de información en estos repositorios legacy, esto a fin de reducir el riesgo de que información sensible quede vulnerable. Se refiere a políticas de retención y de disposición de datos a procedimientos a seguir al momento de realizar un requerimiento de información; se debe tomar en cuenta que datos son esenciales para guardarlos y hacer uso en la transacción

Finalmente se recomienda dotar un sistema web para el tema de la gestión del metadato que soporta el control de acceso a datos, que en el proyecto e concebida como una aplicación de base de datos.

## VII. REFERENCIAS BIBLIOGRÁFICAS


PowerData. (2022). *La autenticación de usuarios para proteger datos sensibles*. Obtenido de La autenticación de usuarios para proteger datos sensibles: https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/bid/234655/La-autenticaci-n-de-usuarios-para-proteger-datos-sensibles

Acosta, D. (18 de Agosto de 2022). *¿Qué es PCI DSS?* Obtenido de https://www.pcihispano.com/que-es-pci-dss/

Allianz Global Corporate. (06 de 05 de 2022). *Covid, Cyber, Compliance and ESG top risk concerns for financial services sector*. Obtenido de Financial Services Risk Trends: https://www.allianz.com/en/press/news/studies/210506_Allianz-covid-cyber-compliance-ESG-top-risk-concerns-for-financial-services-sector.html

Dahn, M. (2022). *Guía de cumplimiento de la normativa PCI*. Obtenido de https://stripe.com/es-us/guides/pci-compliance

*Database Security Guide*. (2022). Obtenido de Using Oracle Virtual Private Database to Control Data Access: https://docs.oracle.com/cd/E11882_01/network.112/e36292/vpd.htm#DBSEG244

Diario Gestión. (27 de 06 de 2017). *Ningún cliente se vio afectado por desvío de S/ 5 millones que hizo cajera del BCP*. Obtenido de https://gestion.pe/economia/empresas/cliente-vio-afectado-desvio-s-5-millones-hizo-cajera-bcp-138197-noticia/

Somerville, I. (2011). *Ingenieria de Software.* Pearson Education.

ISOTools Excellence. (01 de 02 de 2018). *Blog especializado en Seguridad de la*. Obtenido de Seguridad Informática: https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

KPMG . (2022). *Una triple amenaza en las Américas.* Mexico.

KPMG S.A. (05 de 2019). *La amenaza multifacética del fraude: ¿Están los bancos preparados?* Obtenido de Encuesta global de fraude bancario 2019: https://home.kpmg/cr/es/home/tendencias/2019/07/fraude_bancario.html

Lorena, F. (2022 de 06 de 29). *Control de acceso: qué es y cómo ayuda a proteger nuestros datos.* Obtenido de Seguridad: https://www.redeszone.net/tutoriales/seguridad/control-de-acceso-que-es/

Microsoft. (2022). *¿Qué es el control de acceso?* Obtenido de Control de acceso definido: https://www.microsoft.com/es-es/security/business/security-101/what-is-access-control

ORACLE . (12 de 2022). *Documentación de Oracle Cloud Infrastructure*. Obtenido de Control de acceso a datos: https://docs.oracle.com/es-ww/iaas/autonomous-database/doc/data-access-control.html

PCI Security Standar Counsil. (2006). *Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI)* . Obtenido de Procedimientos de Auditoría de Seguridad: https://listings.pcisecuritystandards.org/pdfs/spanish_pci_dss_audit_procedures_v1-1.pdf

Power Data. (2022). *Data Warehouse: todo lo que necesitas saber sobre almacenamiento de datos*. Obtenido de Datawarehouse: https://www.powerdata.es/data-warehouse

Power Data. (2022). *Seguridad de datos*. Obtenido de Seguridad de datos: En qué consiste y qué es importante en tu empresa: https://www.powerdata.es/seguridad-de-datos

Purificacion, A. L. (s.f.). *Seguridad Informatica 1era Edicion.* Editex.

SAP. (2021). *What is a data warehouse?* Obtenido de Sap insights: https://www.sap.com/insights/what-is-a-data-warehouse.html

Vietes, A. G. (s.f.). *Enciclopedia de la Seguridad Informatica 2da edicion.* RA-MA.

# VIII. ANEXOS

## ANEXO 01: CUESTIONARIO PARA MEDIR LA VARIABLE DEPENDIENTE.

### I. Indicaciones

A continuación, se le presenta una serie de preguntas, las cuales deberá responder marcado con una (X) en la respuesta que considere correcta:

(1). Totalmente en desacuerdo

(2). En desacuerdo

(3). Ni de acuerdo ni en desacuerdo

(4). De acuerdo

(5). Totalmente de acuerdo

| Dimensión | Indicador | Ítems | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| Controles de acceso y protección de datos sensibles | **Límite de acceso a componentes** | 1.¿El sistema limita el acceso a la información sensible con granularidad (por columna) a todos los usuarios del darawarehouse, de acuerdo a una clasificación y función establecida?. | | | | | |
| | | 2. ¿El sistema limita el acceso a los a usuarios privilegiados permitiéndole al mínimo el acceso a información sensible siendo lo necesario para sus tareas?. | | | | | |
| | | 3. ¿El sistema limita el acceso al datawarehouse de cuentas de genéricas privilegiados, solo a las personas autorizadas para el uso del mismo?. | | | | | |
| | | 4. ¿El acceso al datawahouse permite aplicar restricciones horarias de conexión para los usuarios dependiendo de su tareas?. | | | | | |
| | | 5. ¿El sistema controla el acceso al datawarehouse de los usuarios, validando los datos de terminal y SO registrados?. | | | | | |
| | | 6. ¿El sistema brinda las interfaces necesarias que permiten la gestión de componentes, datos y mantenimiento del control de autenticación?. | | | | | |
| | | 7.¿El Sistema de información permite el rastro del acceso a datos sensibles que ha realizado un usuario del Datawarehouse?. | | | | | |
| | **Funcionalidad y gestión** | 8. ¿El sistema de información permite la gestión de los componentes de información del datawarehouse con data sensible de forma automatizada? | | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | 9.¿ El Sistema de información en la aplicación de los mecanismo y control de accesos de datos permite que la información del Datawarehouse permanezca correcta y no haya sido modificada?. | | | | | |
| | | 10.¿El Sistema de protección de datos y el control de acceso garantiza que tanto que los datos del Datawarehouse están disponibles al usuario en todo momento?. | | | | | |
| | | 11.¿El Sistema aplica los mecanismos de control de acceso a datos sensibles de manera que no presenta problemas en la entrega de la información para las entidades catalogadas?. | | | | | |
| | | 12.¿El sistema mantiene las capacidades adecuadas para asegurar la disponibilidad?. | | | | | |
| | | 13. ¿El sistema gestiona y permite tener conocimiento de todos los componentes relacionados con información sensible, así como tablas, columnas, Usuarios, terminales, etc. que contiene el datawarehouse?. | | | | | |
| | | 14. ¿El sistema permite que los datos en reposo almacenados en el datawahouse estén protegidos?. | | | | | |
| | | 15. ¿El sistema cuenta con la posibilidad de ocultar la información catalogada como sensible a todos los usuarios?. | | | | | |
| | | 16.¿El sistema Detecta accesos no autorizados y pone en marcha mecanismos de alerta efectivamente?. | | | | | |
| | **Derechos de Acceso** | 17.¿ El sistema permite restringir o permitir el acceso a cierta Información a personas y áreas determinadas según las aprobaciones correspondientes?. | | | | | |
| Mecanismos de Seguridad | **Enmascaramiento Datos** | 18. ¿Los mecanismos de enmascaramiento controlan efectivamente el acceso de datos sensibles almacendos en el datawarehouse (Numero de tarjetas, Datos de Titulares, Direcciones, telefono, Nombres, etc)?. | | | | | |
| | **Políticas** | 19. ¿Se tiene definido las políticas de acceso al datawarehouse y de la informacion sensible que se almacena?. | | | | | |
| | **Procedimiento** | 20. ¿Se tiene definido los procedimientos respectivos para la para la confirguracion del control de acceso de componentes?. | | | | | |
| | | 21. ¿Se tiene definido los procedimientos respectivos para la para el acceso a la informacion sensible de cara a los usuarios?. | | | | | |

## ANEXO 02: CUESTIONARIO DE EVALUACIÓN DEL REQUISITO 7 DEL ESTÁNDAR PCI DSS

| Respuesta a la Pregunta sobre las PCI - DSS: | SI | NO | Especial* |
|---|---|---|---|
| 7.1 ¿Se limita el acceso a los componentes del sistema y a los datos de titulares de tarjeta a aquellos individuos cuyas tareas necesitan de ese acceso, de la manera siguiente?: | | | |
| 7.1.1 ¿Los derechos de acceso para usuarios con ID privilegiados están restringidos a los privilegios mínimos necesarios para llevar a cabo las responsabilidades del trabajo? | ☐ | ☐ | |
| 7.1.2 ¿Los privilegios se asignan a personas de acuerdo con su clasificación y función de su cargo (también denominados "control de acceso por funciones" o RBAC).? | ☐ | ☐ | |
| 7.1.3 ¿Se requiere una aprobación documentada de partes autorizadas (por escrito o electrónicamente) que especifique los privilegios requeridos? | ☐ | ☐ | |
| 7.1.4 ¿Se implementan controles de acceso a través de un sistema de control de acceso automatizado? | ☐ | ☐ | |
| 7.2 ¿Se implementó un sistema de control de acceso para los componentes del sistema con usuarios múltiples que restrinja el acceso basado en la necesidad del usuario de conocer y que se configure para “negar todo”, salvo que se permita específicamente, de la siguiente manera? | | | |
| 7.2.1 ¿Se implementaron sistemas de control de acceso en todos los componentes del sistema? | ☐ | ☐ | |
| 7.2.2 ¿Están configurados los sistemas de control de acceso a los efectos de hacer cumplir los privilegios asignados a los individuos sobre la base de la clasificación de la tarea y la función? | ☐ | ☐ | |
| 7.2.3 ¿Poseen los sistemas de control de acceso un ajuste predeterminado de "negar todos"? | ☐ | ☐ | |
| 7.3 ¿Se dispone de políticas de seguridad y los procedimientos operativos para restringir el acceso a los datos del titular de la tarjeta y estas estan documentados, implementados y que son de conocimiento para todas las partes afectadas | ☐ | ☐ | |

## ANEXO 03: MATRIZ DE CONSITENCIA

| PROBLEMA | OBEJTIVO | HIPÓTESIS | VARIABLES | DIMENSIONES | INDICADORES | INSTRUMENTO |
|---|---|---|---|---|---|---|
| **PROBLEMA GENERAL**<br>¿En qué medida la implementación de un sistema de información de protección de datos mejora el cumplimiento del requisito 7 del estándar de seguridad de datos para la industria de tarjeta de pago para un datawarehouse en una entidad bancaria en el Perú? | **OBEJTIVO GENERAL**<br>Mejorar el cumplimiento del requisito 7 del estándar de seguridad de datos para la industria de tarjeta de pago para un datawarehouse mediante la implementación de un sistema de información de protección de datos en una entidad bancaria en el Perú. | **HIPÓTESIS GENERAL**<br>La implementación de un sistema de información de protección de datos mejorará el cumplimiento del requisito 7 del estándar de seguridad de datos para la industria de tarjeta de pago para un datawarehouse en una entidad bancaria en el Perú. | **VARIABLE INDEPENDIENTE**<br>Sistema de información de protección de datos | Sistema de información | Disponibilidad<br>Integridad<br>Confiabilidad<br>Seguridad<br>Usabilidad | |
| **PROBLEMAS ESPECÍFICOS**<br><br>¿En qué medida la implementación de un sistema de información de protección de datos mejora el control de acceso de un datawarehouse en una entidad bancaria en el Perú?.<br><br>¿En qué medida la imlementación de un sistema de información de protección de datos mejora el mecanismos de seguridad de un datawarehouse en una entidad bancaria en el Perú?. | **OBJETIVOS ESPECÍFICOS**<br><br>Mejorar el control de acceso con la implementación de un sistema de información de protección de datos para un datawarehouse en una entidad bancaria en el Perú.<br><br>Mejorar el mecanismo de seguridad con la implementación de un sistema de información de protección de datos para un datawarehouse en una entidad bancaria en el Perú. | **HIPÓTESIS ESPECÍFICAS**<br><br>La implementación de un sistema de información de protección de datos mejorará el control de acceso en un datawarehouse de una entidad bancaria en el Perú.<br><br>La implementación de un sistema de información de protección de datos mejorará el mecanismo de seguridad en un datawarehouse de una entidad bancaria en el Perú. | **VARIABLE DEPENDIENTE**<br>Cumplimiento del requisito 7 del estándar | Control de acceso<br><br>Mecanismo de Seguridad | - Limite de acceso a Componentes<br>- Derechos de Acceso<br>- Funcionalidad y gestión<br>- Politicas<br>- Procedimientos<br>- Enmascaramiento Datos | **Cuestionario:**<br>**Escala de Likert:**<br>(1) Totalmente en desacuerdo<br>(2) En desacuerdo<br>(3) Ni deacuerdo ni en desacuerdo<br>(4) De acuerdo<br>(5) Totalmente deacuerdo<br>**Niveles y rangos:**<br>Variable<br>Bajo (0-35)<br>Medio(36-70)<br>Alto(71-105)<br><br>Dimensión 1<br>Bajo (0-28)<br>Medio(29-57)<br>Alto(58-85)<br><br>Dimensión 2<br>Bajo (0-6)<br>Medio(7-13)<br>Alto(14-20) |

## ANEXO 04: FICHA DE REGISTRO DE DATOS PRETEST PARA LA VARIABLE DEPENDIENTE

| PRE TEST | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Dimensión | Controles de acceso y protección de datos sensibles | | | | | | | | | | | | | | | | | Mecanismos de Seguridad | | | | |
| Indicadores | Límite de acceso a componentes | | | | | | | Funcionalidad y gestión | | | | | | | | | Derechos de Acceso | Enmascaramiento Datos | Políticas | Procedimiento | | |
| Pregunta / Persona | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 | Q8 | Q9 | Q10 | Q11 | Q12 | Q13 | Q14 | Q15 | Q16 | Q17 | Q18 | Q19 | Q20 | Q21 | |
| P1 | 1 | 1 | 1 | 1 | 2 | 1 | 2 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 2 | |
| P2 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 2 | 2 | 1 | 1 | 1 | 1 | 2 | 1 | 2 | |
| P3 | 2 | 1 | 2 | 1 | 1 | 1 | 2 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 2 | 2 | 1 | 1 | 1 | 2 | 1 | |
| P4 | 1 | 1 | 2 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | |
| P5 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | |
| P6 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 2 | 1 | 2 | 1 | 1 | 2 | 1 | 1 | 2 | 1 | 1 | 1 | |
| P7 | 1 | 1 | 1 | 1 | 2 | 1 | 2 | 1 | 2 | 1 | 1 | 1 | 1 | 2 | 1 | 2 | 1 | 2 | 2 | 1 | 2 | |
| P8 | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | |
| P9 | 2 | 2 | 2 | 1 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 | 2 | |
| P10 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 2 | |
| P11 | 2 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 2 | 2 | 1 | 2 | 1 | |
| P12 | 1 | 1 | 2 | 2 | 1 | 2 | 1 | 1 | 2 | 1 | 2 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 2 | |
| P13 | 1 | 1 | 1 | 2 | 1 | 2 | 1 | 2 | 1 | 2 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 2 | 1 | 1 | |
| P14 | 1 | 1 | 2 | 1 | 2 | 1 | 2 | 2 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | |
| P15 | 1 | 2 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 2 | 1 | 1 | |
| P16 | 2 | 1 | 2 | 2 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 2 | |
| P17 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 2 | 1 | 1 | |
| P18 | 1 | 1 | 2 | 1 | 1 | 2 | 1 | 2 | 1 | 1 | 2 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | |
| P19 | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 2 | 1 | 1 | |
| P20 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | |

## ANEXO 05: FICHA DE REGISTRO DE DATOS POSTEST PARA LA VARIABLE DEPENDIENTE

| POST TEST | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Dimensión | Controles de acceso y protección de datos sensibles | | | | | | | | | | | | | | | | | Mecanismos de Seguridad | | | |
| Indicadores | Límite de acceso a componentes | | | | | | | Funcionalidad y gestión | | | | | | | | | Derechos de Acceso | Enmascaramiento Datos | Políticas | Procedimiento | |
| Pregunta / Persona | QQ1 | QQ2 | QQ3 | QQ4 | QQ5 | QQ6 | QQ7 | QQ8 | QQ9 | QQ10 | QQ11 | QQ12 | QQ13 | QQ14 | QQ15 | QQ16 | QQ17 | QQ18 | QQ19 | QQ20 | QQ21 |
| P1 | 5 | 4 | 4 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 4 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| P2 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 |
| P3 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 4 | 5 | 4 | 5 | 5 | 4 | 4 |
| P4 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| P5 | 5 | 5 | 5 | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 3 | 5 |
| P6 | 4 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 4 | 5 | 4 | 5 | 5 | 5 | 3 |
| P7 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 4 | 4 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 |
| P8 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |
| P9 | 4 | 5 | 5 | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 |
| P10 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 4 | 5 | 5 | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 5 |
| P11 | 5 | 4 | 5 | 5 | 4 | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 3 | 3 |
| P12 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 |
| P13 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 |
| P14 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 |
| P15 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 |
| P16 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 |
| P17 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 4 | 3 | 4 |
| P18 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 5 | 5 | 5 |
| P19 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 |
| P20 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |

## ANEXO 06: RESULTADO DE LA PRUEBA DE NORMALIDAD

| Variable - Dimension | Momento | Valor p | Resultado |
|---|---|---|---|
| Variable dependiente | Pretest | 0.0005 | Distribucion no normal |
| | Postest | 0.6406 | Distribucion normal |
| Dimension 1: Control de Acceso | Pretest | 0.0078 | Distribucion no normal |
| | Postest | 0.0911 | Distribucion normal |
| Dimension 2: Mecanismo de Seguridad | Pretest | 0.0006 | Distribucion no normal |
| | Postest | 0.0004 | Distribucion no normal |

**Interpretación de Resultado:**

Como se aprecia en la Tabla 5 en todos los casos se observó que al menos uno de los pares comparados cumplió distribuciones diferentes a la normal. Por tal motivo, fue necesario recurrir a pruebas no paramétricas, siendo seleccionada la prueba de Wilcoxon, considerando un valor p inferiror al 5% para confirmar diferencias significativas.

## ANEXO 07: PRIMER INFORME DE JUCIO DE EXPERTO SOBRE EL INTRUMENTO DE INVESTIGACIÓN

UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO
FACULTAD DE CIENCIAS
ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

### INFORME DE JUCIO DE EXPERTOS SOBRE INTRUMENTO DE INVESTIGACIÓN

**I. DATOS GENERALES**

| | |
|---|---|
| **Apellidos y nombres del experto:** | Joseph Darwin Alvarado Tolentino |
| **Institución donde labora:** | UNASAM |
| **Título y/o grado académico:** | Magister en ciencias en ingeniería con mención en auditoría y seguridad informática. |
| **Autor del instrumento:** | Bach. Carlos Eduardo Maguiña Javier |

**II. ASPECTOS DE VALIDACIÓN**

| Dimensiones | Indicadores | Deficiente 00-20% | Regular 21-40% | Buena 41-60% | Muy buena 61-80% | Excelente 81-100% |
|---|---|---|---|---|---|---|
| 1.CLARIDAD | Está formulado con lenguaje claro. | | | | ✓ | |
| 2.OBJETIVIDAD | Está expresado en conductas observables | | | | ✓ | |
| 3.ACTUALIDAD | Adecuado al avance de la ciencia y tecnología. | | | | ✓ | |
| 4.ORGANIZACIÓN | Existe una organización lógica. | | | | ✓ | |
| 5.SUFICIENCIA | Comprende los aspecto en cantidad y calidad | | | | ✓ | |
| 6.CONSISTENIA | Basado en aspectos teóricos - científicos | | | ✓ | | |
| 7.COHERENCIA | Entre los indicadores y dimensiones | | | | ✓ | |
| 8.METODOLOGIA | La estrategia responde al propósito. | | | | ✓ | |

**III. OBSERVACIONES:** NINGUNO

**IV. PROMEDIO DE VALORACIÓN:** MUY BUENA

Firma del experto

## ANEXO 08: SEGUNDO INFORME DE JUCIO DE EXPERTO SOBRE EL INTRUMENTO DE INVESTIGACIÓN

UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO
FACULTAD DE CIENCIAS
ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

### INFORME DE JUCIO DE EXPERTOS SOBRE INTRUMENTO DE INVESTIGACIÓN

### I. DATOS GENERALES

| | |
|---|---|
| **Apellidos y nombres del experto:** | Carlos Alberto Gonzales Ramos |
| **Institución donde labora:** | Poder Judicial de Ancash |
| **Título y/o grado académico:** | Magister en tecnologías de la información y comunicaciones. |
| **Autor del instrumento:** | Bach. Carlos Eduardo Maguiña Javier |

### II. ASPECTOS DE VALIDACION

| Dimensiones | Indicadores | Deficiente 00-20% | Regular 21-40% | Buena 41-60% | Muy buena 61-80% | Excelente 81-100% |
|---|---|---|---|---|---|---|
| 1.CLARIDAD | Está formulado con lenguaje claro. | | | | X | |
| 2.OBJETIVIDAD | Está expresado en conductas observables | | | | X | |
| 3.ACTUALIDAD | Adecuado al avance de la ciencia y tecnologia. | | | | | X |
| 4.ORGANIZACION | Existe una organización lógica. | | | | X | |
| 5.SUFICIENCIA | Comprende los aspecto en cantidad y calidad | | | | X | |
| 6.CONSISTENIA | Basado en aspectos teóricos - científicos | | | | | X |
| 7.COHERENCIA | Entre los indicadores y dimensiones | | | | X | |
| 8.METODOLOGIA | La estrategia responde al propósito. | | | | | X |

### III. OBSERVACIONES: NINGUNA

### IV. PROMEDIO DE VALORACIÓN: MUY BUENA

Firma del experto

FIRMA DIGITAL
Firmado digitalmente por: GONZALES RAMOS Carlos Alberto FAU 20571436575 soft
Motivo: Doy V° B°
Fecha: 10/12/2022 16:01:50-0500

## ANEXO 09: PAQUETE BASE DATOS DE ADMINISTRACION DML_VPD_ADMIN

| TIPO | NOMBRE DE LA ENTIDAD | DESCRIPCIÓN |
|---|---|---|
| PROCEDURE | output_error_message | Muestra el mensaje de error en el Output |
| FUNCTION | username_exists | Devuelve 1 si existe el usuario de la base de datos. Si no existe devuelve 0 |
| FUNCTION | client_identifier_exists | Devuelve 1 si existe el client_identifier. Si no existe devuelve 0. |
| PROCEDURE | create_priviledged_user | Crea el usuario privilegiado. El usuario privilegiado es el usuario que no tiene ninguna restricción de conexión |
| PROCEDURE | create_client_identifier | Crea el client_identifier o el identificador de cliente. Sirve para agrupar varios usuarios en un solo rol. |
| FUNCTION | modify_client_identifier_desc | Modifica la descripción de client_identifier. |
| FUNCTION | delete_client_identifier | Borra client_identifier. |
| FUNCTION | recover_client_identifier | Recupera el registro borrado de client_identifier. |
| PROCEDURE | create_rel_clid_user | Crea la relación entre el usuario de la base de datos y client_identifier. |
| FUNCTION | modify_user_clid | Modifica la relación entre el usuario de la base de datos y client_identifier |

| | | |
|---|---|---|
| FUNCTION | delete_rel_clid_user | Borra la relación de usuario de la base de datos y client_identifier. |
| FUNCTION | delete_clid_users | Borra todos los usuarios relacionados con un client_identifier. |
| PROCEDURE | create_terminal | Crea el registro de terminal. |
| PROCEDURE | create_rel_terminal_user | Crea la relación entre el usuario y terminal registrado. |
| FUNCTION | delete_rel_terminal_user | Borra la relación entre el usuario y el terminal registrado. |
| PROCEDURE | create_gora_vpd_param | Crea el parámetro de VPD. |
| FUNCTION | delete_gora_vpd_param | Borra el parámetro de VPD. |
| PROCEDURE | mask_column | Enmascara una columna de una tabla para un usuario de la base de datos o un client_identifier. (Crea la política y procedimiento que va a controlar el acceso a la columna). |
| PROCEDURE | unmask_column | Desenmascara la columna enmascarada. Ejecutar este proceso en horario de mantenimiento. |
| PROCEDURE | create_masked_column_exclusion | Crea la exclusión de la política de enmascaramiento de una columna para un usuario de la base de datos. |
| PROCEDURE | delete_masked_column_exclusion | Borra la exclusión de la política de enmascaramiento de una columna para un usuario de la base de datos. |
| PROCEDURE | restrict_session | Restringe la sesión de un usuario de la base de datos o client_identifier. |
| FUNCTION | unrestrict_session | Borra la restricción de un usuario de la base de datos o client_identifier. |
| PROCEDURE | create_username_sess_exclusion | Crea la exclusión de restricción de conexiones para un usuario de la base de datos. |
| PROCEDURE | audit_package_log | Crea el log de rastreo de las ejecuciones de los procedimientos del paquete. |
| FUNCTION | user_generic_exists | Devuelve 1 si existe el usuario genérico existe en el catálogo de la custodia. Si no existe devuelve 0. |
| FUNCTION | rel_terminal_gen_osuser_exists | Devuelve 1 si existe la relación de terminal con osuser y el usuario genérico ingresado en el catálogo de la custodia. Si no existe devuelve 0. |
| FUNCTION | delete_user_generic | Borra el usuario genérico del catálogo de custodia. Devuelve 0 si la operación concluyo satisfactoriamente. |
| PROCEDURE | delete_user_generic | Invoca la función de borrado de un usuario genérico del catálogo de custodia y fuerza el borrado de las relaciones existentes. |

| | | |
|---|---|---|
| PROCEDURE | delete_owner_generic | Borra el usuario dueño de un usuario genérico del catálogo de custodia. genérico del catálogo de custodia. |
| PROCEDURE | create_owner_user_generic | Crea un usuario dueño(OWNER) para un usuario genérico del catálogo de custodia. |
| PROCEDURE | modify_email_owner_generic | Modifica el email de un owner de usuario genérico matriculado. |
| PROCEDURE | modify_nombres_owner_generic | Modifica el nombre y apellido de un owner de usuario genérico matriculado. |
| PROCEDURE | modify_area_owner_generic | Modifica el área de un owner de usuario genérico matriculado |
| PROCEDURE | modify_caducidad_owner_generic | Modifica la fecha de caducidad de un owner de usuario genérico matriculado. |
| FUNCTION | create_user_generic | Crea un usuario genérico en el catálogo de custodia. Devuelve 0 si la operación concluyo satisfactoriamente. |
| PROCEDURE | create_user_generic | Invoca la función de borrado de un usuario genérico del catálogo de custodia. |
| PROCEDURE | delete_terminal | Procedimiento que invoca la función de eliminación de un terminal registrado. |
| PROCEDURE | delete_rel_terminal_gen_osuser | Procedimiento que invoca la función de eliminación de la relación existente entre un usuario genérico, terminal y el usuario de sistema operativo. |
| PROCEDURE | create_rel_terminal_gen_osuser | Procedimiento que invoca la función de creacion de una relación de entre un usuario genérico, terminal y el usuario de sistema operativo. |
| PROCEDURE | disable_rel_terminal_gen_osuser | Procedimiento que deshabilita una relación entre un usuario genérico, terminal y el usuario de sistema operativo |
| PROCEDURE | change_expiration_for_generic | Procedimiento que modifica la fecha de caducidad de todas las relaciones existentes respecto de un usuario genérico |
| PROCEDURE | recreate_policy_catalog | Procediemitno que recrea políticas en la BD en referencia de los datos del catálogo de la VPD pudiendo recrear todo el catalogo o una tabla especifica. |
| PROCEDURE | drop_all_policies_table | Procediemitno que elimina políticas en la BD, pero no del catálogo de la VPD de una tabla especifica. |

## ANEXO 10: PAQUETE BASE DATOS DE ADMINISTRACION DML_VPD

| TIPO | NOMBRE DE LA ENTIDAD | DESCRIPCIÓN |
|---|---|---|
| PROCEDURE | set_client_identifier | Se asigna al usuario un cliente identifier al inicio de su session. |
| PROCEDURE | check_session_restrictions | Realiza la validación de las restricciones y controles de inicio de session. |
| FUNCTION | mask_column_data | Función que aplica las restricciones de enmascaramiento de columnas. |
| PROCEDURE | session_logon_log | Procediemitno que realiza la grabación del log de inicio de session según las validacionesde restricciones echas. |
| PROCEDURE | get_etl_hour | Función que retorna el valor de la fecha de inicio de la restricción horaria de acuerdo conlos parámetros registrados para un usuario indicado. |

## ANEXO 11: DICCIONARIO DE TABLAS

| DML_VPD_AUDIT_LOGON | |
|---|---|
| COLUMNA | COMENTARIO |
| LOGON_TIME | Representa la fecha y hora de conexión a la base de datos. |
| AUDSID | Representa el identificador único de sesiones dentro de la base de datos Oracle (v$sesion). |
| USERNAME | Nombre de usuario de la base de datos Oracle. |
| CLIENT_IDENTIFIER | Representa el agrupador de usuarios de la base de datos según las restricciones establecidas.<br>Este valor se asigna al momento de conectarse con la base de datos Oracle. |
| OS_USER | Representa el nombre de usuario de sistema operativo (valor de la vista v$session de la base de datos Oracle) del usuario que se conectó a la base de datos. |
| TERMINAL | Representa el nombre de terminal (valor de la vista v$session de la base de datos Oracle) del usuario que se conectó a la base de datos. |
| MODULE | Representa el nombre del aplicativo (valor de la vista v$session de la base de datos Oracle) del usuario que se conectó a la base de datos. |
| RESTRICTION | Representa la restricción que se ha efectuado durante la conexión a la base de datos, según las reglas establecidas.<br>Por ejemplo:<br>0 - No tiene ninguna restricción (conexión admitida).<br>1 - Conexión rechazada (el horario de conexión no permite conectarse durante la ejecución del proceso ETL diario).<br>2 - Conexión rechazada (el número de sesiones supera el límite establecido por usuario).<br>3 - Conexión rechazada (terminal de usuario no corresponde al asociado). |
| LOGOFF_TIME | Representa la fecha y hora de la desconexión a la base de datos. |

| DML_VPD_CLIENT_IDENTIFIER | |
|---|---|
| CLIENT_IDENTIFIER | Representa el agrupador de usuarios de la base de datos según las restricciones establecidas. |
| CLIENT_IDENTIFIER_DESC | Representa la descripción de client_identifier. |

| | |
|---|---|
| CREATION_DATE | Representa la fecha de creación de registro. |
| USERNAME_CREATED | Representa al usuario de la base de datos que ha creado el registro. |
| MODIFIED_DATE | Representa la fecha de modificación de registro. |
| USERNAME_MODIFIED | Representa al usuario de la base de datos que ha modificado el registro. |

| DML_VPD_CLIENT_IDENTIFIER_LOG | |
|---|---|
| NUMSEQ | Representa el número único secuencial de modificaciones efectuadas en la tabla DML_VPD_CLIENT_IDENTIFIER. |
| CLIENT_IDENTIFIER | Representa el agrupador de usuarios de la base de datos según las restricciones establecidas. |
| OPERATION | Representa la operación efectuada (INSERT, UPDATE, DELETE). |
| CLIENT_IDENTIFIER_DESC | Representa la descripción de client_identifier (última antes de la operación efectuada). |
| CREATION_DATE | Representa la fecha de creación de registro. (última antes de la operación efectuada). |
| USERNAME_CREATED | Representa al usuario de la base de datos que ha creado el registro. (última antes de la operación efectuada). |
| MODIFIED_DATE | Representa la fecha de modificación de registro. (última antes de la operación efectuada). |
| USERNAME_MODIFIED | Representa al usuario de la base de datos que ha modificado el registro. (última antes de la operación efectuada). |
| DELETED_DATE | Representa la fecha de eliminación de registro. |
| USERNAME_DELETED | Representa al usuario de la base de datos que ha borrado el registro. |
| CLIENT_LEVEL | Representa el nivel de enmascaramiento. 1 - Nivel client_identifier = 2 - Usuario de la base de datos |
| CLIENT_NAME | Nombre del cliente dependiendo del nivel. |
| COLUMN_ID | Representa el identificador único por columna enmascarada. |
| CREATION_DATE | Representa la fecha de creación de registro. |

| | |
|---|---|
| USERNAME_CREATED | Representa al usuario de la base de datos que ha creado el registro. |
| MODIFIED_DATE | Representa la fecha de modificación de registro. |
| USERNAME_MODIFIED | Representa al usuario de la base de datos que ha modificado el registro. |

| DML_VPD_COLUMN_MASKING_EXCL | |
|---|---|
| CLIENT_LEVEL | Representa el nivel de enmascaramiento. 1 - Nivel client_identifier 2 - Usuario de la base de datos |
| CLIENT_NAME | Nombre del cliente dependiendo del nivel. |
| COLUMN_ID | Representa el identificador único por columna enmascarada. |
| CREATION_DATE | Representa la fecha de creación de registro. |
| USERNAME_CREATED | Representa al usuario de la base de datos que ha creado el registro. |
| MODIFIED_DATE | Representa la fecha de modificación de registro. |
| USERNAME_MODIFIED | Representa al usuario de la base de datos que ha modificado el registro. |
| EXPIRATION_DATE | Representa la fecha de caducidad del registro. |
| STATE | Representa el estado de habilitación del registro. |

| DML_VPD_MASKED_COLUMNS | |
|---|---|
| COLUMN_ID | Representa el identificador único por columna enmascarada. |
| OBJECT_OWNER | Representa el propietario del objeto que contiene la columna por enmascarar. |
| OBJECT_NAME | Representa el nombre del objeto cuya columna se va a enmascarar. |
| COLUMN_NAME | Representa el nombre de la columna que se va a enmascarar. |
| POLICY_IS_EXCLUSIVE | Representa el identificador si la política es exclusiva o no (S/N). |

| | |
|---|---|
| POLICY_NAME | Representa el nombre de la política generada automáticamente asociada al procedimiento también generado automáticamente. |
| CREATION_DATE | Representa la fecha de creación de registro. |
| USERNAME_CREATED | Representa al usuario de la base de datos que ha creado el registro. |
| MODIFIED_DATE | Representa la fecha de modificación de registro. |
| USERNAME_MODIFIED | Representa al usuario de la base de datos que ha modificado el registro. |

| GORA_VPD_PARAM | |
|---|---|
| PARAM_NAME | Representa el nombre único de parámetro. |
| PARAM_TYPE | Representa el tipo de parámetro. |
| | Por ejemplo, TIME representa el tiempo y el formato del mismo es HH:MI: SS |
| PARAM_VALUE | Representa el valor del parámetro |
| PARAM_DESCRIP | Representa la descripción de la función del parámetro. Por ejemplo: ETL_HOUR_INI - Inicio de hora etl - todos los días |
| CREATION_DATE | Representa la fecha de creación de registro. |
| USERNAME_CREATED | Representa al usuario de la base de datos que ha creado el registro. |
| MODIFIED_DATE | Representa la fecha de modificación de registro. |
| USERNAME_MODIFIED | Representa al usuario de la base de datos que ha modificado el registro. |

| DML_VPD_PRIVILEDGED_USERS | |
|---|---|
| USERNAME | Representa el nombre de usuario de la base de datos (USERNAME) que tiene privilegios de conexión a la base de datos sin restricciones establecidas. |
| DESCRIP | Representa la descripción o rol que cumple el usuario privilegiado. |
| CREATION_DATE | Representa la fecha de creación de registro. |

| | |
|---|---|
| USERNAME_CREATED | Representa al usuario de la base de datos que ha creado el registro. |
| MODIFIED_DATE | Representa la fecha de modificación de registro. |
| USERNAME_MODIFIED | Representa al usuario de la base de datos que ha modificado el registro. |

| DML_VPD_REL_CLID_USER | |
|---|---|
| USERNAME | Nombre de usuario de la base de datos Oracle. |
| CLIENT_IDENTIFIER | Representa el agrupador de usuarios de la base de datos según las restricciones establecidas. |
| CREATION_DATE | Representa la fecha de creación de registro. |
| USERNAME_CREATED | Representa al usuario de la base de datos que ha creado el registro. |
| MODIFIED_DATE | Representa la fecha de modificación de registro. |
| USERNAME_MODIFIED | Representa al usuario de la base de datos que ha modificado el registro. |

| DML_VPD_REL_TERMINAL_USER | |
|---|---|
| USERNAME | Nombre de usuario de la base de datos Oracle. |
| TERMINAL | Representa el nombre de terminal. |
| CREATION_DATE | Representa la fecha de creación de registro. |
| USERNAME_CREATED | Representa al usuario de la base de datos que ha creado el registro. |
| MODIFIED_DATE | Representa la fecha de modificación de registro. |
| USERNAME_MODIFIED | Representa al usuario de la base de datos que ha modificado el registro. |

| DML_VPD_SESSION_RESTRICT_EXCL | |
|---|---|
| CLIENT_LEVEL | Representa el nivel de enmascaramiento. 2 - Usuario de la base de datos |
| CLIENT_NAME | Nombre del cliente dependiendo del nivel. |
| RESTRICTION_TYPE | Representa el tipo de exclusión. |
| RESTRICTION_VALUE | Representa el valor de exclusión. |

| | |
|---|---|
| CREATION_DATE | Representa la fecha de creación de registro. |
| USERNAME_CREATED | Representa al usuario de la base de datos que ha creado el registro. |
| MODIFIED_DATE | Representa la fecha de modificación de registro. |
| USERNAME_MODIFIED | Representa al usuario de la base de datos que ha modificado el registro. |

| DML_VPD_SESSION_RESTRICTIONS | |
|---|---|
| CLIENT_LEVEL | Representa el nivel de enmascaramiento. 1 - Nivel client_identifier = 2 - Usuario de la base de datos |
| CLIENT_NAME | Nombre del cliente dependiendo del nivel. |
| CONTROL_TERMINAL | Representa el Flag de control (S/N) si se controla el acceso a la base de datos por terminal. |
| CONTROL_ETL_HOUR | Representa el Flag de control (S/N) si se controla el horario restringido (proceso de rutina ETL). |
| MAX_NO_SESSIONS | Representa el número máximo de sesiones que se pueden establecer con la base de datos Oracle. |
| CREATION_DATE | Representa la fecha de creación de registro. |
| USERNAME_CREATED | Representa al usuario de la base de datos que ha creado el registro. |
| MODIFIED_DATE | Representa la fecha de modificación de registro. |
| USERNAME_MODIFIED | Representa al usuario de la base de datos que ha modificado el registro. |

| DML_VPD_TERMINAL | |
|---|---|
| TERMINAL | Representa el nombre de terminal. |
| TERMINAL_DESC | Representa la descripción de terminal. |
| CREATION_DATE | Representa la fecha de creación de registro. |
| USERNAME_CREATED | Representa al usuario de la base de datos que ha creado el registro. |
| MODIFIED_DATE | Representa la fecha de modificación de registro. |
| USERNAME_MODIFIED | Representa al usuario de la base de datos que ha modificado el registro. |

| DML_VPD_USER_GENERIC | |
|---|---|
| USER_GENERIC_NAME | Nombre de usuario genérico de la base de datos Oracle. |
| USER_GENERIC_DESC | Descripción del usuario genérico de la base de datos Oracle. |
| CREATION_DATE | Representa la fecha de creación de registro. |
| USERNAME_CREATED | Representa al usuario de la base de datos que ha creado el registro. |
| MODIFIED_DATE | Representa la fecha de modificación de registro. |
| USERNAME_MODIFIED | Representa al usuario de la base de datos que ha modificado el registro. |

| DML_VPD_REL_TERMIN_OSUSER_GEN | |
|---|---|
| USER_GENERIC_NAME | Nombre de usuario genérico de la base de datos Oracle. |
| OSUSER | Nombre del usuario de sistema operativo. |
| TERMINAL | Representa el nombre de terminal (valor de la vista v$session de la base de datos Oracle) del usuario que se conectó a la base de datos. |
| STATE | Representa el estado de habilitación del registro. |
| CREATION_DATE | Representa la fecha de creación de registro. |
| USERNAME_CREATED | Representa al usuario de la base de datos que ha creado el registro. |
| MODIFIED_DATE | Representa la fecha de modificación de registro. |
| USERNAME_MODIFIED | Representa al usuario de la base de datos que ha modificado el registro. |
| EXPIRATION_DATE | Representa la fecha de caducidad del registro. |

| DML_VPD_AUDIT_LOGON_PART | |
|---|---|
| LOGON_TIME | Representa la fecha y hora de conexión a la base de datos. También representa la clave de Particionamiento. |
| CODMES | Valor del código de mes que se realiza el registro (YYYYMM) |

| | |
|---|---|
| AUDSID | Representa el identificador único de sesiones dentro de la base de datos Oracle (v$sesion). |
| USERNAME | Nombre de usuario de la base de datos Oracle. |
| CLIENT_IDENTIFIER | Representa el agrupador de usuarios de la base de datos según las restricciones establecidas.<br>Este valor se asigna al momento de conectarse con la base de datos Oracle. |
| OS_USER | Representa el nombre de usuario de sistema operativo (valor de la vista v$session de la base de datos Oracle) del usuario que se conectó a la base de datos. |
| TERMINAL | Representa el nombre de terminal (valor de la vista v$session de la base de datos Oracle) del usuario que se conectó a la base de datos. |
| MODULE | Representa el nombre del aplicativo (valor de la vista v$session de la base de datos Oracle) del usuario que se conectó a la base de datos. |
| RESTRICTION | Representa la restricción que se ha efectuado durante la conexión a la base de datos, según las reglas establecidas.<br>Por ejemplo:<br>0 - No tiene ninguna restricción (conexión admitida).<br>1 - Conexión rechazada (el horario de conexión no permite conectarse durante la ejecución del proceso ETL diario).<br>2 - Conexión rechazada (el número de sesiones supera el límite establecido por usuario).<br>3 - Conexión rechazada (terminal de usuario no corresponde al asociado). |
| LOGOFF_TIME | Representa la fecha y hora de la desconexión a la base de datos. |