
# UNIVERSIDAD PRIVADA TELESUP

## FACULTAD DE INGENIERÍA Y ARQUITECTURA
## ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMATICA

## TESIS

# PROPUESTA DE UNA POLÍTICA DE SEGURIDAD PARA LA BASE DE DATOS OSSAB DEL AMBIENTE DE PRODUCCIÓN EN EL ORGANISMO ESPECIAL DEL FONDO DE VIVIENDA MILITAR DEL EJÉRCITO ORES-FOVIME LIMA – PERÚ EN EL AÑO 2017

**PARA OPTAR EL TÍTULO PROFESIONAL DE:**

**INGENIERIO DE SISTEMAS E INFORMATICA**

**AUTOR:**

**BACH. VILLAR ROMERO MARIA PAULINA**

**LIMA-PERU**
**2017**

**ASESOR DE TESIS**

---

**ING. ANGEL NOÉ QUISPE TALLA**

**JURADO EXAMINADOR**

---

**MG. EDMUNDO JOSE BARRANTES RIOS**

**PRESIDENTE**

---

**MG. DENIS CHRISTIAN OVALLE PAULINO**

**SECRETARIO**

---

**MG. EDWIN HUGO BENAVENTE ORELLANA**

**VOCAL**

## DEDICATORIA

A Dios por brindarme salud, a mis padres por traerme a este mundo maravilloso, a mi familia por su paciencia y apoyo incondicional y a mis familiares que contribuyeron para que se concluya con éxito este proyecto. Sin ellos nada de esto habría podido ser.

## AGRADECIMIENTO

A Dios por permitirme conocer esta experiencia maravillosa de la vida, por darme salud y fortaleza, agradecer a mi esposo e hijos por su tolerancia en todo momento y compañeros de la universidad Privada Telesup.

.

## RESUMEN

El presente trabajo de investigación tiene como objetivo determinar si la fuga de información tiene influencia en la seguridad de la información en la base de datos OSSAB en el ambiente de producción del Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME". El enfoque de la de la investigación fue cualitativo y cuantitativo con un esquema deductivo y lógico de tipo exploratorio – descriptivo, con un alcance correlacional que permite especificar las propiedades del problema sometido a estudio e interpretar la realidad existente.

Se tuvo en cuenta la información oficial disponible acerca de la seguridad en la información para el adecuado uso de los lineamientos en una política de seguridad en la información, así como producciones originales que se proponen profundizar el conocimiento de la seguridad en la información, que en la actualidad presenta un nivel de conocimiento incipiente. Por otro lado, se tuvo en cuenta la muestra representada por presentada 70 colaboradores de la entidad, los mismos que participaron de la encuesta compuesta por veinticinco preguntas de tipo cerradas, las que con ayuda de la estadística se pudo obtener resultados claros y precisos, los mismos que se procesaron mediante el programa informático SPSS. El resultado permitió la contratación de las hipótesis planteadas en la investigación, lo que se evidencia la vulnerabilidad en la seguridad para la Base de Datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME.



Palabras Claves: Política de seguridad, base de datos, vulnerabilidad de datos.

## ABSTRACT

The objective of this research work is to determine if information leakage influences the security of information in the OSSAB database in the production environment of the Special Agency of the Military Housing Fund of the ORES-FOVIME Army. " The focus of the research was qualitative and quantitative with a deductive and logical scheme of exploratory - descriptive type, with a correlational scope that allows specifying the properties of the problem under study and interpreting the existing reality.

The available official information about information security was taken into account for the adequate use of the guidelines in an information security policy, as well as original productions that aim to deepen the knowledge of information security, which in the present presents a level of incipient knowledge. On the other hand, the sample represented by 70 employees of the entity was taken into account, the same ones that participated in the survey composed of twenty-five closed type questions, which with the help of the statistics could obtain clear and precise results, the same that were processed through the SPSS software. The result allowed the hiring of the hypotheses raised in the investigation, which demonstrates the vulnerability in the security of the OSSAB database information of the production environment in the Special Organism of the Military Housing Fund of the ORES-FOVIME Army.



Keywords: Security policy, database, data vulnerability.

## INDICE DE CONTENIDO

## INDICE DE TABLAS

## INDICE DE FIGURAS

# INTRODUCCIÓN

Propuesta de una política de seguridad para la información de la base de datos del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejercito ORE-FOVIME constituye un factor clave para el resguardo de la información, siendo un activo principal dentro de una empresa, en la actualidad no basta que una organización contrate a personal para administrar la información de base de datos, sino también se debe tener claro los controles y procedimientos de acceso al personal que accede al servidor de base de datos, habitualmente desarrollan sus actividades cotidianas sin un enfoque de seguridad en la información que manejan.

En el Perú, hoy en día la tecnología abarca un gran porcentaje de crecimiento, lo cual se desprende que en la mayoría de las empresas en nuestro país utilizan sistemas informáticos, en consecuencia, implica una serie de factores, entre ellos considerar políticas de seguridad para proteger la información que almacenan los equipos informáticos, siendo un proceso que se debe dar cumplimiento a las políticas planteadas.

Pero hasta ahora las políticas de seguridad han merecido análisis como un problema en la seguridad de la información en los equipos informáticos que almacena información de baja, media y alta importancia. Ha sido muy poco explorado el tema de la relación entre las políticas de seguridad y la información que se almacena en los equipos tecnológicos.

Por lo cual el presente trabajo de investigación busca hacer un análisis conociendo los factores de la incidencia de la seguridad informática y como poder proteger la información de los equipos informáticos en las diferentes entidades de nuestro país.

# I. PROBLEMA DE INVESTIGACIÓN

## 1.1 Planteamiento del problema

El Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME cuenta actualmente con dos bases de datos en el ambiente de producción. Donde se almacenan datos del personal militar, información de estados de cuentas, registros de aportes del personal militar y créditos hipotecarios del personal militar del Organismo Especial del Fondo de Vivienda ORES-FOVIME actualmente la información almacenada en la base de datos "ADWIN" cuenta con registros que son usados de consultas información el año 2004 hasta el 2012. A partir de esa fecha la información se empezó a registrar en la nueva base de datos "OSSAB" hasta la fecha.

La información almacenada en la base de datos "ADWIN" se ha venido migrando a la base de datos "OSSAB". Y el objetivo es migrar toda la información a esta base de datos. Para la base de datos "ADWIN" existen políticas de seguridad. Sin embargo, para la nueva base de datos "OSSAB" no se tiene definida ninguna política de seguridad.

Se realizó consultas a la base de datos OSSAB y los aplicativos mediante el cual ingresan la información a la base de datos OSSAB, siendo uno de los principales activos para el Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME. El enraizamiento de ataques informáticos en nuestro país se ha dado en diferentes entidades, es una de las actividades de alcance económico, que funciona como una maquina o un negocio donde rige el principio de la jerarquía piramidal, cuyas cimas quedan en el más alto absoluto anonimato cuando sucede un ataque informático, debido a las políticas de seguridad que no se encuentran establecidas en la mayoría de las entidades públicas.

En la actualidad los ataques informáticos son cada vez más frecuentes en las entidades que no cuentan con un plan de políticas establecidas para la protección de su información. Es en este ámbito de la tecnología, hoy en día la demanda de las grandes y medianas empresas se han incrementado conforme a las necesidades del negocio el cual en muchos aspectos tiende a ser incierto y cambiante, para que las empresas puedan adaptarse a este

escenario necesitan tener una cultura donde predomine la flexibilidad y mejora continua en sus procesos. Uno de los rubros del mercado tecnológico donde esta tendencia es mucho mayor son las consultoras y agencias de publicidad digital las cuales tienden a actualizar su forma de trabajo conforme la tecnología avance, esto con el fin de ofrecer un producto competitivo a sus clientes tales como aplicaciones web, aplicaciones para dispositivos móviles, servicios web, tratamiento de datos, documentación, etc.

La demanda cambiante y la diversidad de proyectos a veces juega en contra de la gestión de los mismos, muchas veces durante el desarrollo de los proyectos informáticos se tiende a perder visión del avance y la gestión de los recursos los cuales se ven reflejados en atrasos y principalmente de un seguimiento de control y monitoreo de acceso a la información y en algunos casos no se aplica lo cual impacta negativamente en la protección de la información en las empresas, una de las causas de esta mala gestión es la ausencia de un plan de políticas de seguridad que permitan realizar el seguimiento adecuado.

Por las consideraciones anteriores la investigación se analizará y desarrollará una propuesta de políticas de seguridad del acceso a la información, que se adapte con facilidad a los aplicativos que manejan, para el seguimiento del desarrollo del proyecto informático.

En consecuencia, la base de datos OSSAB asegure mantener la integridad, confidencialidad y disponibilidad de los sistemas. Para cumplir con estos objetivos se definen los aspectos más importantes que deberá contemplar dicha política:

Seguridad de la plataforma de las Bases de datos, Seguridad de los usuarios de la base de datos, Seguridad de las credenciales de las bases de datos, Seguridad de las conexiones a las bases de datos, Integridad de las bases de datos, Auditoria de las Bases de datos.

Otro aspecto de seguridad a tener en cuenta es que este servidor de base de datos se encuentra sin ningún firewall (muro de fuego sistema que es utilizado para proteger una computadora en particular o bien una red, normalmente su objetivo es evitar el ingreso de agentes externos, no

autorizados); lo cual implica riesgos de fuga de información debido a que cualquier usuario externo puede conectarse.

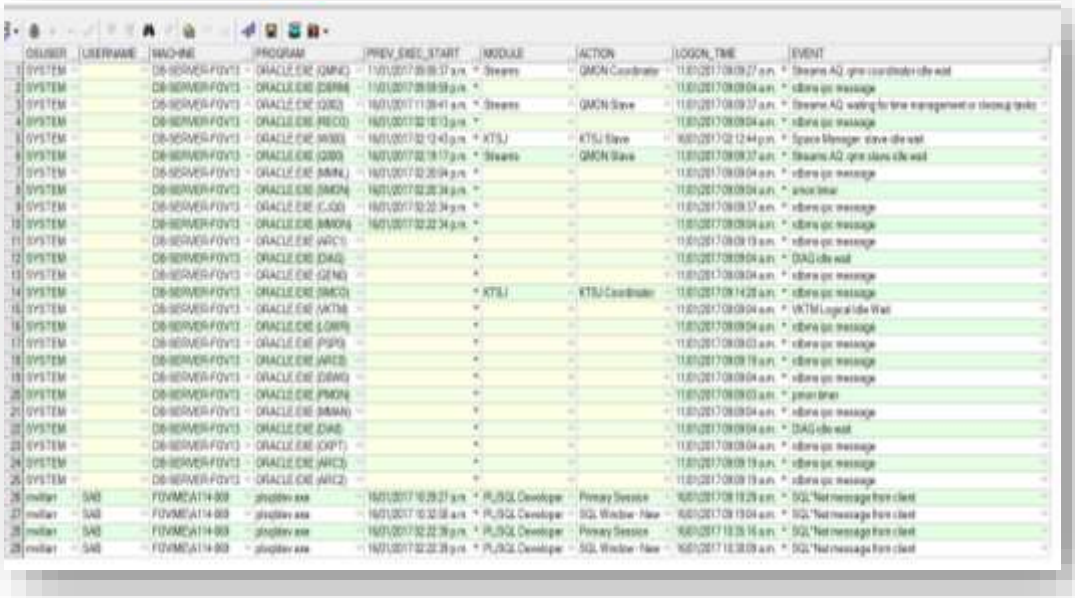
Para apoyar con el cumplimiento y seguimiento de la política de seguridad de la base de datos se ha adquirido una herramienta (Firewall para protección de base de datos). Con la cual se busca hacer seguimiento a las medidas de seguridad planteadas en la definición de la política. Para mitigar las diferentes vulnerabilidades.

**Figura 1:** Nombre de la base de datos del ambiente de producción OSSAB

| | NAME | TYPE | VALUE | DISPLAY_VALUE | ISBASIC | DESCRIPTION | HASH |
|---|---|---|---|---|---|---|---|
| 1 | db_name | 2 | OSSAB | OSSAB | TRUE | database name specified in CREATE DATABASE | 704871292 |

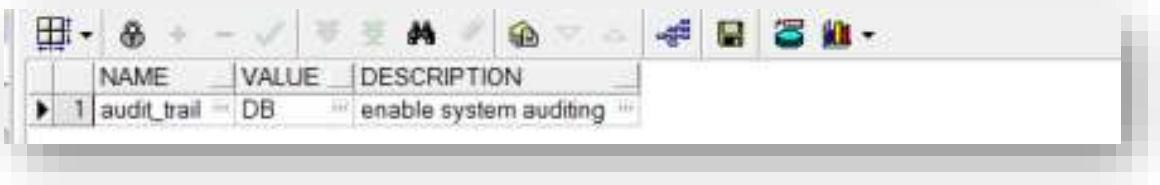
**Fuente**: Elaboración propia

**Figura 2:** Vista que muestra conexiones a la base de datos OSSAB



**Fuente**: Elaboración propia

**Figura 3:** Auditoria por default que es manipulada por administrador de Base de Datos



| | NAME | VALUE | DESCRIPTION |
|---|---|---|---|
| 1 | audit_trail | DB | enable system auditing |

## 1.2 Formulación del Problema

### 1.2.1 Problema General

¿De qué manera influye una política de seguridad para la base de datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME?

### 1.2.2 Problemas Específicos

**a)** ¿De qué manera influye la revisión de la configuración en la base de datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME?

**b)** ¿De qué manera influyen las pruebas de penetración en la base de datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME?

## 1.3 Justificación del Estudio

La seguridad informática es una necesidad presente en cualquier institución, cuando se tienen protocolos, controles y procedimientos que permitan verificar que los objetivos de continuidad de servicio, confidencialidad y seguridad de la información, se cumpliría satisfactoriamente con las características primordiales de la información, y así se prevería la alteración de sistemas, ataques y accesos no autorizados. Es por ello que una política de seguridad en la información para el ambiente de producción OSSAB de base de datos para el registro de información debe estar debidamente establecido de acuerdo a su función que realiza cada colaborador y así pueda realizarse un mayor control a cada usuario para que carece de políticas en su acceso al sistemas y también tener en cuenta la protección en sus estaciones de punto final en la red del ORES – FOVIME, debido a que se le lleve un seguimiento adecuado y sirva como materia de investigación en casos que sean necesarios. Actualmente en la mayoría de las entidades, han considerado implementar políticas y lineamientos para la protección en su información y llevar una seguridad adecuada, para sus activos de

información, debido a los casos críticos que suceden por falta de asesoramiento o personal no capacitado para la implementación de políticas.

Líneas anteriores mencione que actualmente las empresas manejan su información y la administran por medio de un software, así como también consideran otros factores necesarios para la evaluación de riesgos de su información que manejan con el fin de salvaguardar la integridad y seguridad de la información, en donde esta política de seguridad evitará pérdidas de información, motivo por el cual se propone la implementación de una política de seguridad para la información de la base de datos del ORES-FOVIME, que de acuerdo a la auditoría realizada se presenta como una necesidad que se fundamenta en los casos expuestos por los funcionarios. En base a ello se considera tener políticas implementadas de procedimientos y métodos con el objetivo de administrar y proteger el activo de la información.

Respecto a la implementación de política de seguridad para la información de la base de datos OSSAB del ambiente de producción del ORES-FOVIME, se podrán evaluar los riesgos en las estaciones de trabajo dentro de la organización y llegar a obtener el control total de la información alojada en sus servidores y se creará la responsabilidad de cada colaborador por la información que manipule, de lo anterior concurrirá un sentido de conciencia del funcionamiento adecuado del acceso a datos. El resultado de lo anterior admitirá el control de los datos en las terminales de punto final de los colaboradores en la organización.

El desarrollo de una política de seguridad en la empresa es posible, porque el investigador se desempeñó como auditor de sistemas por lo tanto es factible que tenga acceso de explorar la seguridad en la base de datos de la empresa ya que, si se aplica una metodología para evaluar el riesgo que ésta corre al no tener los mecanismos de certidumbre en la entidad, se podrían presentar inconvenientes en sus actividades y como consecuencia violación a la información confidencial.

De tal manera, existe la posibilidad que la empresa tenga pérdidas en sus proyectos de desarrollo y en sus bancos de datos que mantienen

convenios, por lo que esto implicaría pérdidas para la empresa, que podría ser derivado del robo de información lo cual le afectaría económicamente y llevaría a la quiebra de la misma.

El estudio de amenazas y riesgos de la información nos proporciona ventajas para implantar procedimientos y controles con el objeto de administrar y proteger y salvaguardar uno de los activos más importantes, la información. También repercute en el uso debido de recursos de hardware y el acceso controlado a las necesidades del usuario para cumplir eficientemente con sus actividades. Así de esta manera favorecer a que otras empresas tomen este ejemplo de implantación de políticas.

En base a la experiencia se elaboró la siguiente pregunta de investigación. Las bases de datos del Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME almacenan datos sensibles como se define en su Reglamento del Organismo Especial del Fondo de Vivienda Militar del Ejército (ORES - FOVIME) Para los cuales la ley exige que en ninguna circunstancia puedan ser revelados. Además, almacenan información del personal acerca de sus aportes al Fondo y préstamos de crédito hipotecarios, información que hace que las bases de datos sean atractivas para cualquier atacante.

Un servicio con deficiencias de políticas de seguridad que han ocasionado a la fecha casos que no se identifican a los responsables debido a que la auditoría interna de Base de Datos no se encontraba activa y no existen políticas de acceso a la información, el cual permitió obtener un control total de la red interna del servidor de Base de Datos OSSAB para realizar dichos movimientos de dinero, siendo una amenaza para todos los clientes de la misma, perjudicándolos económicamente. Estos ataques dirigidos contra datos sensibles información del personal Militar aportes, créditos hipotecarios, se debido a la importancia de la información almacenada en las bases de datos del ambiente de producción OSSAB del ORES-FOVIME, en efecto este debe cumplir ciertos estándares de seguridad de la información, dando cumplimiento de la norma ISO 27001 y la Norma Técnica Peruana para el uso y desarrollo de software. Norma en la cual el ORES-FOVIME busca apoyarse como marco de referencia y aplicar las

buenas prácticas estipuladas para el uso de la información y el desarrollo de software.

Para obtener este procedimiento el ORES-FOVIME deberá implementar una serie de políticas. Entre ellas una de seguridad de bases de datos; que contenga lineamientos y controles a los cuales se les pueda hacer un seguimiento de cumplimiento.

## 1.4 Objetivos de la Investigación

### 1.4.1 Objetivo General

Proponer una política de seguridad para la base de datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME.

### 1.4.2 Objetivos específicos

**a)** Proponer la revisión de la configuración en la base de datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME.

**b)** Proponer las pruebas de penetración en la base de datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME.

# II. MARCO TEÓRICO

## 2.1. Antecedentes de la investigación

### 2.1.1. Antecedentes Nacionales

**a) PORRAS y HERRERA (2016),** el autor describe

**b)** En su tesis para optar el Título Profesional de Ingeniero de Sistemas, de la Universidad San Martin de Porres, Perú, Titulada: "*Diseño e implementación de un sistema de Gestión de Seguridad de Información en Procesos Tecnológicos*", Conclusiones:

- Concluye que el implementar una política de seguridad implica que los colaboradores conozcan e interiorizan la importancia de un activo y por ello se debe tener como prioridad un plan de políticas de seguridad de la información y que esté vigente para utilizar en cualquier ambiente de producción de base de datos, debido a que conllevará a tener una visión clara sobre la protección de datos y el grado de datos sensibles que manejan por tratarse de dinero y son atractivos para cualquier experto en ataques cibernéticos, en consecuencia deben tenerlo presente en sus accesos diarios a la información que consultan, registran o generan reportes y así evitar riesgos de fuga de información o ataques de hackers.
- Tener en cuenta que el implementar políticas de seguridad, va acompañado de otros factores, para cumplir el objetivo de la protección de datos. Como es de conocimiento general el tener implementado reglas y normas en un ambiente de producción no siempre cumple con lo establecido, debido a que no se realiza el seguimiento e implementación completa de todos los mecanismos necesarios y en un futuro no se presenten amenazas, vulnerabilidades y, mayores riesgos. Este escenario se puede controlar y evitar; siempre y cuando las políticas estén bien definidas y los colaboradores estén

comprometidos con el cuidado de acceso a datos, de lo contrario se debe estar preparado los mecanismos para actuar de manera inmediata ante cualquier vulnerabilidad que se identifique.

- Analizar, evaluar e implementar lineamientos claros para gestionar los riesgos y ejecutando los planes de tratamiento de riesgos planteados, para lograr reducir a niveles aceptables gran porcentaje de riesgos que afecten a los activos de información.
- El personal colaborador es un factor crítico para la implementación de las políticas de seguridad, es por ello que se deben realizar talleres se sensibilización, concientización y capacitación de los mismos siendo indispensable para lograr una implementación exitosa.
- Mayormente las entidades mantienen de manera desordenada sus activos, sin considerar la importancia que tienen, y crecen con paradigmas equivocados, algunos quieren documentar todo lo que se pueda, y otras creen que documentar las incidencias es una pérdida de tiempo. Sin realizar un análisis previo de todos los casos expuestos, que se debe documentar solo lo necesario.

De lo anterior se concluye que es necesario sensibilizar, concientizar y capacitar al colaborador para que aplique en su totalidad el uso correcto del sistema para el acceso a datos y se realice el cumplimiento a la política implementada para evitar riesgos de perdida de información.

c) **Según TERAN (2014),** en su tesis para optar el Título Profesional de Ingeniero Industrial, de la Universidad Pontificia Católica del Perú, Perú, Titulada: "*Propuesta de implementación de un sistema de gestión de seguridad para el control de accesos a las aplicaciones en empresas que se desarrollan software administrativo y de negocio*", el autor concluye lo siguiente:

El módulo se seguridad que se desarrolla de acuerdo a la plataforma que se encuentran desarrolladas las aplicaciones de negocio y sistemas administrativos, deben tener lineamientos y políticas establecidos para el acceso a datos, y evitar fugas de información, teniendo en cuenta los casos críticos que ya existieron respecto a la vulnerabilidad de la información que ocasiono perdidas de dinero. Las políticas y lineamientos, deben ser actualizados de acuerdo a las necesidades de la entidad y mantenerse en un nivel de adecuado para el seguimiento y control de los accesos. Es por ello que los colaboradores antes de asumir dicha función deben aceptar como requisito fundamental el compromiso de la protección de datos, y deben ser debidamente capacitados y motivados, y otorgar ideas y puntos de vista que faciliten la adaptación a los cambios.

Otro aspecto de gran jerarquía es la creación de una cultura en la entidad que eleve un nivel de formación y participación de todos los colaboradores, así como el espacio y mantenimiento del apropiado clima laboral.

Considerar los registros de las incidencias diarias presentados en la entidad, con el fin de establecer planes de prevención para evitar casos repetitivos de estos.

La implementación de la política de seguridad favorece con el resguardo de la información y con el progreso continuo de la entidad a través de los mecanismos implementados para el control y la unificación de la prevención en todos los niveles jerárquicos de la entidad al acceso a datos y la utilización de las políticas definidas y se ejecute de manera adecuada para la protección de datos.

d) **Según CARRANZA y VASQUEZ (2013),** en su tesis para optar el Título Profesional de Ingeniero de Sistemas, de la Universidad Privada Antenor Orrego, Perú, Titulada: *"Plan de mejora de la Seguridad de Información y Continuidad del Centro de Datos de la*

*Gerencia Regional de Educación La Libertad aplicando lineamientos de políticas y buenas prácticas apoyado del ISO 27001*", el autor concluye:

Que, a través del estudio de requisitos, evaluación de riesgos, optimización y alineación de los documentos a través de políticas propuestas, permitió tener un mayor enfoque para la mejora de las actividades de cada una de las fases de la auditoría facilitando con ello el análisis y evaluación del centro de datos, concluyéndose que tiene una seguridad insipiente, de baja aplicación de las normas técnicas y buenas prácticas, adolece de políticas de seguridad para la información.

Uno de los factores importantes para el cumplimiento de normas y políticas es el compromiso de los colaborares, como menciones líneas anteriores, se requiere el apoyo total y compromiso de ambas partes y el apoyo de la Gerencia, así poder aplicar en su totalidad los lineamientos establecidos en la política propuesta. Y considerando un seguimiento necesario para encontrar sus debilidades y así mejorar continuamente las políticas establecidas que se adapten a las necesidades de la entidad. De la misma manera, considerar todos los factores y en conjunto buscará el beneficio de la organización a través de las recomendaciones expuestas por los especialistas. Continuamente se debe tener en cuenta el personal autorizado y no autorizado a los ambientes de los servidores donde se aloja la información considerado como un activo principal de la entidad y evitar inconvenientes. Ej.: Personas que vienen a realizar trámites de reportes de estado de deudas u otros que se encuentren en el mismo edificio y transitan por pisos que no son los adecuados. El personal de recepción entrega un ticket de visitante y no pregunta a quien va a visitar la persona a la cual le entrega el ticket. Las puertas de acceso a la base de datos no se lleva un control para el acceso al software, no existe un control de quienes ingresan o salen del centro del acceso a datos a través del software al ambiente de producción OSSAB, así como

la hora en que se produjo la entrada o salida. Se deben realizar procedimientos de control, para mejora alineados a buenas prácticas y lineamientos internacionales, Así mismo el Plan de la propuesta de políticas que debe estar definido y alineado a las necesidades de la entidad. Básicamente tener un seguimiento y control del acceso de usuarios, considerando el acceso al software por modulo, perfiles y roles en la organización y que se encuentren identificados la cantidad que existe con acceso a datos, respecto a ello se debe determinar los tiempos las validaciones correspondientes del software que cumpla con el ciclo de vida de desarrollo del software, bajo los lineamientos y políticas establecidos en los procesos de cada dirección definida mediante directivas y resoluciones y no afectar financieramente a la entidad. Las normas de control interno se cumplen en un 50% debido al cambio de colaboradores en la entidad, 131 puestos que los encargados del área de sistemas, operaciones y soporte técnico se retiraron borrando toda la información. Lo que conlleva a revisar el procedimiento de contratación de servicios con terceros que afectan servicios de TI en que se considera un análisis de riesgo previo por cambios de proveedores o cambios en el alcance del servicio de colaboradores. Lo cual debe ponerse mayor énfasis en el Control de Cambios en los Sistemas, para clasificarlos debidamente de acuerdo a su urgencia y prioridad del core del negocio que se maneja en la entidad. Necesariamente debe asignarse un personal responsable para la administración de las fuentes en el ambiente de desarrollo, que sea quién libere los objetos mediante solicitudes aprobadas y sustentadas técnicamente para la continuidad de los servicios.

Los escenarios de contingencia expuestos que cubren el Plan de Continuidad de Negocio son insuficientes para cubrir las operaciones de negocio ante catástrofes: incendio del edificio de la institución, terremotos, etc., se basan en un Plan de

contingencia que debe ser contemplado para la entidad y los recursos que administra,

El plan de políticas de seguridad de la información, mejora a través de tallares de concientización y capacitación a los colabores, aplicando las buenas prácticas, lo cual requiere una participación completa a nivel estratégico. El personal responsable de la implementación de políticas, debe tener conocimiento claro sobre el entorno de la entidad y los bienes que administra, ya que, de esta manera lograra tener actualizado el plan de acuerdo a la necesidad que requiere la entidad y poder obtener resultados de los objetivos propuestos como meta por parte de la entidad. De implantarse un Sistema de gestión de Seguridad de la Información y la instalación de un ambiente de prueba, estos impactarán significativamente sobre la calidad de los sistemas de información.

e) **Según MAMANI (2014),** en su tesis para optar el Título Profesional de Ingeniero de Sistemas, de la Universidad Nacional del Altiplano, Perú, Titulada: "*Modelo de Sistemas Criptográfico de seguridad para las redes de comunicaciones en la región Puno – 2012*", conclusiones:

**PRIMERO**: Utilizando modelo de seguridad, buenas prácticas y arquitecturas que pueden asegurar al cliente la integridad y fiabilidad de sus datos e información se consigue la anhelada confianza y satisfacción que es muy importante para cualquier empresa.

**SEGUNDO**: La aplicación del modelo de seguridad y el uso del protocolo SSL junto con la técnica de cifrado asimétrica, ayuda a mantener la confidencialidad e integridad de los datos e información durante el envío sobre las redes de comunicaciones, protegiendo de esta manera las transacciones de información privada de una entidad a través de Internet.

**TERCERO**: El uso de protocolo SSL VeriSign ofrece de manera sencilla crear conexiones seguras por internet, es el más indicado

para controlar operaciones en determinadas aplicaciones web cuando los ataques son múltiples y sofisticados, es muy apropiado para la seguridad de una página web de la entidad. Así mismo la metodología de proceso unificado de desarrollo de software, es adecuada para todo tipo de aplicación, sobre todo en lo referente al análisis y diseño.

f) **Según CAMPOS (2015), el** desarrollo del Sistema de Gestión de Seguridad y Salud Ocupacional bajo los requerimientos de la Norma Internacional OHSAS 18001, a diferencia de los sistemas de seguridad actuales, puede evaluarse y certificar, siendo enteramente compatible con las normas internacionales ISO 9001 e ISO 14001 facilitando la integración.

   El Sistema de Gestión de Seguridad y Salud Ocupacional tiene su base en el Plan General de Fonación, Capacitación y Entrenamiento.

   El trabajo de Monitoreo y Medición es muy importante en el control de la Gestión.

   Las constantes Auditorías Internas programadas son nuestros indicadores de desempeño inmediatos.

   Estos requerimientos de la norma OHSAS 18001 son verdaderas herramientas de Gestión, que ayuda enormemente a ordenar un sistema normal de dirección de seguridad el cual podrá auditarse y certificar por un organismo externo dejando clara evidencia de la gestión y mejoramiento de la calidad ambiental.

### 2.1.2. Antecedentes Internacionales.

a) **GONZALES (2014),** en su tesis para optar el Título de Administrador en Seguridad y Salud Ocupacional, de la Universidad Militar Nueva Granada, Bogotá, Titulada: "*El riesgo y la falta de Políticas de Seguridad Informática una amenaza en las Empresas Certificadas BASC*", conclusiones:

La implementación de políticas de seguridad informática en una organización es una solución que no sólo busca proteger, preservar y administrar de una manera eficiente todo tipo de recursos con los que cuenta una organización, sino que también busca dar solución, prevenir, evitar, controlar y minimizar los daños de incidentes que afectan a la organización es por esto que preparar y capacitar al personal en temas asociados a la seguridad informática y cómo hacer frente a incidentes que se llegarán a presentar con el fin de responder de una manera adecuada es una de las principales metas de esta estrategia. Capacitar al personal de la compañía es primordial debido a que éste puede tomar un papel activo dentro de la organización de manera que aplique este conocimiento en las diversas actividades que realiza dentro y fuera de la organización con el propósito de proteger de una forma adecuada la información que se le confía, así como la propia.

**b) MACEN (2014),** en su tesis para optar el Título de Master en Auditoria y Sistemas de la Información, de la Universidad Tecnológica Internacional, Paraguay, Titulada: "*Políticas de Seguridad de la Información*", conclusiones:

El autor realiza una investigación sobre las políticas de seguridad de la información para área Departamento de Tecnología Informática cuyo objetivo fue la de describir la realidad que presentaba en ese momento la UTIC, respecto a lo mencionado propuso la construcción de una política de seguridad de la información en la Sedes de la Regional Central, para ellos, realizo las coordinaciones con los funcionarios para que aporten en la investigación, para ello se tuvo en cuenta diferentes puntos. Considerando como principales plantear el problema general y los objetivos específicos. Consecuencia de ello se obtuvieron resultados:

Después de Recopilar y analizar la información de la seguridad de la información en la UTIC, donde el autor sostiene proponer un plan

de políticas de seguridad para la información resulto favorable y arrojo pun porcentaje considerado dentro de lo establecido según las cifras que se solicitaron.

c) **PERAFÁN y CAICEDO (2014),** en su tesis para optar el Título de Especialista en Seguridad Informática, de la Universidad Nacional Abierta a Distancia Escuela de Ciencias Básicas Tecnológicas e Ingeniería Especialización en Seguridad Informática, Popayán, Titulada: "*Análisis de riesgos de la seguridad para la Institución Universitaria Colegio Mayor del Cauca*", conclusiones:

   Finalizado el proyecto se logra alcanzar todos los objetivos planteados; los controles generados permiten mejorar y normalizar los procesos de la IUCMC aplicando los conceptos de seguridad de la información. Aplicar la metodología MAGERIT para el análisis de riesgo es el primer paso para garantizar la seguridad de los activos de información y el normal funcionamiento interno de la IUCMC. El análisis de riesgo aplicado, permite conocer de manera global el estado actual de la seguridad informática dentro de la IUCMC. Los controles y políticas de seguridad de la información resultado de este análisis de riesgos pueden ser tomados como soporte para la implementación del SGSI; encaminado a: Reducir el ambiente de riesgo vigente. Disponer de las medidas de control interno necesarias. Disminuir el grado de exposición de los sistemas que se procesan. Incrementar la confiabilidad, integridad y disponibilidad de la información. Optimizar los procesos orientados al cumplimiento de los objetivos de la Institución. Conseguir disminuir el riesgo actual a su nivel mínimo. La IUCMC actualmente presenta un nivel de riesgo informático considerable, que con el apoyo de las directivas (alta gerencia) y de todo el personal es posible contrarrestar.

d) **VITERI (2014),** en su tesis para optar el Título de Ingeniero de Sistemas, de la Universidad Técnica Estatal de Quevedo, Ecuador,

Titulada: "*Políticas de seguridad informática en el departamento de tecnologías de la información y comunicación en beneficio de la Universidad Técnica Estatal de Quevedo. Manual de Procedimientos 2014*", conclusiones:

- Se efectuó un análisis de riesgos informáticos mediante encuestas a todo el personal de la Unidad de TIC's, para valorar los activos y así adecuar las políticas a la realidad de la institución.
- Gracias a la definición de políticas se pudo concluir (CIUDAD GAYOSO, 2012) que las conexiones a Internet deben contar con elementos de prevención, detección de intrusos, filtros contra virus, manejo de contenidos, los mismos que afectan la integridad de los sistemas y la información institucional.
- Los usuarios no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el departamento de TIC's.
- Se pudo definir que el departamento de TIC's diseñará los mecanismos necesarios para administrar acceso a los servicios de la red institucional de la UTEQ.

**e) GARZÓN (2015),** en su tesis para optar el Título Profesional de Ingeniero de Sistemas, de la Universidad Distrital Francisco José de Caldas, Bogotá D.C., Titulada: "*Creación, implementación y evaluación de la política de seguridad de base de datos para los ambientes de producción del Instituto Colombiano para la evaluación de la educación* "ICFEES", conclusiones:

- Para facilitar la actualización y mantenimiento de cualquier política de seguridad es necesario diferenciar claramente las políticas de las normas estándares y procedimientos en su definición.
- Las políticas de seguridad pueden apoyarse en herramientas tecnológicas sin embargo las definiciones de la política debe ser independientes de ellas.

- El uso de firewalls dedicados como IMPERVA Secure Sphere Database, permite implementar controles de seguridad adicionales a las bases de datos ayudando a mitigar las amenazas y vulnerabilidades a las que se encuentra expuesta.
- La identificación de los activos de información relacionados con la base de datos y su correcta clasificación, permite una más fácil identificación de las amenazas y vulnerabilidades que los afectan.
- Se deben incluir en las políticas de seguridad las definiciones específicas a las que hace referencia para evitar ambigüedades y confusiones para los responsables del cumplimiento.
- La concientización del personal de una organización sobre la importancia de la seguridad de la información es fundamental para reducir los incidentes relacionados con ella.

**f) QUIRUMBA (2015),** en su tesis para optar el Título de Magister en Seguridad Informática Aplicada, de la Escuela Superior Politécnica del Litoral, Guayaquil, Titulada: "*Desarrollo del esquema de seguridad, plan de recuperación ante desastres informáticos y solución para el nivel de exposición de amenazas y vulnerabilidades aplicada a los servidores y equipos de comunicación del centro de datos de la Municipalidad de la ciudad del Este*", conclusiones:

- Aplicar análisis de vulnerabilidades periódicas a la infraestructura Tecnológica del Centro de Procesamiento de Datos Municipal, principalmente a los servicios que se encuentran expuestas al Internet.
- Gestionar la pronta adquisición de Servidores de Datos más robustos, que permitan agilitar los servicios brindados por el Municipio, mejorando la atención al contribuyente y usuario en común.

- Monitorear de forma continua a través de analizadores de tráfico o sistemas de detección de intrusos (IDS), para que sirva de alerta ante cualquier intrusión o problemas de ataque que se quiera ejecutar en los servidores de datos de la Institución.
- Segmentación Física y Lógica de la Red LAN, con el objetivo de aislar el tráfico en fragmentos optimizando de manera eficiente los recursos de la institución. Además, se logra identificar que luego de realizar el proceso de Ethical Hacking a cada uno de los Servidores de Datos de la Institución, este permitió identificar muchas deficiencias y debilidades que poseían estos xxviii equipos, logrando de esta manera la eliminación de vulnerabilidades a través de la correcta configuración y actualización de software.

Finalmente se ha considerado la implementación de estándares que permitan desarrollar el plan de recuperación ante desastres y respaldos, basados en las necesidades y servicios que brinda el Municipio, para lograr de esta manera mantener siempre la continuidad operativa de la Institución evitando posibles problemas al momento de ocurrir algún percance o incidente Tecnológico; así como también la aplicación y socialización de la política de seguridad que esté acorde a las necesidades de las Entidades Públicas actuales permitiendo penalizar al empleado por el mal uso de los recursos Municipales.

**g) GARCÉS (2015),** en su tesis para optar el Título de Ingeniero en Sistemas Computacionales e Informáticos, de la Universidad Técnica de Ambato, Ecuador, Titulada: "*Seguridad informática para la red de datos en la Cooperativa de Ahorro y Crédito Unión Popular LTDA*", conclusiones:

Tener conocimientos acerca de metodologías y mecanismos de seguridad informática es necesario ya que la tecnología de las comunicaciones avanza y la información que se transmite por los diferentes canales de comunicación son de gran importancia para

sus propietarios por lo que es necesario resguardarla adecuadamente. La instalación de recursos de seguridad informática sean estos hardware o software son de vital importancia para cualquier tipo de organización, ya que estos son barreras de protección para su recurso informático.

Una adecuada planificación para recolectar información acerca de los activos, se la realiza en base a metodologías que ayudarán en reconocer la importancia de cada uno de los activos para la comunicación. Existen varias herramientas que nos permiten monitorear los eventos que se producen dentro de una red, estos nos presentan información relevante para conocer que puertos son utilizados, además conocer los hosts interconectados y reconocer a posibles intrusos.

El análisis de riesgos y vulnerabilidades con base a NIST 800-30, en el cual se definieron los activos, amenazas y vulnerabilidades son un punto inicial para la implementación de una adecuada seguridad informática para la red de datos. Se deben definir y documentar las reglas y derechos de acceso a los recursos del sistema de información y comunicación para cada usuario o grupo de usuarios en una declaración de política de accesos.

Es muy útil implementar un servidor de dominio que tenga la función además de active directory ya que este permite un control adecuado de todos los usuarios de una organización permitiendo de esta manera restringir y otorgar permisos necesarios de acuerdo a las funciones de los usuarios. Una correcta configuración de mecanismos software como servidores proxy, firewall e IDs son fundamentales para brindar seguridad básica a una organización, ya que estos brindan control de contenido, denegación de puertos innecesarios y además nos permiten el monitoreo de paquetes dentro de la red.

Una de las bases fundamentales es el apoyo de la alta gerencia, ya que se requiere un cambio de cultura y concientización hace necesario el impulso constante de la Dirección. La seguridad de la

información no se debe considerar como un aspecto solo tecnológico sino de tipo organizacional y de gestión, es decir organizar la seguridad de la información e implementar la seguridad en base a los requerimientos de la empresa.

**h) MUÑOZ (2016),** en su tesis para optar el Título de Magister en Gestión Estratégica de Tecnologías de Información, de la Universidad de Cuenca, Ecuador, Titulada: "*Diseño de Políticas de Seguridad Informática para la Dirección de Tecnologías de la Información y Comunicación (DTIC*)", conclusiones:

Como se indicó en el alcance del presente trabajo de tesis, se estableció unas políticas de seguridad informática más relevantes para la DTIC basado en el análisis de la información proporcionada por los funcionarios que allí laboran, se pudo identificar algunos controles que no se aplican por la naturaleza de la Universidad de Cuenca, como, por ejemplo: Servicios de Comercio Electrónico.

Además, recordamos que la norma ISO 27002 está diseñada para aplicarla en cualquier tipo de empresa de cualquier magnitud, donde va a depender de los objetivos, modelo de negocio, metas, naturaleza de cada una de las empresas en aplicar o no cierto control de seguridad informática, por ese motivo el porcentaje de cumplimiento total estimado para la DTIC no sería del 100%.

Se tiene la confianza que la implementación de las políticas de seguridad informática definidas en el presente documento va ayudar en primer lugar a la concientización de todos los funcionarios que laboran en la DTIC, ya que el incumplimiento de alguna política de seguridad informática puede poner en riesgo a la información, equipos informáticos de toda la comunidad Universitaria. En segundo lugar se va a conseguir un mejoramiento sustancial en aquellos puntos débiles de la seguridad informática que tiene actualmente la DTIC, como por ejemplo se conseguirá un fortalecimiento en la seguridad de los sistemas informáticos institucionales, en los equipos informáticos y en los equipos de

comunicación que administran los funcionarios de la DTIC, también se dispondrá de documentación técnica y de adiestramiento actualizado, se elaborará y se realizará revisiones periódicas de los planes de contingencia.

## 2.2. Bases Teóricas

### 2.2.1 Políticas de seguridad de la información

Una Política de seguridad de información es un lineamiento o reglas aplicada a las acciones afines a la administración de la información de un ente, con el fin de resguardar la información, los recursos y la ética de la misma.

Implementar políticas de seguridad para un ambiente de contenido de datos que se manejan informaciones sensibles, es necesario considerar lineamientos y políticas para el resguardo de la información, debido a que existen ataques informáticos de diferentes factores, por ello es necesario considerar medidas de seguridad para la protección de datos de los recursos que son activos importantes del negocio.

### 2.2.2 Cumplimiento Obligatorio

Para el aplicar las políticas y lineamientos de seguridad para la protección de la información es necesario realizar talleres de sensibilización al personal involucrado, de esa manera el personal tome en cuenta los riesgos que existen, respecto a la información sensible que se maneja y así puedan utilizar de forma obligatoria el uso correcto de la información y debe ser considerado como una condición en los contratos del personal.

### 2.2.3 Organización de la Seguridad

Definir roles y responsabilidades respecto a la protección de recursos de información. Donde se fijarán lineamientos para cada perfil y rol según corresponda en sus funciones, de los cuales lo colaboradores deben cumplir con el rol y la administración de la

seguridad de la información. Todos los empleados son responsables de mantener un ambiente seguro, en tanto que el área de seguridad informática debe monitorear el cumplimiento de la política de seguridad definida y realizar las actualizaciones que sean necesarias, producto de los cambios en el entorno informático y las necesidades del negocio.

### 2.2.4 Estructura Organizacional

Para el cumplimiento de sus fines y objetivos, el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME tiene la siguiente organización:

a. Consejo Directivo
b. Comité de Vigilancia y Supervisión
c. Dirección Ejecutiva
d. Órganos de Apoyo
e. Órganos de Asesoramiento
f. Órganos de Ejecución.

**Organización del ORES-FOVIME**

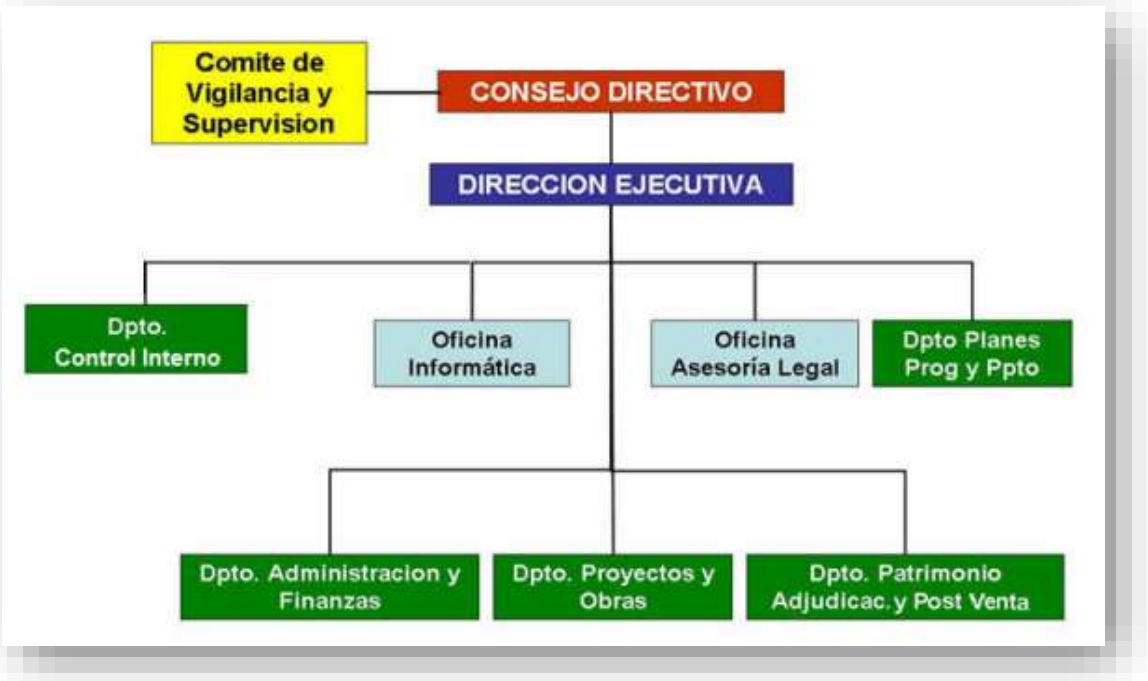



**Figura 4.** Elaboración propia

### 2.2.5 Base de Datos

Conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido; una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta. Actualmente, y debido al desarrollo tecnológico de campos como la informática y la electrónica, la mayoría de las bases de datos están en formato digital, siendo este un componente electrónico, por tanto, se ha desarrollado y se ofrece un amplio rango de soluciones al problema del almacenamiento de datos.

### 2.2.6 Base de Datos OSSAB

Es el almacén de la información de uso diario para prácticamente todo. Almacenan datos del personal militar, aportes del personal militar, estados de cuenta del personal militar, créditos hipotecarios, préstamos del personal militar entre otros, por lo que está claro que son una pieza clave y jugosa para cualquier atacante, ante la que cualquier medida de protección es poca. Esto no sería un gran problema si nuestras bases de datos se encontraran guardadas en una caja de seguridad en un lugar desconocido, pero entonces tampoco serían muy útiles. Las bases de datos forman parte de los aplicativos por áreas desde el cual se permite el acceso a la información que contienen a ciertos usuarios que son controlados los permisos y accesos por el administrador de la Base de Datos OSSAB del ORES-FOVIME.

Esta solución consiste en instalar dos dispositivos entre los servidores de datos y el switch que comunica los servidores con la red. El primer dispositivo es una puerta de enlace (Gateway X2500) donde se realiza el monitoreo de la base de datos y el segundo es un dispositivo de administración centralizada. (Appliance M150 MX). El cual cuenta con dos interfaces de manejo, de las cuales una de ellas está dispuesta para la administración de la plataforma en la red

LAN y la otra interfaz se utiliza para el intercambio de gran cantidad de información de auditoría y control entre los dispositivos. Estos dispositivos han sido instalados en modo puente (Bridge mode), como se observa en la ilustración 3; Todo el tráfico pasa a través del gateway, el cual lo monitorea y bloquea las conexiones maliciosas descartando paquetes (Dropping) (Ormella 2015).

### 2.2.7 Usuarios

Actualmente los usuarios, tienen acceso a diferentes aplicaciones que se conectan a la base de datos de producción, Cada usuario debe ser responsable de su usuario y contraseña que se le asigne para realizar sus funciones a través del software para el acceso a datos del ambiente de producción OSSAB del ORES-FOVIME, de acuerdo a las políticas definidas, los datos mencionados deben ser únicos e intransferibles a otro usuario, para el acceso a las soluciones informáticas, considerando que hay un personal responsable que controla, monitorea y revisa el ingreso y salida del sistema de los usuarios que acceden.. Los terminales y computadoras personales deben bloquearse luego de quince (15) minutos de inactividad. El usuario tendrá que autenticarse antes de reanudar su actividad. El usuario debe ser instruido en el uso correcto de las características de seguridad del terminal y funciones de todas las plataformas, estaciones de trabajo, terminales, computadoras personales, etc., y debe cerrar la sesión o bloquear la estación de trabajo cuando se encuentre desatendida.

### 2.2.8 La información como activos importantes

La información es gran importancia para la entidad, debido a que contiene información relevante y sensible del core del negocio y de sistemas administrativos que es esencial para el personal responsable, en consecuencia, necesita ser protegido adecuadamente. Para ello se debe tener claro las políticas definidas, considerando todos los criterios necesarios para el uso adecuado de

la conexión a datos. De lo contrario como resultado de esta creciente interconectividad, la información podría estar expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades. La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida. (p.8)

### 2.2.9 Protección de datos y privacidad de la información

Se debiera asegurar la protección y privacidad de la data conforme lo requiera la legislación, regulaciones y, si fuesen aplicables, las cláusulas contractuales relevantes. La responsabilidad por el manejo de la información personal y el reforzamiento del conocimiento de los principios de protección de data debieran ser tratados en concordancia con la legislación y las regulaciones relevantes. Se debieran implementar las apropiadas medidas técnicas y organizacionales para protección la información personal. (p.155)

### 2.2.10 Acuerdos de confidencialidad o no-divulgación de las informaciones

Los acuerdos de confidencialidad o no-divulgación debieran tener en cuenta el requerimiento de proteger la información confidencial utilizando términos legalmente ejecutables. Para identificar los requerimientos de los acuerdos de confidencialidad o no-divulgación, se debieran considerar los siguientes elementos:

- una definición de la información a protegerse (por ejemplo, información confidencial);
- duración esperada de un acuerdo, incluyendo casos donde se podría necesitar mantener la confidencialidad indefinidamente;

- acciones requeridas cuando se termina un acuerdo;
- responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada (tal como “sólo lo que necesita saber”);
- propiedad de la información, secretos comerciales y propiedad intelectual, y cómo se relaciona esto con la protección de la información confidencial;
- uso permitido de la información confidencial, y los derechos del firmante para utilizar la información;
- proceso de notificación y reporte de divulgación no autorizada o incumplimiento del acuerdo de información confidencial; condiciones para el retorno o destrucción de la información una vez que se termina el acuerdo; y acciones esperadas a realizarse en caso de incumplimiento de este acuerdo. (Ibíd.)

### 2.2.11 Definición de términos básicos

Para Veyrat (2014), la adopción de medidas técnicas tendientes a garantizar la seguridad de los datos las empresas que traten, almacenen y accedan a datos; medidas que deberán adoptarse en función del nivel de los datos almacenados/tratados, de la estructura y organización de la Empresa y del estado de la tecnología. Los casos de incidentes informáticos que en el pasado causaron daños y perjuicios económicos importantes, han ido abriendo los ojos a muchas empresas a la necesidad de implantar mecanismos para proteger su información almacenada y tratada en los equipos informáticos de incidencias externas (intencionadas y/o accidentales); pero también, de la importancia de la protección de la información desde una órbita interna que representan los aspectos técnicos del manejo de las informaciones en la empresa.(p 5).

### 2.2.12 Gestión de las claves secretas de los usuarios

Las claves secretas son un medio común para verificar la identidad del usuario antes de otorgar acceso a un sistema o servicio de

información en concordancia con la autorización del usuario. Están disponibles, y se debiera considerar la idoneidad, de otras tecnologías para la identificación y autenticación del usuario; tales como biométricas, por ejemplo, verificación de huellas digitales, verificación de firmas; y el uso de dispositivos de hardware como tarjetas inteligentes. (p. 98-99)

### 2.2.13 Restricción del acceso a la información

El acceso de los usuarios y el personal de soporte a la información y las funciones del sistema de la aplicación debiera limitarse en concordancia con la política de control de acceso definida. Las restricciones para el acceso se debieran basar en los requerimientos de las aplicaciones comerciales individuales. La política de control de acceso también debiera ser consistente con la política de acceso organizacional (p.115).

### 2.2.14 Calidad

Según Camisón, Cruz y Gonzáles (2006, p.149), indican que:

El concepto se aplica para describir los productos con los máximos estándares de calidad en todas sus características. Este concepto de calidad tiene su importancia por incidir en la trascendencia de la calidad de diseño, que marca el grado de excelencia del producto. La expresión «producto de calidad» sería entonces equivalente a la de producto con la mejor calidad de diseño posible. El lujo o su ausencia se traducen en especificaciones concretas tales como alfombras de piel o tapetes de hule, cuadros de primeras firmas o cuadros que son reproducciones baratas.

### 2.2.15 Control de acceso a datos

El personal responsable debe ser precavido y cuidadoso con la información que se les asigna a sus funciones, entre ellos el usuario y contraseña que es de uso único e intransferible para el acceso al sistema de información, considerando todos los factores

involucrados que conllevan a proteger adecuadamente la seguridad de la información que se almacena en los servidores de base de datos contra modificaciones no autorizadas, divulgación o destrucción. El uso de las normas, políticas y lineamientos definidos para el acceso a datos, previene errores o negligencias de los colaboradores, así como reduce la posibilidad del acceso no autorizado.

### 2.2.16 Identificación de usuarios

Respecto a este punto cada colaborador que acceda a una solución de software debe de ser identificado de manera única, para realizar su actividad en los sistemas de producción y debe de ser controlado, monitoreado y revisado. Seguidamente cada usuario que tenga el acceso al sistema debe tener en claro las políticas de protección a la información y adicional a ello también debe firmar un compromiso de cumplimiento a las políticas.

El usuario debe ser instruido en el uso correcto de las características de seguridad del terminal y funciones de todas las plataformas, estaciones de trabajo, terminales, computadoras personales, etc., y debe cerrar la sesión o bloquear la estación de trabajo cuando se encuentre desatendida.

### 2.2.17 Seguridad de contraseña

Es importante que todos los colaboradores de la entidad y que tengan acceso a los sistemas informáticos, es necesario que firmen un compromiso de confidencialidad de la información, para que de esa manera la entidad y la información puedan estar respaldados. También es necesario que los colaboradores protejan sus contraseñas, debiendo seguir las siguientes regulaciones:

- Bajo ninguna circunstancia, se debe escribir las contraseñas en papel, o almacenarlas en medios digitales no encriptados.
- Las contraseñas no deben ser divulgadas a ningún otro usuario salvo bajo el pedido de un gerente, con autorización del área de

seguridad informática y auditoría interna. Si se divulga la contraseña, esta debe ser cambiada durante el próximo ingreso.

- El usuario autorizado es responsable de todas las acciones realizadas por alguna persona a quién se le ha comunicado la contraseña o identificador de usuario.

### 2.2.18 Controles de acceso de programas

Los colaboradores de cada entidad, deben regiré a lo establecido en el compromiso sostenido con la entidad para no tener inconvenientes, es así que al momento de utilizar o acceder a los programas, lo cual debe estar establecido en las políticas de seguridad de los equipos donde se almacenan la información (servidores de prueba, calidad y producción) lo cual deben poder generar una pista de auditoria de todos los accesos y violaciones. Las violaciones de los controles de acceso deben ser registradas y revisadas por el propietario o por el personal del área de sistemas custodio de los datos. Las violaciones de seguridad deben ser reportadas al responsable de la entidad y al área responsable de la administración de la seguridad de la información. Se debe tener cuidado particular en todos los ambientes para asegurar que ninguna persona tenga control absoluto. Los operadores de sistemas, por ejemplo, no deben tener acceso ilimitado a los identificadores de súper usuario. Dichos identificadores de usuario, son solo necesarios durante una emergencia y deben ser cuidadosamente controlados por la gerencia usuaria, quien debe realizar un monitoreo periódico de su utilización.

### 2.2.19 Administración de acceso de usuarios

Respecto a este punto, es necesario que los responsables de la administración y asignación de usuarios en especial o privilegiado (como cuentas administrativas y supervisores) deben tener un seguimiento de control y monitoreo, adicional a ello deben ser revisadas cada 3 meses, para realizar el cambio de contraseña. Los

propietarios de la información son responsables de revisar los privilegios de los sistemas periódicamente y de retirar todos aquellos que ya no sean requeridos por los usuarios. Es recomendable realizar revisiones trimestralmente debido al continuo cambio de los ambientes de trabajo y la importancia de los datos que se almacenan en los servidores de producción, calidad y pruebas. Es responsabilidad del propietario de la información y de los administradores de sistemas ver que los privilegios de acceso estén alineados con las necesidades del negocio, sean asignados basándose en requerimientos y que se comunique la lista correcta de accesos al área de sistemas de información.

### 2.2.20 Políticas de seguridad de la información

Las políticas de seguridad de la información son lineamientos plasmados en un documento de alto nivel (nivel estratégico) donde se definen las directrices a seguir para la conexión a la base de datos del ambiente de producción en concreto para garantizar la confidencialidad, integridad y disponibilidad de la información.

Es decir, estos documentos deben ser elaborados, revisados y mantenidos por el consejo directivo (preferiblemente) o la máxima autoridad de la organización, dependiendo de cómo funcione la misma; la formulación de las políticas de seguridad para la información son lineamientos establecidos en coordinación con los directivos involucrados, para definir los accesos, perfiles y roles de cada usuario y en función a ello poder clasificar una gestión estratégica, que involucre a todos los usuarios que acceden a dicha información, así como también proteger la información de usuarios no autorizados. Las políticas de seguridad desarrolladas son importantes para un ambiente de producción, calidad y desarrollo, debido a que se maneja información sencilla en su mayoría y son activos principales en las entidades públicas y privadas.

En consecuencia, a ello, según el autor que se describe menciona lo siguiente: “La intención es generar y/o confirmar el compromiso

de la alta gerencia (de allí la importancia de la participación del consejo directivo) en materia de seguridad de la información. (Solís, 2014)" .

También el siguiente autor: "Navarro (2003) considera que las políticas son directrices u orientaciones sobre una determinada materia en un entorno concreto. Se trata de fijar objetivos sin decir cómo conseguirlos y viene a representar el marco o filosofía de actuación de la entidad. No deben ser largas ni farragosas, una o dos páginas por política, a lo sumo. Tienen que ser fáciles de entender por todo el personal de la empresa. (p. 57)".

### 2.2.21 Elaboración de la política

La elaboración de la política de seguridad para la información, se diseñó, considerando todos los artículos y normas al que se rige cada plan, siendo las siguientes leyes al que rige:

Ley Nª 30096 "Ley de Delitos Informáticos"

LEY DE DELITOS INFORMÁTICOS CAPÍTULO I FINALIDAD Y OBJETO DE LA LEY Artículo 1. Objeto de la Ley La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia. CAPÍTULO II DELITOS CONTRA DATOS Y SISTEMAS INFORMÁTICOS Artículo 2. Acceso ilícito El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa. Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado. Artículo modificado por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente: "Artículo 2. Acceso

ilícito El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado." Artículo 3. Atentado contra la integridad de datos informáticos El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa. Artículo modificado por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente: "Artículo 3. Atentado a la integridad de datos informáticos El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa." Artículo 4. Atentado contra la integridad de sistemas informáticos El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa. Artículo modificado por el Artículo 1 de la Ley N° 30171, publicada el 10 marzo 2014, cuyo texto es el siguiente: "Artículo 4. Atentado a la integridad de sistemas informáticos El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa."

# III. METODOS Y MATERIALES

## 3.1. Hipótesis de la investigación

### 3.1.1. Hipótesis general

La propuesta de una política de seguridad influye positivamente en la base de datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME.

### 3.1.2. Hipótesis especifica

a) La revisión de la configuración protege a la base de datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME.
b) Las pruebas de penetración protegen a la base de datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME.

## 3.2. Variables de estudio

### 3.2.1. Definición conceptual

**a) Política de seguridad**

- **Identificar y evaluar los activos:** Qué activos deben protegerse y cómo protegerlos de forma que permitan la prosperidad de la empresa.
- **Identificar las amenazas:** ¿Cuáles son las causas de los potenciales problemas de seguridad? Considere la posibilidad de violaciones a la seguridad y el impacto que tendrían si ocurrieran. Estas amenazas son externas o internas:
- **Amenazas externas:** Se originan fuera de la organización y son los virus, gusanos, caballos de Troya, intentos de ataques de los hackers, retaliaciones de ex-empleados o espionaje industrial.
- **Amenazas internas:** Son las amenazas que provienen del interior de la empresa y que pueden ser muy costosas porque el infractor tiene mayor acceso y perspicacia para saber dónde reside la información sensible e importante.

- **Evaluar los riesgos**: Éste puede ser uno de los componentes más desafiantes del desarrollo de una política de seguridad. Debe calcularse la probabilidad de que ocurran ciertos sucesos y determinar cuáles tiene el potencial para causar mucho daño. El costo puede ser más que monetario - se debe asignar un valor a la pérdida de datos, la privacidad, responsabilidad legal, atención pública indeseada, la pérdida de clientes o de la confianza de los inversionistas y los costos asociados con las soluciones para las violaciones a la seguridad.
- **Asignar las responsabilidades:** Seleccione un equipo de desarrollo que ayude a identificar las amenazas potenciales en todas las áreas de la empresa. Sería ideal la participación de un representante por cada departamento de la compañía. Los principales integrantes del equipo serían el administrador de redes, un asesor jurídico, un ejecutivo superior y representantes de los departamentos de Recursos Humanos y Relaciones Públicas.
- **Establecer políticas de seguridad**: Cree una política que apunte a los documentos asociados; parámetros y procedimientos, normas, así como los contratos de empleados. Estos documentos deben tener información específica relacionada con las plataformas informáticas, las plataformas tecnológicas, las responsabilidades del usuario y la estructura organizacional. De esta forma, si se hacen cambios futuros, es más fácil cambiar los documentos subyacentes que la política en sí misma.
- **Implementar una política de seguridad para el ambiente productivo OSSAB de la organización**: La política que se escoja debe establecer claramente las responsabilidades en cuanto a la seguridad y reconocer quién es el propietario de los sistemas y datos específicos. También puede requerir que todos los empleados firmen la declaración; si la firman, debe comunicarse claramente. Éstas son las tres partes esenciales de cumplimiento que debe incluir la política.

- **Cumplimiento**: Indique un procedimiento para garantizar el cumplimiento y las consecuencias potenciales por incumplimiento.
- **Funcionarios de seguridad**: Nombre individuos que sean directamente responsables de la seguridad de la información. Asegúrese de que no es la misma persona que supervisa, implementa o revisa la seguridad para que no haya conflicto de intereses.
- **Financiación**: Asegúrese de que a cada departamento se le haya asignado los fondos necesarios para poder cumplir adecuadamente con la política de seguridad de la compañía.
- **Administre el programa de seguridad**: Establezca los procedimientos internos para implementar estos requerimientos y hacer obligatorio su cumplimiento.

### 3.2.1. Definición Operacional

La definición operacional se reporta en la tabla siguiente.

**Tabla 1:** *Definición operacional*

| Variable | Dimensión | Unidades |
|---|---|---|
| **Independiente** La implementación de una política de seguridad | Información | Datos |
| **Dependiente** Base de datos | Productividad | Numero de políticas exitosas |

## 3.3. Tipo de Investigación

El tipo de investigación es cuantitativa, se trata de una investigación explicativa, debido a que se buscará demostrar el resguardo de la información (política de seguridad) que viene

hacer la (variable independiente), causará productividad en el resguardo de la información (variable dependiente).

Tal como lo afirma Méndez (2011, p.134) el propósito de formular el tipo de investigación, es que "... el instigador señale el tipo de información que necesita, así como el nivel de análisis que deberá realizar, tomando en cuenta los objetivos y las hipótesis planteadas anteriormente.

Al respecto el mismo autor (ob.cit.: 2001, p.134), señala que un estudio de tipo descriptivo". Es la delimitación de los hechos que conforman el problema de investigación de la información, como la observación, las entrevistas y los cuestionarios", en vista de ello, la investigación considero ajustarse a los lineamientos de un estudio de **tipo explicativa**, pues se explicó el implementar una política de seguridad que suceden con una política se seguridad y el resguardo de la información de la base de datos del ambiente productivo OSSAB en el ORES-FOVIME.

### 3.3.1. Nivel de Investigación.

**Descriptivo:** Se describió las políticas de seguridad de la información, para el ORES-FOVIME.

Las acciones realizadas para el desarrollo de investigación fueron a través de un enfoque **metodológico cuantitativo** (Hernández, 2006), es decir se describió Una cadena de su influencia en la seguridad de la información que almacena el ambiente productivo OSSAB en la empresa ORES-FOVIME., y a partir de las teorías existentes de los factores que generan y resguardo de la información; se estableció un tratamiento de los datos recolectados para finalmente derivar la propuesta del modelo.

Bunge, (1999) El método que guio el proceso de investigación fue el cuantitativo a través de un razonamiento deductivo que consistió en:

- La elección del campo de investigación o directo: Es de campo porque se realizó en el ambiente en el que se desarrollan las actividades de las personas consultadas quienes proporcionarán los datos relevantes que serán analizados.
- Revisión previa de investigaciones que han tratado el tema de Política de seguridad y su influencia en la seguridad de la información.

## 3.4. Diseño de la investigación

El diseño de la investigación que se aplicó, es el diseño cuasi experimental que consta dos grupos muestrales.

Se utilizará el diseño cuasi experimental con pre y post test con un solo grupo, con prueba de entrada y prueba de salida.

El esquema es:

Ge: $O_1$ X $O_2$

Gc: $O_3$ - $O_4$

Donde:

Ge: Grupo experimental

Gc: Grupo Control

$O_1$ y $O_3$: Prueba de entrada (pre prueba o Pretest)

$O_2$ y $O_4$: Prueba de salida (pos prueba o Pos test)

X: Estímulo (aplicativo)

## 3.5. Población y Muestra del estudio

### 3.5.1. Población

La población se compuso de los funcionarios del Organismo Especial del Fondo de Vivienda Militar del Ejército (ORES-FOVIME) de los cuales pretendemos indagar y conocer sus características o una de ellas, y para el cual serán válidas las conclusiones obtenidas en la investigación.

1 (un) Director de Tecnología Informática

3 (tres) Analistas Programadores

2 (dos) Administradores de Base de Datos

3 (tres) Encargados de Telecomunicaciones

También se aplicó un cuestionario a los funcionarios del ORES FOVIME que manejan sistemas de informaciones, de las siguientes Departamentos:

- Departamento de Control Interno (04 funcionarios)
- Departamento de Planes y Presupuesto (03 funcionarios)
- Departamento de Administración y Finanzas (06 funcionarios)
- Departamento de Proyectos y Obras (02 funcionarios)
- Oficina de Informática (06 funcionarios)
- Oficina de Asesoría Legal (02 funcionarios)

### 3.5.2. Muestra

Según Arias (1998, p.52) la población es “el conjunto de elementos, seres o eventos, concordantes entre sí en cuanto a una serie de características, de la cuales se puede obtener alguna información”. Es por ello que en esta investigación se trabajó con una población conformada por una empresa inmobiliaria de viviendas para el personal militar del Ejército ubicada en Av. Los Álamos s/n Conjunto Residencial "Héroes de San Juan y Miraflores" Altura KM 13.5 Carretera Panamericana Sur (Frente al Puente Alipio Ponce) .- SJM, con una sucursal - en Av. Boulevard s/n Pentagonito Of. ORES- FOVIME, los sujetos informantes son 30 personas de esta empresa; 3 representantes legales de la empresa, 1 Director General de la empresa y 21 trabajadores relacionados al área de Finanzas, contabilidad, Logística, Obras y Presupuestos, almacén y Sección de Telemática de la empresa.

## 3.6. Técnicas e Instrumentos de recolección de datos

### 3.6.1. Técnicas de recolección de datos

A los funcionarios de los departamentos y oficinas del ORES – FOVIME se les entrego un cuestionario, cuyos contenidos fueron

expresados en preguntas que se extrajeron de las dimensiones. Es decir, de sus indicadores: Lista de cotejo, Pre y Pos test

Para Méndez (2001, p. 152), las técnicas “Son hechos o documentos a los que acude el investigador y que le permiten obtener información. Las técnicas son los medios empleados para recolectar la información”

En la investigación la técnica que se utilizo fue la encuentra, método de investigación que permite requerir datos a un grupo de personas que están involucradas con el tema de estudio y que nos permitirán acceder a la información desde la fuente primaria y directa”. En este sentido y tomado en cuenta el tipo de técnica a aplicar en la investigación se aplicó un cuestionario compuesto por 25 preguntas cerradas y se-abiertas a los Representantes Legales. Director General y empleados relacionados con la administración de la Base de Datos del ambiente productivo OSSAB en la empresa ORES-FOVIME.

### 3.6.2. Instrumentos de recolección de datos

Estadística descriptiva, inferencial

Software SPSS versión 22 – Star Graphis 2016

#### 3.6.2.1. Confiabilidad del Instrumento

**Tabla 2: Estadísticos de Fiabilidad**

| Alfa de Cronbach | Alfa de Cronbach basada en los elementos tipificados | N° de elementos |
|---|---|---|
| 89.97% | 90,05% | |

**Fuente: Elaboración propia en SPSS**

El resultado de confiabilidad es alto 89,97% por tanto tú instrumento ha tenido buena consistencia interna. Mide la

consistencia interna del diseño del instrumento (Preguntas de la encuesta). Esta expresada en términos relativos a media que se acerca a la unidad el instrumento será más consistente y confiable y si se acerca a 0.50 entonces la consistencia interna del cuestionario seria débil y poco fiable en la investigación

- ✓ **La Encuesta.**

  Según Arratia García, Galisteo Gonzáles, Pérez Rodríguez, & García Arista (2009) Una encuesta es un conjunto de preguntas tipificadas dirigidas a una muestra representativa para averiguar estados de opinión o diversas cuestiones de hecho que abarca preguntas sobre la información de la base de datos del ambiente productico OSSAB y su influencia en la seguridad de la información en la Empresa ORES - FOVIME con el objetivo de obtener la información correspondiente para aplicar en los resultados.

- ✓ **El cuestionario.**

  Según Hurtado De Barrera, J. (2000:469) un cuestionario es un instrumento que agrupa una serie de preguntas relativas a un evento, situación o temática particular, sobre el cual el investigador desea obtener información. Son preguntas de cinco opciones en un formato de escala Likert que consiste en un conjunto de ítems presentados en forma de afirmaciones o juicios referidos al evento o situación actual acerca del cual se quiere medir.

### 3.6.2.2. Valides del Instrumento

**Tabla 3**: Validación de Expertos

| | |
|---|---|
| Mgtr. Ing. Ángel Quispe | Experto Metodológico |
| Mgtr. Ing. Ángel Quispe | Experto Temático |

**Fuente: Elaboración propia**

## 3.7. Métodos de análisis de datos

El cuestionario o instrumento se realizó de acuerdo a lo siguiente:

- Redacción y número de indicadores: se elaboraron una serie de indicadores, en número tal, que no afectaran a la validez y que reflejaran una política de seguridad para el ambiente productivo de base de datos OSSAB y su Influencia en la seguridad de la información del ORES - FOVIME.
- El instrumento tiene una respuesta a la elección de una de las cinco categorías presentadas, las cuales se incrementan del 1 (menor) al 5 (mayor), Cuya escala de intervalo será la siguiente: 1 = muy deficiente, 2 = deficiente, 3 = regular, 4 = bueno, 5 = excelente.
- El instrumento está conformado por 25 preguntas.
- Se aplicará a 30 personas incluyen colaboradores del área de finanzas, sistemas, contabilidad.

## 3.8. Aspectos Éticos

Como profesional en servicio a la sociedad y a mi país prima en mí la honestidad para considerar los derechos de autor que se tipifican en esta investigación. En el rubro de seguridad de la información y base de datos se siguen lineamientos verificados por Norma ISO 27001 (Seguridad de la Información), Norma ISO 1911 (Seguridad Auditorias de Sistemas), ISO 2703 (Seguridad en la red) y Otros. Es por esta razón que se siguieron las normas éticas al realizar esta investigación no experimental bajo las directrices en cuanto a normas para la elaboración de esta investigación.

# IV. RESULTADOS

## 4.1. Resultados (Solución Temática y Estadística)

### 4.1.1. Presentación de los resultados descriptivos

Esta Investigación demostrara la Influencia de una política de seguridad en la seguridad de la información del ORES - FOVIME.

Para la tabulación de datos se le realizo en una hoja Excel, representada mediante una tabla en la que se encuentra las opciones que tiene cada pregunta, la frecuencia, y frecuencia representada en porcentajes, su función es demostrar de forma sencilla la lectura de los resultados en las encuestas.

Para estos resultados se aplicó una encuesta a los trabajadores de la Empresa que laboran en el área de Sistemas, Finanzas y Contabilidad. Los resultados se demuestran a continuación:

**Tabla 4:**

**Pregunta Nº 1:** ¿Revisa, controla el Ingreso y Salida de usuarios que acceden a la información del ambiente productivo de la base de datos OSSAB?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 0 | 0 |
| Casi nunca | 3 | 10 |
| A veces | 7 | 23 |
| Casi siempre | 18 | 60 |
| Siempre | 2 | 7 |
| **TOTAL** | **30** | **100** |

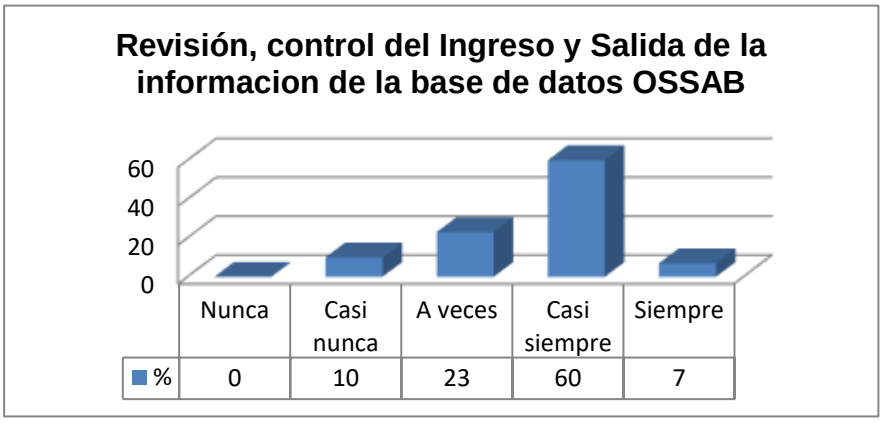



**Figura 5: Pregunta 1**
**Fuente: Encuesta Aplicada - Elaboración propia**

✓ **Análisis Pregunta 1.**

Del total de encuestados, el 60%, responden que casi siempre revisan, controlan el ingreso y salida de usuarios que acceden a la información del ambiente de producción del ORES-FOVIME, el 23% A veces, mientras que el 10% casi nunca y 7% opinan siempre.

✓ **Interpretación Pregunta 1.**

Con los datos obtenidos se determina que la mayor parte de los encuestados dicen que Casi siempre se revisa, controla el ingreso y salida del acceso a la información de la base de datos OSSAB, este criterio se sustenta con la opinión del 60% de los encuestados, lo que demuestra que no es segura la afirmación.

**Tabla 5:**

**Pregunta Nº 2:** ¿Se promueve la participación activa de las Buenas Prácticas del acceso a datos?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 0 | 0 |
| Casi nunca | 0 | 0 |
| A veces | 21 | 70 |
| Casi siempre | 0 | 0 |
| Siempre | 9 | 30 |
| **TOTAL** | **30** | **100** |

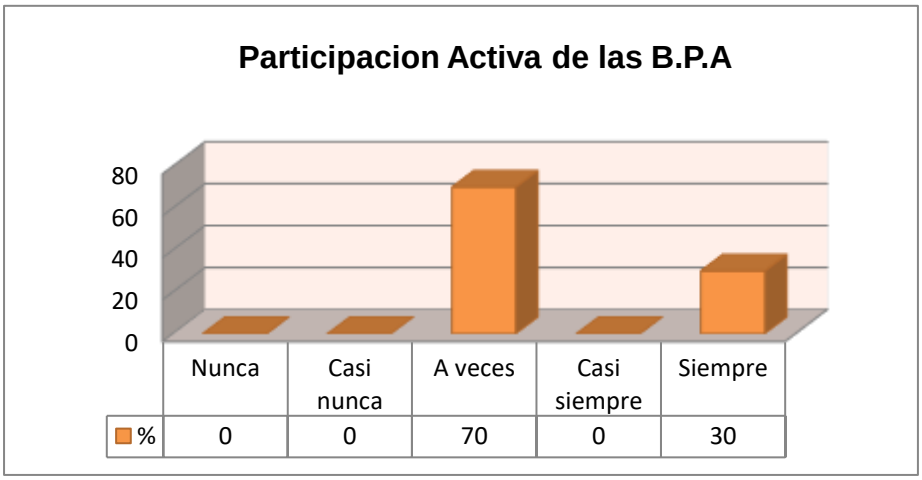



**Figura 6: Pregunta 2**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 2**

Del total de encuestados, el 70%, responden que a veces se promueve la participación activa de la buenas prácticas del acceso a datos, mientras que el 30% opinan siempre.

✓ **Interpretación Pregunta 2**

Con los datos obtenidos se determina que la mayor parte de los encuestados afirman a veces se promueve la participación activa de la buenas prácticas del acceso a datos, este criterio se sustenta con la opinión del 70% de los encuestados, lo que demuestra que no es segura.

**Tabla 6:**

**Pregunta Nº 3**: ¿Considera que debería controlarse el ingreso y salida de usuarios al sistema?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 4 | 13 |
| Casi nunca | 0 | 0 |
| A veces | 13 | 43 |
| Casi siempre | 2 | 7 |
| Siempre | 11 | 37 |
| **TOTAL** | **30** | **100** |

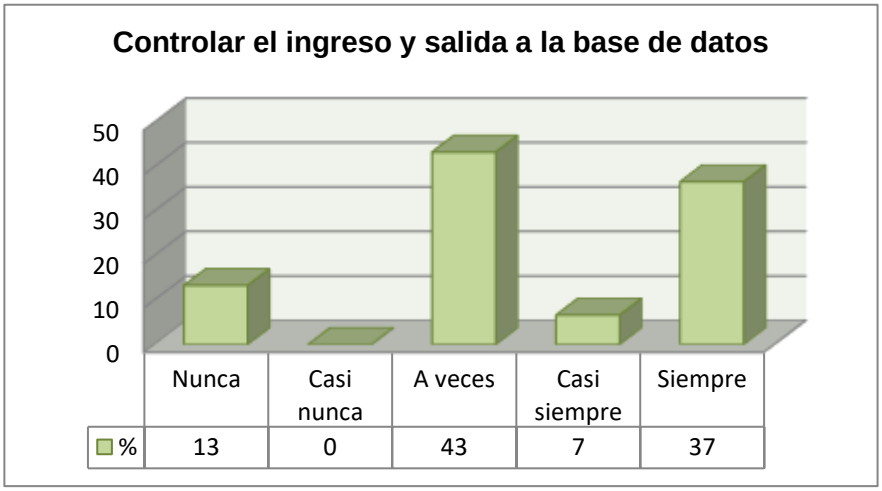



**Figura 7: Pregunta 3**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 3.**

Del total de encuestados, el 13%, responden nunca mientras que el 43% a veces, el 7% casi siempre y el 37% siempre.

✓ **Interpretación Pregunta 3.**

Con los datos obtenidos se determina que la mayor parte de los encuestados afirman a veces se considera que debería controlarse el ingreso y salida de existencias. Este criterio se sustenta con la opinión del 43% de los encuestados, lo que demuestra que no siempre consideran este criterio.

**Tabla 7:**

**Pregunta Nº 4**

¿Considera que las actividades se monitorean por perfiles?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 0 | 0 |
| Casi nunca | 16 | 64 |
| A veces | 9 | 36 |
| Casi siempre | 0 | 0 |
| Siempre | 0 | 0 |
| **TOTAL** | **25** | **100** |

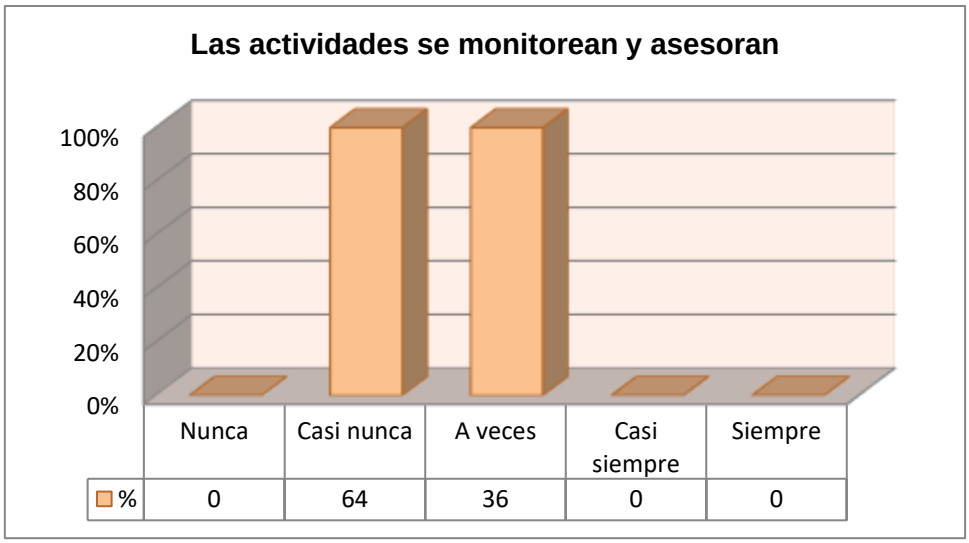



**Figura 8: Pregunta 4**
**Fuente: Encuesta Aplicada - Elaboración propia.**

- ✓ **Análisis Pregunta 4.**

  Del total de encuestados, el 64%, responden nunca mientras y el 36% a veces.

- ✓ **Interpretación Pregunta 4.**

  Con los datos obtenidos se determina que la mayor parte de los encuestados afirman casi nunca se monitorean y asesoran las actividades. Este criterio se sustenta con la opinión del 64% de los encuestados, lo que demuestra que no realizan este criterio.

**Tabla 8:**

**Pregunta Nº 5:** ¿La información cada cierto periodo es consolidada y validada?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 0 | 0 |
| Casi nunca | 3 | 10 |
| A veces | 23 | 77 |
| Casi siempre | 2 | 7 |
| Siempre | 2 | 7 |
| **TOTAL** | **30** | **100** |

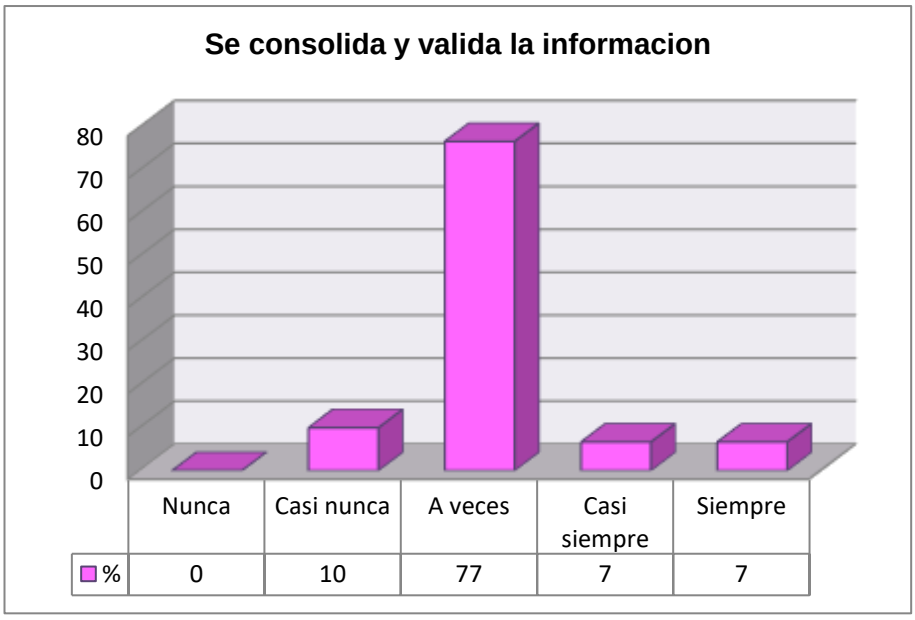



**Figura 9: Pregunta 5**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 5.**

Del total de encuestados, el 10%, responden casi nunca, mientras 77% A veces, el 7% casi siempre y el 7% siempre.

✓ **Interpretación Pregunta 5.**

Con los datos obtenidos se determina que la mayor parte de los encuestados afirman a veces se consolida y valida la información cada cierto periodo información relacionada a existencias en la empresa. Este criterio se sustenta con la opinión del 77% de los encuestados, lo que demuestra que no siempre consideran esta actividad.

**Tabla 9:**

**Pregunta Nº 6:** ¿Genera confianza los accesos externos al sistema del ORES-FOVIME?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 0 | 0 |
| Casi nunca | 9 | 30 |
| A veces | 15 | 50 |
| Casi siempre | 2 | 7 |
| Siempre | 4 | 13 |
| **TOTAL** | **30** | **100** |

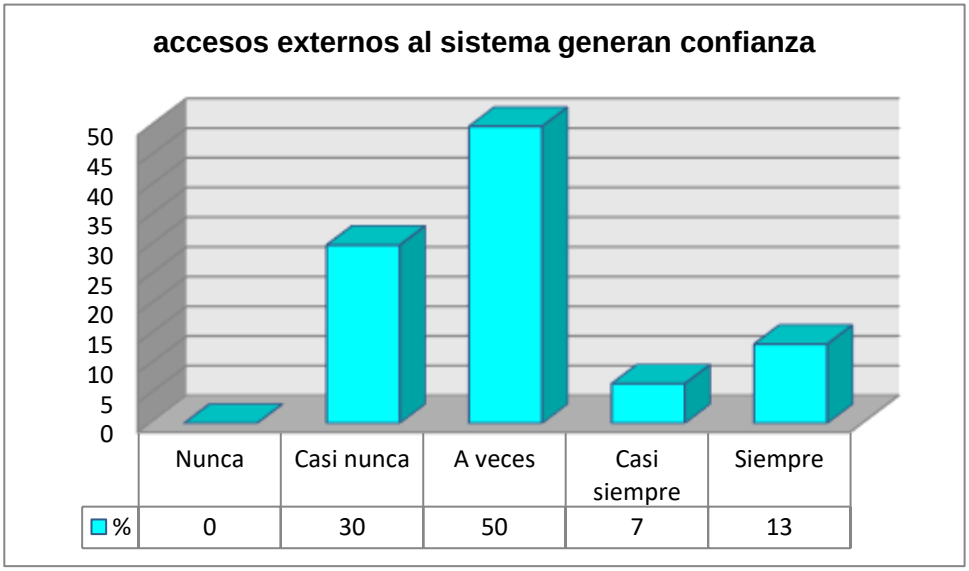



**Figura 10: Pregunta 6**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 6.**

Del total de encuestados, el 30%, responden casi nunca, mientras 50% A veces, el 7% casi siempre y el 13% siempre.

✓ **Interpretación Pregunta 6.**

Con los datos obtenidos se determina que la mayor parte de los encuestados afirman a veces se genera confianza los accesos externos al sistema. Este criterio se sustenta con la opinión del 50% de los encuestados, lo que demuestra que no es segura esta confianza.

**Tabla 10:**

**Pregunta Nº 7:** ¿Considera que la toma decisiones es a partir de la información que le brinda el área de sistemas?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 0 | 0 |
| Casi nunca | 2 | 7 |
| A veces | 22 | 73 |
| Casi siempre | 0 | 0 |
| Siempre | 6 | 20 |
| **TOTAL** | **30** | **100** |

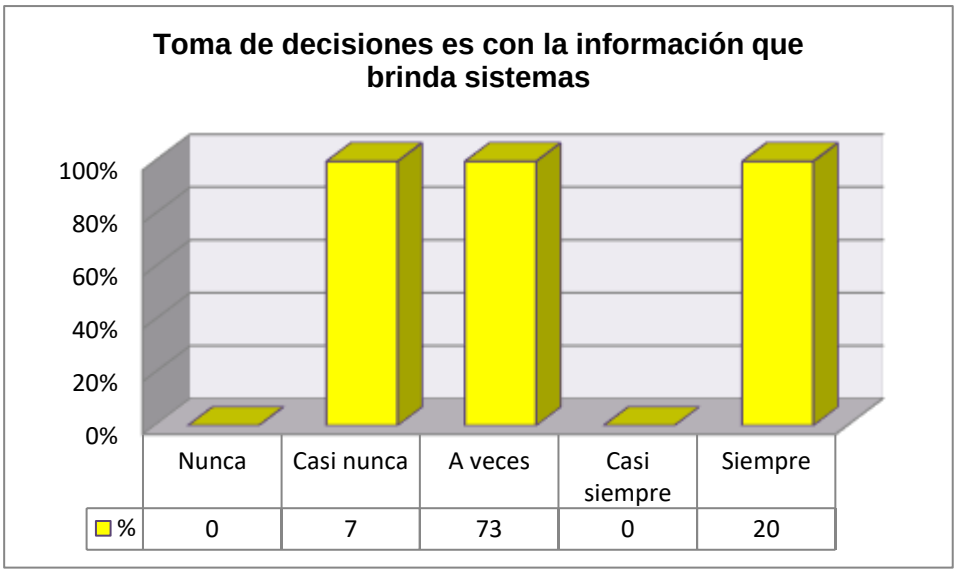



**Figura 11: Pregunta 7**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 7.**

Del total de encuestados, el 7%, responden casi nunca, mientras 73% A veces, y el 20% siempre.

✓ **Interpretación Pregunta 7.**

Con los datos obtenidos se determina que la mayor parte de los encuestados afirman a veces se toma decisiones a partir de la información del área de sistemas. Este criterio se sustenta con la opinión del 73% de los encuestados, lo que demuestra que la información de almacén la consideran para la toma de decisiones.

**Tabla 11:**

**Pregunta Nº 8:** ¿Considera que la inmovilización equipos genera pérdidas?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 0 | 0 |
| Casi nunca | 0 | 0 |
| A veces | 7 | 23 |
| Casi siempre | 8 | 27 |
| Siempre | 15 | 50 |
| **TOTAL** | **30** | **100** |

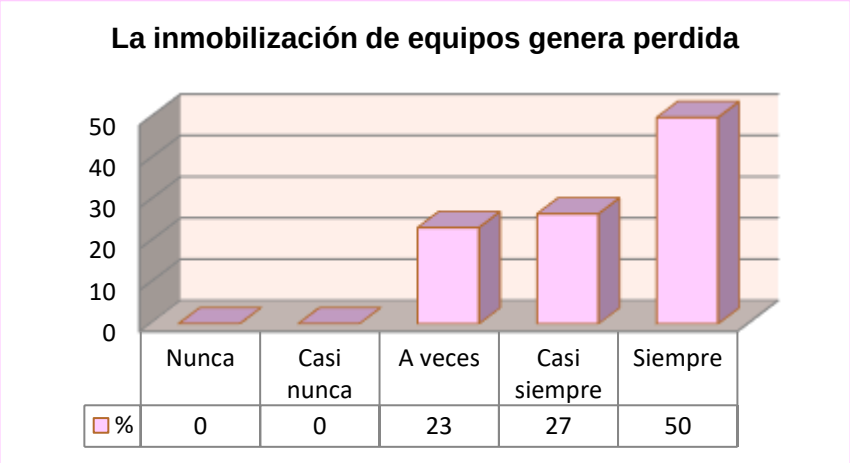



**Figura 12: Pregunta 8**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 8.**

Del total de encuestados, el 23%, responden a veces, mientras 27% casi siempre, y el 50% siempre.

✓ **Interpretación Pregunta 8.**

Con los datos obtenidos se determina que la mayor parte de los encuestados afirman siempre se Considera que la inmovilización de equipos genera pérdidas. Este criterio se sustenta con la opinión del 50% de los encuestados, lo que demuestra que siempre toman en cuenta este punto.

**Tabla 12:**

**Pregunta Nº 9:** ¿Utiliza algún proceso para que la información se convierta con rapidez en efectivo?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 9 | 30 |
| Casi nunca | 9 | 30 |
| A veces | 12 | 40 |
| Casi siempre | 0 | 0 |
| Siempre | 0 | 0 |
| **TOTAL** | **30** | **100** |

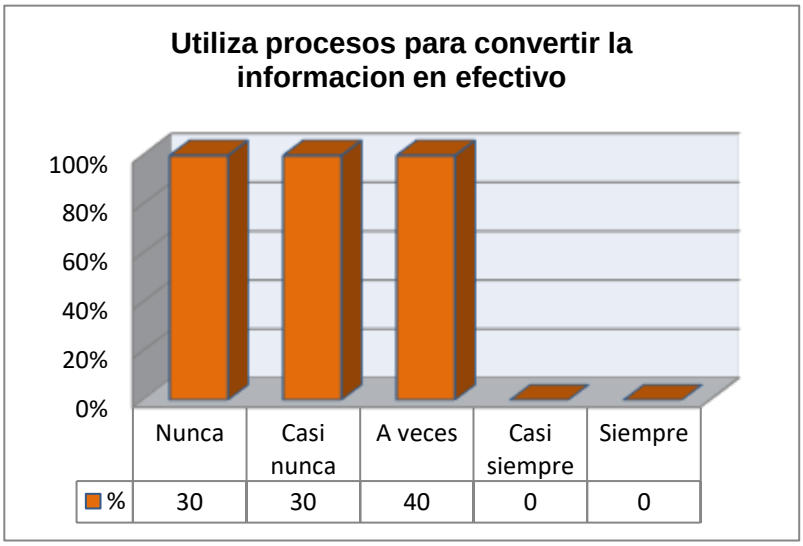



**Figura 13: Pregunta 9**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 9.**

Del total de encuestados, el 30%, responden nunca, mientras 30% casi nunca, y el 40% a veces.

✓ **Interpretación Pregunta 9.**

Con los datos obtenidos se determina que la mayor parte de los encuestados afirman a veces Utiliza algún tipo de proceso para que la información se convierta con rapidez en efectivo. Este criterio se sustenta con la opinión del 40% de los encuestados, lo que demuestra que no utilizan estas actividades.

**Tabla 13:**

**Pregunta Nº 10:** ¿El área de sistemas se encarga de la seguridad de la información?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 0 | 0 |
| Casi nunca | 0 | 0 |
| A veces | 18 | 60 |
| Casi siempre | 12 | 40 |
| Siempre | 0 | 0 |
| **TOTAL** | **30** | **100** |

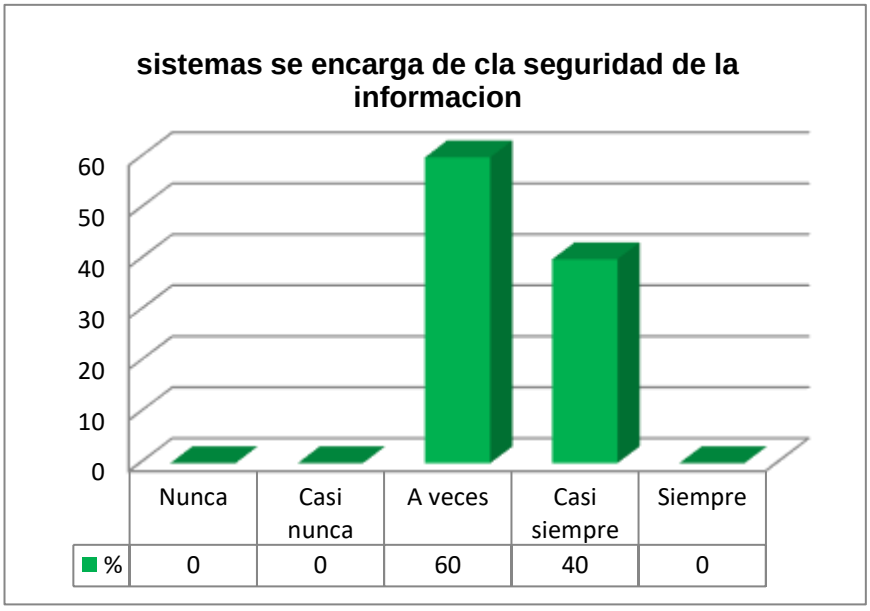



**Figura 14: Pregunta 10**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 10.**

Del total de encuestados, el 40%, responden casi siempre, y a veces 60%

✓ **Interpretación Pregunta 10.**

Con los datos obtenidos se determina que la mayor parte de los encuestados afirman a veces el área de sistemas se encarga de la seguridad de la información. Este criterio se sustenta con la opinión del 60% de los encuestados, lo que demuestra que ventas es el encardo de ocuparse en esta actividad.

**Tabla 14:**

**Pregunta Nº 11:** ¿Tiene alguna idea de cuánto tiempo dura un usuario externo conectado a la base de datos OSSAB?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 0 | 0 |
| Casi nunca | 26 | 87 |
| A veces | 4 | 13 |
| Casi siempre | 0 | 0 |
| Siempre | 0 | 0 |
| **TOTAL** | **30** | **100** |

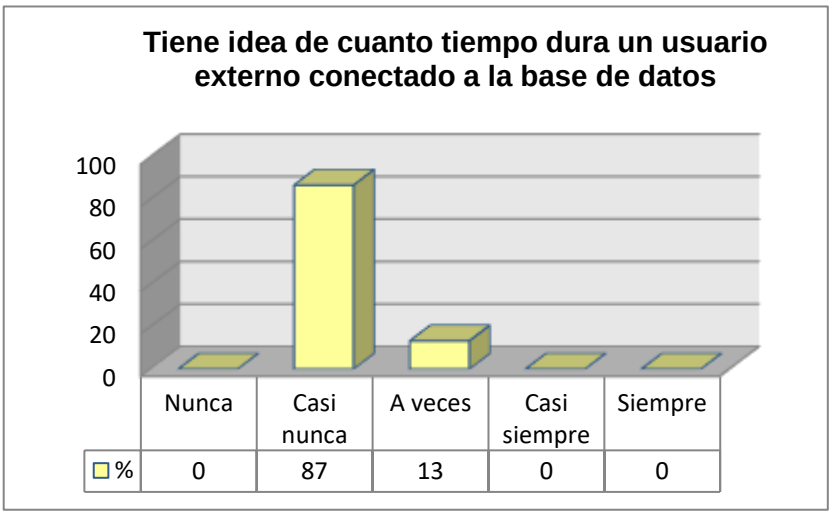



**Figura 15: Pregunta 11**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 11.**

Del total de encuestados, el 87%, responden casi nunca, y a veces 13%.

✓ **Interpretación Pregunta 11.**

Con los datos obtenidos se determina que la mayor parte de los encuestados afirman que casi nunca tienen alguna idea de cuánto tiempo dura un usuario externo conectado a la base de datos OSSAB. Este criterio se sustenta con la opinión del 87% de los encuestados, lo que demuestra que casi nadie tiene en cuenta este detalle.

**Tabla 15:**

**Pregunta Nº 12:** ¿Revisa minuciosamente la información que ingresa diariamente al sistema?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 0 | 0 |
| Casi nunca | 25 | 83 |
| A veces | 5 | 17 |
| Casi siempre | 0 | 0 |
| Siempre | 0 | 0 |
| **TOTAL** | **30** | **100** |

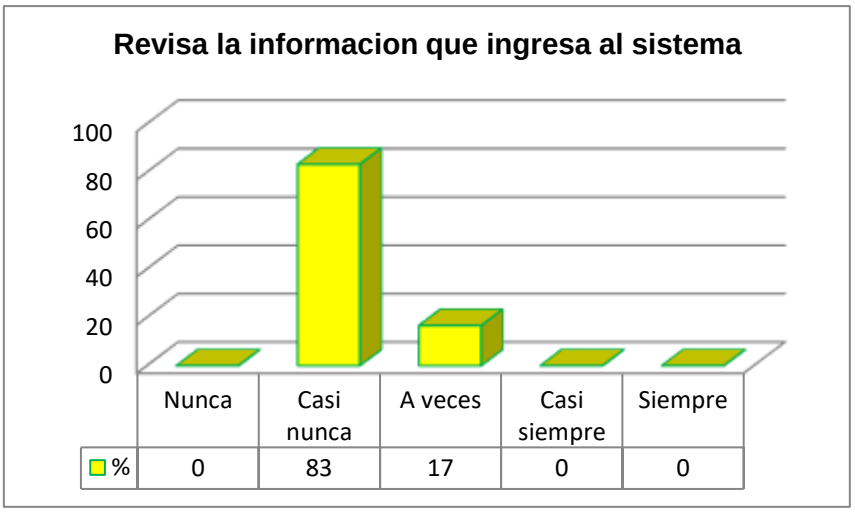



**Figura 16: Pregunta 12**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 12.**

Del total de encuestados, el 83%, responden casi nunca, y a veces 17%.

✓ **Interpretación Pregunta 12.**

Con los datos obtenidos se determina que la mayor parte de los encuestados afirman que casi nunca revisan minuciosamente la información que ingresa diariamente al sistema. Este criterio se sustenta con la opinión del 83% de los encuestados, lo que demuestra que no toman en cuenta esta actividad.

**Tabla 16:**

**Pregunta Nº 13:** ¿Cada cuánto tiempo realiza el cambio de su contraseña de acceso al sistema?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 0 | 0 |
| Casi nunca | 5 | 17 |
| A veces | 13 | 43 |
| Casi siempre | 8 | 27 |
| Siempre | 4 | 13 |
| **TOTAL** | **30** | **100** |

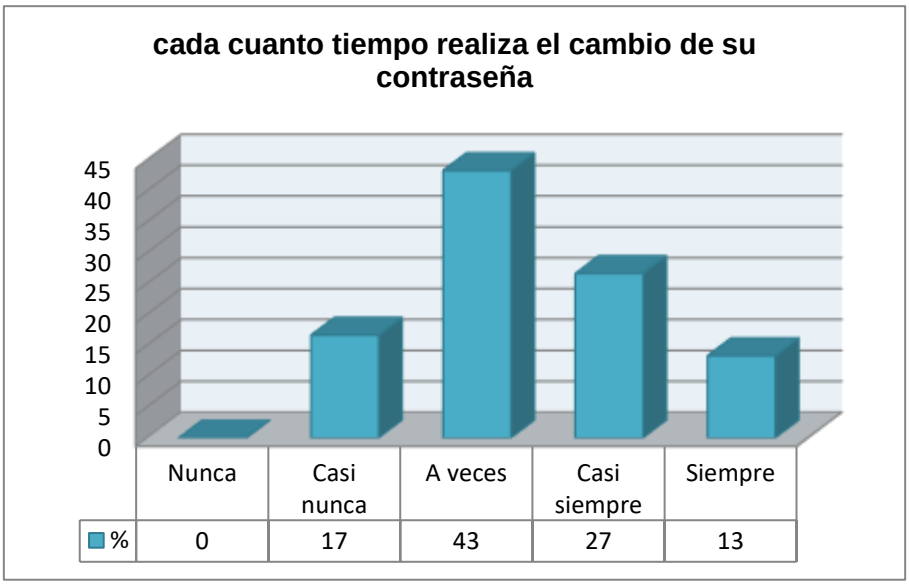



**Figura 17: Pregunta 13**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 13.**

Del total de encuestados, el 17%, responden casi nunca, el 43% a veces, el 27% casi siempre y siempre13%.

✓ **Interpretación Pregunta 13.**

Con los datos obtenidos se determina que la mayor parte de los encuestados afirman que a veces realizan el cambio de su contraseña de acceso al sistema. Este criterio se sustenta con la opinión del 43% de los encuestados, lo que demuestra que no es segura esta afirmación.

**Tabla 17:**

**Pregunta Nº 14:** ¿Considera como un activo esencial la información que está sujeto a amenazas y vulnerabilidades?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 0 | 0 |
| Casi nunca | 5 | 17 |
| A veces | 25 | 83 |
| Casi siempre | 0 | 0 |
| Siempre | 0 | 0 |
| **TOTAL** | **30** | **100** |

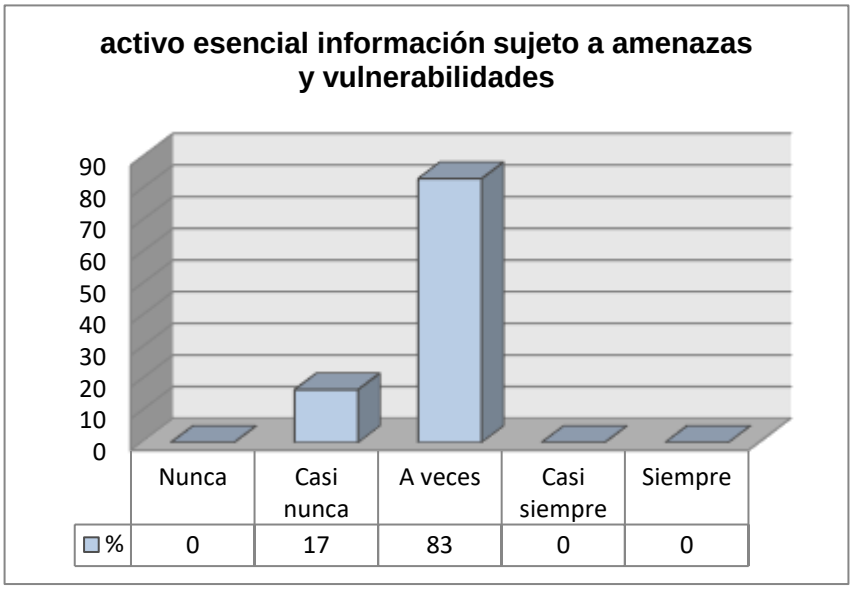



**Figura 18: Pregunta 14**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 14.**

Del total de encuestados, el 17%, responden casi nunca y el 83% a veces.

✓ **Interpretación Pregunta 14.**

Con los datos obtenidos se determina que la mayor parte de los encuestados afirman que a veces considera como un activo esencial la información que está sujeto a amenazas y vulnerabilidades.

**Tabla 18:**

**Pregunta Nº 15:** ¿En la cláusula de su contrato existe un compromiso por parte de la institución de proteger su usuario y clave de acceso al sistema?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 0 | 0 |
| Casi nunca | 0 | 0 |
| A veces | 19 | 63 |
| Casi siempre | 11 | 37 |
| Siempre | 0 | 0 |
| **TOTAL** | **30** | **100** |

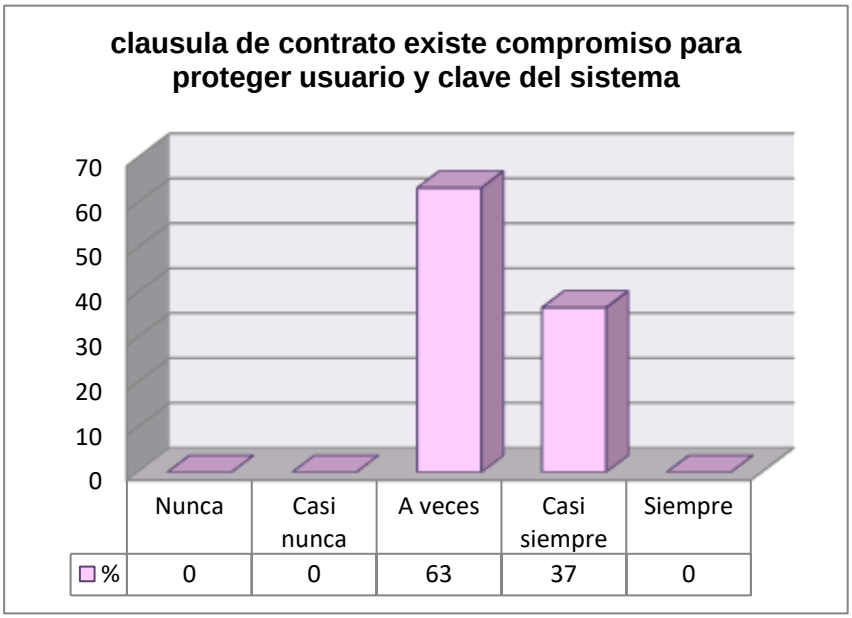



**Figura 19: Pregunta 15**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 15.**

Del total de encuestados, el 63%, responden  a veces y el 37% casi siempre.

✓ **Interpretación Pregunta 15.**

Con los datos obtenidos se determina que la mayor parte de los encuestados afirman que a veces  en la cláusula de su contrato existe un compromiso por parte de la institución de proteger su usuario y clave de acceso al sistema. Este criterio se sustenta con la opinión del 63% de los encuestados, lo que demuestra que no es segura esta actividad.

**Tabla 19:**

**Pregunta Nº 16:** ¿Existe un mecanismo que tú conoces sobre los accesos de los visitantes de la Institución registrando la fecha y hora de entrada y salida de los mismos?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 0 | 0 |
| Casi nunca | 0 | 0 |
| A veces | 18 | 60 |
| Casi siempre | 12 | 40 |
| Siempre | 0 | 0 |
| **TOTAL** | **30** | **100** |

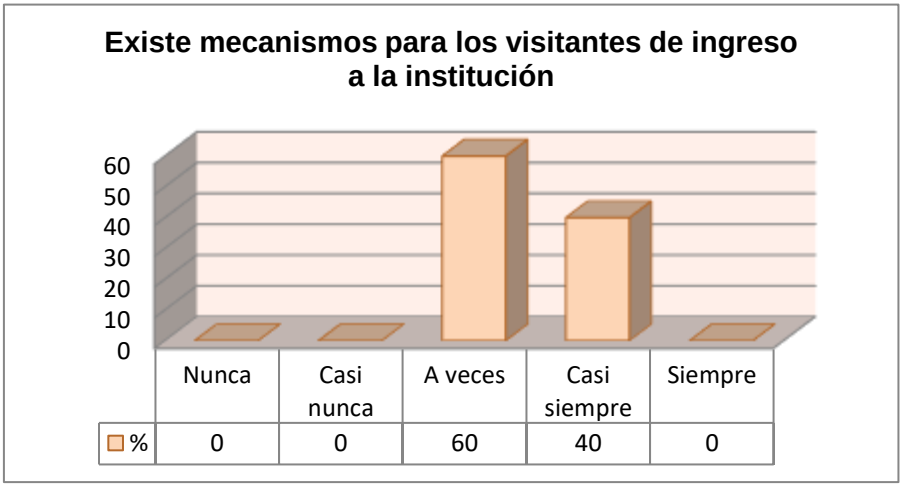



**Figura 20: Pregunta 16**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 16.**

Del total de encuestados, el 60% respondieron a veces y el 40% casi siempre.

✓ **Interpretación Pregunta 16.**

Con los datos obtenidos se determina que la mayor parte de los encuestados afirman que a veces existe un mecanismo que tú conoces sobre los accesos de los visitantes de la Institución registrando la fecha y hora de entrada y salida de los mismos. Este criterio se sustenta con la opinión del 60% de los encuestados, lo que demuestra que no siempre se da esta actividad.

**Tabla 20:**

**Pregunta Nº 17:** ¿Realiza con frecuencia copias de seguridad de la base de datos OSSAB?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 16 | 53 |
| Casi nunca | 0 | 0 |
| A veces | 2 | 7 |
| Casi siempre | 3 | 10 |
| Siempre | 9 | 30 |
| **TOTAL** | **30** | **100** |

**Tabla 19: Pregunta 17**

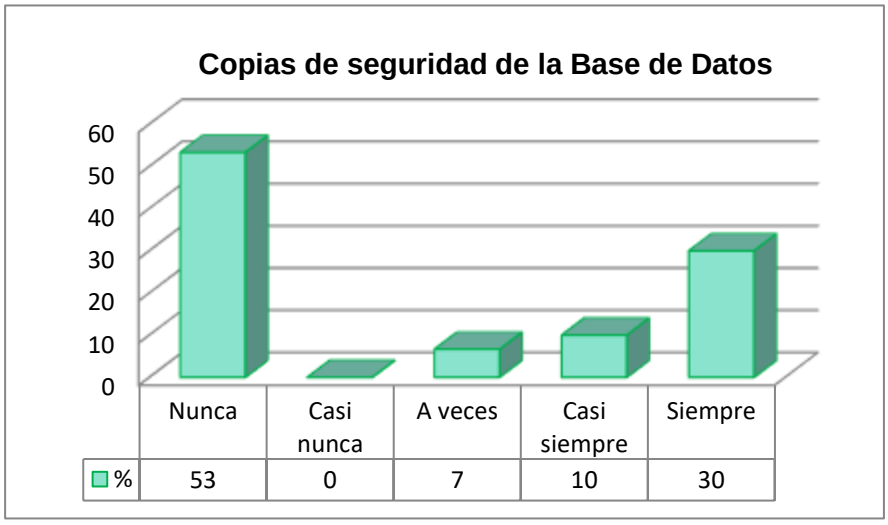



**Figura 21: Pregunta 17**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 17.**

Del total de encuestados, el 53% respondieron nunca, el 7%, el 10% casi siempre y el 30% siempre.

✓ **Interpretación Pregunta 17.**

Con los datos obtenidos se determina que la mayor parte de los encuestados m. Este criterio se sustenta con la opinión del 53% de los encuestados, lo que demuestra que los inversionistas de esta empresa no están tomando en cuenta este detalle.

**Tabla 21:**

**Pregunta Nº 18:** ¿Has firmado un documento para mantener confidenciales las claves secretas de los sistemas de información que maneja?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 4 | 13 |
| Casi nunca | 21 | 70 |
| A veces | 5 | 17 |
| Casi siempre | 0 | 0 |
| Siempre | 0 | 0 |
| **TOTAL** | **30** | **100** |

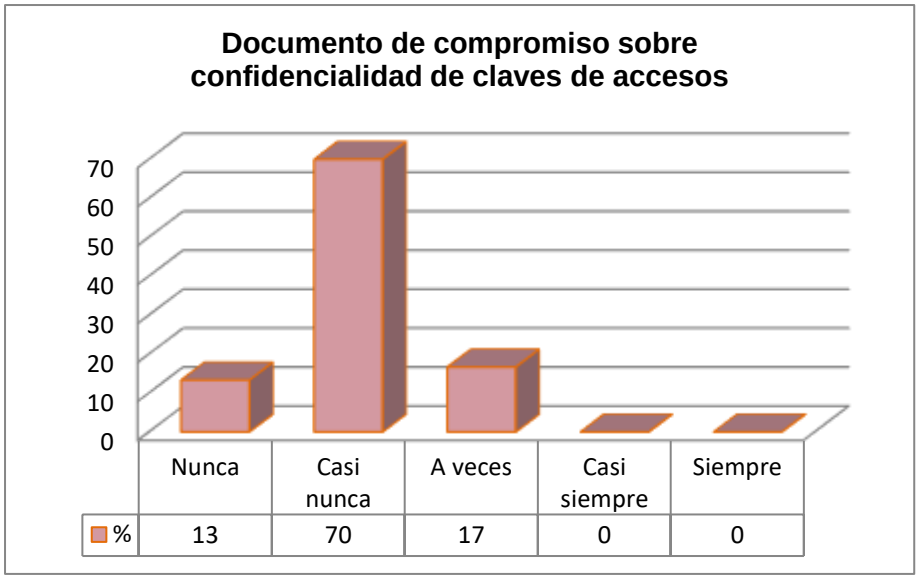



**Figura 22: Pregunta 18**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 18.**

Del total de encuestados, el 13% respondieron nunca, el 70% casi nunca y el 17% a veces.

✓ **Interpretación Pregunta 18.**

Con los datos obtenidos se determina que la mayor parte de los encuestados afirman que casi nunca han firmado un documento para mantener confidenciales las claves secretas de los sistemas de información que maneja el usuario. Este criterio se sustenta con la opinión del 70% de los encuestados, lo que demuestra que no siempre se da esta actividad.

**Tabla 22:**

**Pregunta Nº 19:** ¿Ha recibido capacitación en seguridad de la información en la institución?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 4 | 13 |
| Casi nunca | 7 | 23 |
| A veces | 19 | 63 |
| Casi siempre | | 0 |
| Siempre | 0 | 0 |
| **TOTAL** | **30** | **100** |

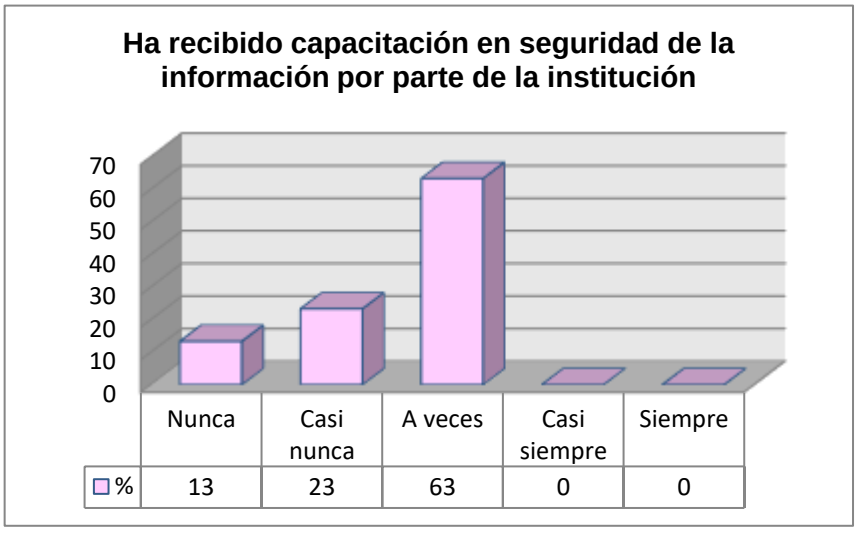



**Figura 23: Pregunta 19**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 19.**

Del total de encuestados, el 13% respondieron nunca, el 23% casi nunca y el 63% a veces.

✓ **Interpretación Pregunta 19.**

Con los datos obtenidos se determina que la mayor parte de los encuestados afirman que a veces el usuario ha recibido capacitación en seguridad de la información en la institución. Este criterio se sustenta con la opinión del 63% de los encuestados, lo que demuestra que no siempre se da esta actividad.

**Tabla 23:**

**Pregunta Nº 20:** ¿Conoce sobre política de seguridad de Base de Datos?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 9 | 30 |
| Casi nunca | 4 | 13 |
| A veces | 10 | 33 |
| Casi siempre | 0 | 0 |
| Siempre | 7 | 23 |
| **TOTAL** | **30** | **100** |

**Tabla 22: Pregunta 20**

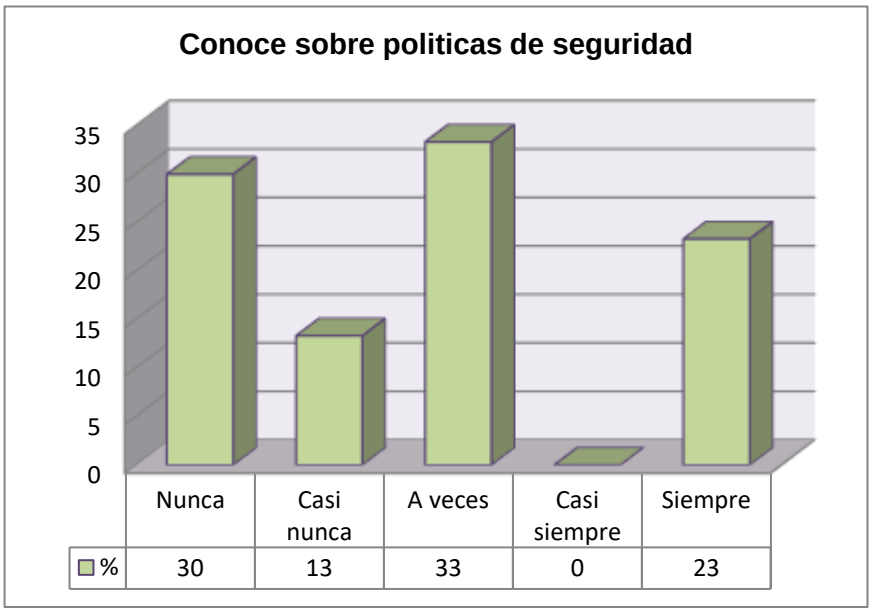



**Figura 24: Pregunta 20**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 20.**

Del total de encuestados, el 30% respondieron nunca, el 13% casi nunca, el 33% a veces y el 23% siempre.

✓ **Interpretación Pregunta 20.**

Con los datos obtenidos se determina que la mayor parte de los encuestados afirman que a veces le mencionaron sobre política de seguridad de Base de Datos. Este criterio se sustenta con la opinión del 33% de los encuestados, lo que demuestra que no siempre se da esta actividad.

**Tabla 24**

**Pregunta Nº 21:** ¿Conoce la seguridad de la Base de Datos OSSAB del ORES-FOVIME?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 4 | 13 |
| Casi nunca | 0 | 0 |
| A veces | 24 | 80 |
| Casi siempre | 2 | 7 |
| Siempre | 0 | 0 |
| **TOTAL** | **30** | **100** |

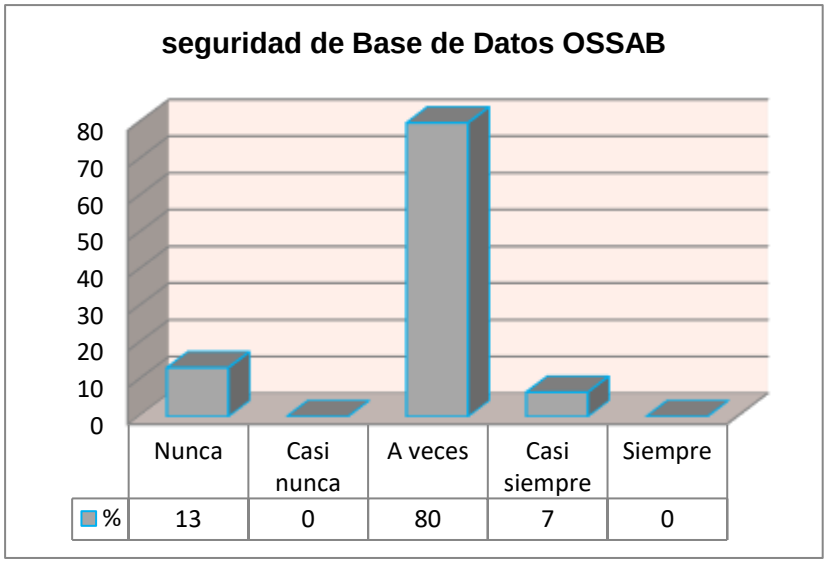



**Figura 25: Pregunta 21**
**Fuente: Encuesta Aplicada - Elaboración propia.**

- ✓ **Análisis Pregunta 21.**

  Del total de encuestados, el 13% respondieron nunca, el 80% a veces y el 7% casi siempre.

- ✓ **Interpretación Pregunta 21.**

  Con los datos obtenidos se determina que la mayor parte de los encuestados afirman que a veces los usuarios no conocen la seguridad de la Base de Datos OSSAB. Este criterio se sustenta con la opinión del 80% de los encuestados, lo que demuestra que no siempre se da esta actividad.

**Tabla 25**

**Pregunta Nº 22:** ¿Se estimula el rendimiento y producción de los usuarios en la seguridad de la información?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 8 | 27 |
| Casi nunca | 0 | 0 |
| A veces | 20 | 67 |
| Casi siempre | 2 | 7 |
| Siempre | 0 | 0 |
| **TOTAL** | **30** | **100** |

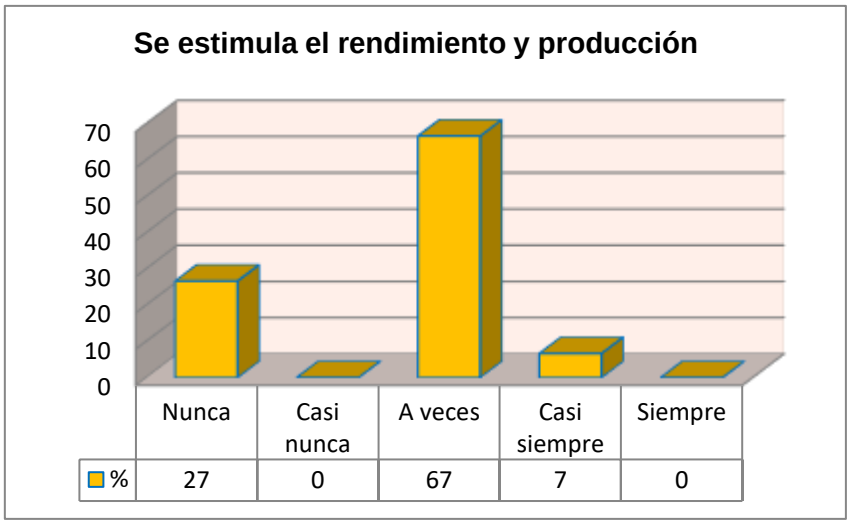



**Figura 26: Pregunta 22**
**Fuente: Encuesta Aplicada - Elaboración propia.**

- ✓ **Análisis Pregunta 22.**

  Del total de encuestados, el 27% respondieron nunca, el 67% a veces, y el 7% casi siempre.

- ✓ **Interpretación Pregunta 22.**

  Con los datos obtenidos se determina que la mayor parte de los encuestados afirman que a veces se estimula el rendimiento y producción de los usuarios en el ORES-FOVIME. Este criterio se sustenta con la opinión del 67% de los encuestados, lo que demuestra que no siempre se da esta actividad.

**Tabla 26**

**Pregunta Nº 23:** ¿Cómo gestiona el ORES-FOVIME los riesgos de seguridad de la información?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 8 | 27 |
| Casi nunca | 4 | 13 |
| A veces | 16 | 53 |
| Casi siempre | 2 | 7 |
| Siempre | 0 | 0 |
| **TOTAL** | **30** | **100** |

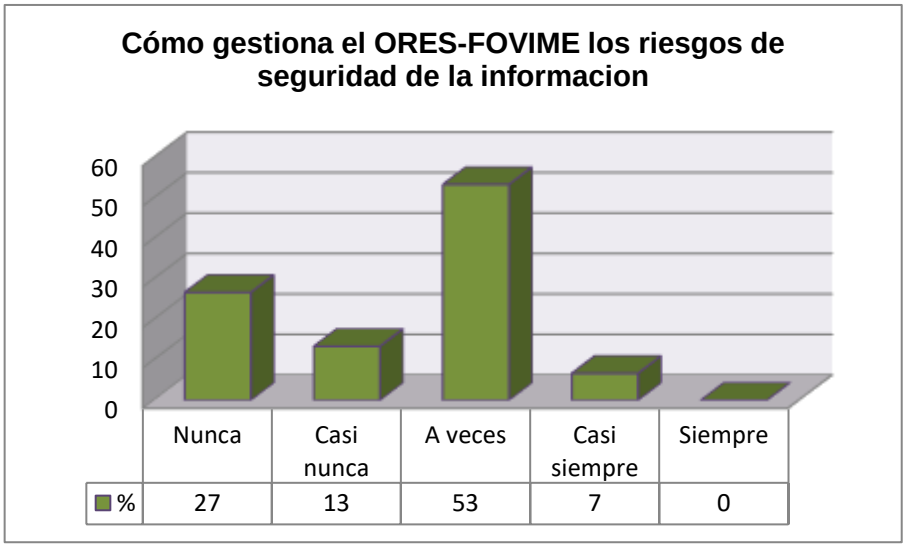



**Figura 27: Pregunta 23**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 23.**

Del total de encuestados, el 27% respondieron nunca, el 13% casi nunca, el 53% a veces, y el 7% casi siempre.

✓ **Interpretación Pregunta 23.**

Con los datos obtenidos se determina que la mayor parte de los encuestados afirman que a veces se desconoce cómo gestiona el ORES-FOVIME los riesgos de la seguridad de la información de la Base de Datos. Este criterio se sustenta con la opinión del 53% de los encuestados, lo que demuestra que no siempre se da esta actividad.

**Tabla 27:**

**Pregunta Nº 24:** ¿Qué tipos de incidentes son mitigados por seguridad?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 5 | 17 |
| Casi nunca | 4 | 13 |
| A veces | 21 | 70 |
| Casi siempre | 0 | 0 |
| Siempre | 0 | 0 |
| **TOTAL** | **30** | **100** |

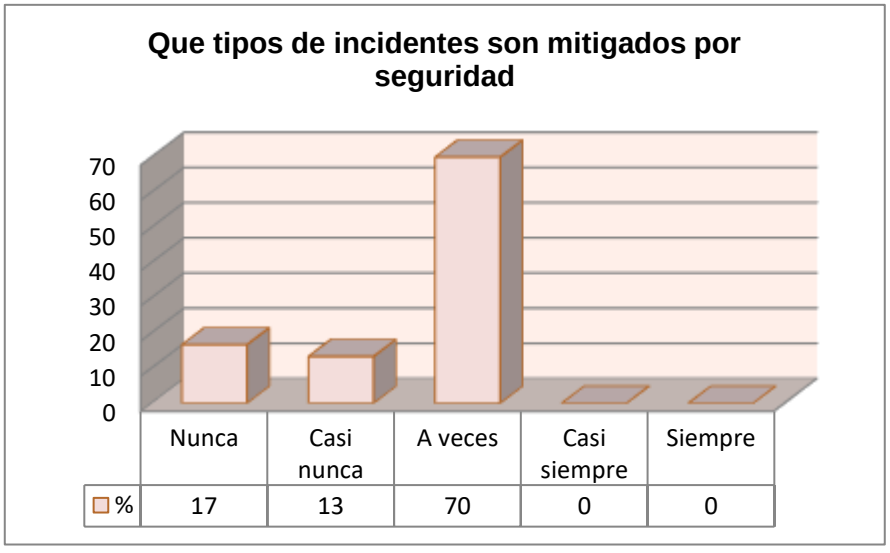



**Figura 28: Pregunta 24**
**Fuente: Encuesta Aplicada - Elaboración propia.**

✓ **Análisis Pregunta 24.**

Del total de encuestados, el 17% respondieron nunca, el 13% casi nunca y el 70% a veces.

✓ **Interpretación Pregunta 24.**

Con los datos obtenidos se determina que la mayor parte de los encuestados afirman que a veces se desconoce qué tipos de incidentes son mitigados por seguridad. Este criterio se sustenta con la opinión del 70% de los encuestados, lo que demuestra que no siempre se da esta actividad.

**Tabla 28:**

**Pregunta Nº 25:** ¿Cree usted que el área de sistemas del ORES-FOVIME se encarga de la seguridad de la información?

| CONOCIMIENTO | Nº | % |
|---|---|---|
| Nunca | 0 | 0 |
| Casi nunca | 0 | 0 |
| A veces | 21 | 70 |
| Casi siempre | 9 | 30 |
| Siempre | 0 | 0 |
| **TOTAL** | **30** | **100** |

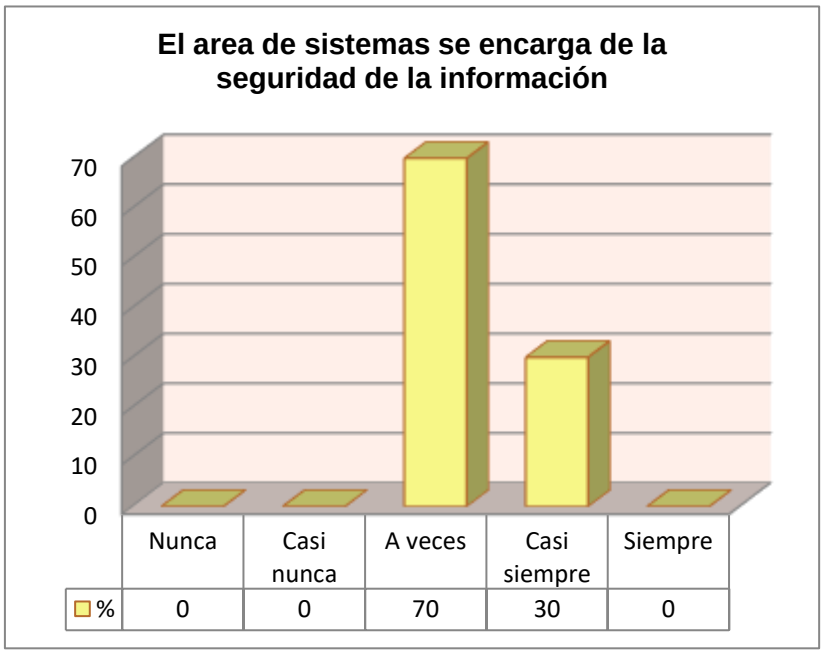



**Figura 29: Pregunta 25**
**Fuente: Encuesta Aplicada - Elaboración propia.**

- ✓ **Análisis Pregunta 25.**

  Del total de encuestados, el 70% respondieron a veces y el 30% casi siempre.

- ✓ **Interpretación Pregunta 25.**

  Con los datos obtenidos se determina que la mayor parte de los encuestados afirman que a veces el área de sistemas del ORES-FOVIME se encarga de la seguridad de la información. Este criterio se sustenta con la opinión del 70% de los encuestados, lo que demuestra que no siempre se da esta actividad.

### 4.2.1 Contrastación de la Hipótesis

La contrastación de la hipótesis general se determinará a través de la propuesta de una política de seguridad que influye en la seguridad de la información de la base de datos del ambiente de producción del ORES – FOVIME.

| | Politica de Seguridad BD | Revisión de configuración | uebas de netración | Ambiente de producción | |
|---|---|---|---|---|---|
| DIMENSIONES DE LAS VARIABLES INDEPENDIENTES Y DEPENDIENTES | Información | 1,000 | ,975 | ,821 | ,950 |
| | Politicas | ,975 | 1,000 | 0,855 | ,837 |
| | Política de seguridad | ,821 | ,855 | 1,000 | 0,920 |
| | Base de Datos | ,950 | ,837 | ,920 | 1,000 |
| Sig. (Unilateral) | Información | | 1,000 | 1,000 | 1,000 |
| | Seguridad | 1,000 | | 1,000 | 1,000 |
| | ANALISIS | 1,000 | ,000 | | 1,000 |
| | RENDIMEINTO | ,1000 | 1,000 | 1,000 | |

**Tabla 30: Matriz de correlaciones entre la variable independiente y variable dependiente. Fuente: Encuesta Aplicada - Elaboración propia en SPSS.**

Los ceros en la parte inferior son índices que se dan para rechazar la hipótesis nula.

### *1.2.2.* El Planteo de las Hipótesis.

#### a) El Planteo de las Hipótesis.

Ho: ” La política se seguridad NO Influye en el rendimiento de la base de datos del ambiente de producción del ORES – FOVIME.”

$H_1$: ” La política se seguridad SI influye en la Seguridad de la información de la base de datos del ambiente de producción de la Empresa ORES - FOVIME”

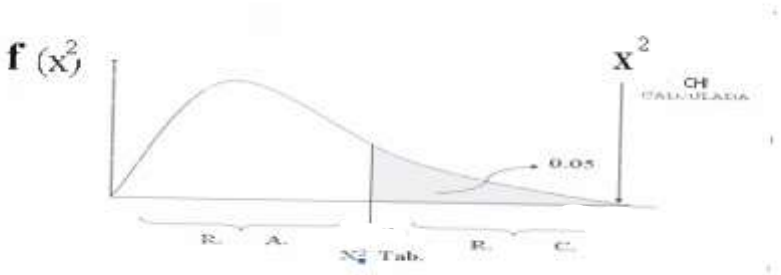
**Tabla 27:** La variable estadística de decisión “Chi- cuadrado”.

**KMO Y PRUEBA DE BARTLETT**

| | | |
|---|---|---|
| Medida de adecuación muestral de Kaiser-Meyer-Olkin. | | 0,914 |
| Prueba de esfericidad de Bartlett | Chi-cuadrado aproximado | 1094,124 |
| | gl | 6 |
| | Sig. | 0,000 |

#### b) La Contrastación de la Hipótesis

$X^2$ Tabular es con 0.95 de probabilidad y 6 grados de libertad es 12,596




**12,596** **1094.124**

**Figura 31: Encuesta aplicada**
**Fuente: Encuesta aplicada – Elaboración propia**

La parte no sombreada es el nivel de confianza de la prueba.

La parte sombreada es el error de la prueba.

Finalmente se observa en el grafico que $X^2_{Calculado}$ es mayor que la $X^2_{Tabular}$ obtenido de la tabla. Por lo que, según el grafico pertenece a la región de rechazo (parte sombreada) es decir se rechaza el Ho (Hipótesis nula).

# V. DISCUSIÓN

Podemos observar en los resultados obtenidos del Organismo Especial del Fondo de Vivienda Militar ORES-FOVIME, la empresa no cuenta con un plan de políticas establecidas para la protección de la información sensible que manejan, donde se especifique claramente los pasos a seguir para la protección de la información registrado a través de los sistemas y alojada en los servidores del ORES-FOVIME. Originando riesgo de pérdida de información sensible de las operaciones diarias que se realizan en la empresa para esto propongo esta cadena de requerimientos de políticas para la seguridad de la información, apoyados de la Norma Técnica Peruana “NTP-ISO/IEC 12207:2016- Ingeniería de Software y Sistemas. Procesos del ciclo de vida del software. 3a Edición”, en todas las entidades integrantes del Sistema Nacional de Informática.

Implementar una política de seguridad para la base de datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME.

### 5.1.1 Análisis de los indicadores

**a)** Al iniciar el proyecto, no existía una política de seguridad de información y mucho menos la cultura para proteger los activos de información. Se puede observar una mejoría del 70% en promedio de los indicadores. Actualmente los colaboradores de la gerencia de telemática conocen como sus funciones cotidianas aportan al mantenimiento y mejora continua del plan de políticas de seguridad para la información implementados

**b)** Con los resultados obtenidos después de la implementación del plan de políticas de seguridad para la información de la Base de Datos OSSAB, se lograron detectar de manera preventiva las vulnerabilidades, mitigando así los futuros riesgos.

De igual manera, se logró implementar procesos de atención inmediata para las vulnerabilidades e incidentes reportados.

Al iniciar el proyecto, se detectó:

- Activos de información sin controles para los cuales se implementaron diferentes tipos de controles preventivos, correctivos y detectivos.
- Muchos riesgos con calificativo no tolerables, los cuales se lograron minimizar a un 0 %.

Si bien todos los colaboradores involucrados en los procesos de tecnología están muy bien entrenados para el cumplimiento de sus labores, no contaban con una formación y concientización sobre la seguridad de información y protección de los activos de información. Se puede observar que después de la implementación de la política de seguridad, los colaboradores incrementaron notablemente su compromiso con la seguridad de los activos de información.
Después de los análisis de brechas PRE y POST, se observa que el cumplimiento mejora en un 52%. Aun así existe una pequeña brecha por cumplir, en la cual la empresa deberá seguir trabajando para cubrirla.

**Beneficios**:

- Provee a la gerencia dirección y apoyo para gestionar la seguridad de la información.
- Ayuda a identificar los activos de información y a protegerlos adecuadamente.
- Enfoque sistemático para el análisis y evaluación del riesgo de información de la empresa.
- Asegura una correcta y segura operación de información de la empresa, reduciendo el riesgo del error humano.
- Incrementa, sustancialmente, el control de acceso a la información.
- Minimiza la interrupción en el funcionamiento de las actividades del negocio.
- Demuestra confianza al mercado, proveedores y sociedad.

## VI. CONCLUSIONES:

1. Se puede concluir, que la política de seguridad si influye en la Seguridad de la información de la base de datos del ambiente de producción de la Empresa ORES - FOVIME", a un nivel de significación.
2. El implementar una política de seguridad y que los colaboradores la conozcan e interiorizan, es de gran utilidad cuando se quiere implementar cualquier sistema de gestión en una organización, ya que les da una visión clara de cómo sus labores cotidianas aportan para el mantenimiento y mejora del plan de políticas de seguridad de la información.
3. Aún después de implementar un buen plan de políticas de seguridad de la información, en el futuro se presentan más activos de información, más amenazas, vulnerabilidades y por lo tanto, mayores riesgos. Este escenario no se puede evitar; es por ello que se concluye, que se debe estar preparado para actuar de manera inmediata ante cualquier nueva vulnerabilidad que se identifique.
4. Diseñando e implementando una buena metodología para gestionar los riesgos y ejecutando los planes de tratamiento de riesgos planteados, se logra reducir a niveles aceptables gran porcentaje de riesgos que afecten a los activos de información.
5. El factor humano es crítico para la implementación de cualquier plan de políticas se seguridad es por ello que la formación y concientización de los mismos es indispensable para lograr una implementación exitosa.
6. Muchas veces las empresas crecen de manera desordenada, crecen con paradigmas equivocados, algunos quieren documentar todo lo que se pueda, otras creen que documentar los procesos es una pérdida de tiempo. De lo anterior se concluye que la documentación de los procesos es una herramienta poderosa para el mantenimiento y mejora de cualquier plan de políticas propuestas para la seguridad se la información sensible que es el principal activo en cada empresa.

## VII. RECOMENDACIONES:

1. Se recomienda mantener una constante revisión de la política de seguridad y verificar el cumplimiento de la misma por parte de los empleados de la organización.
2. Se recomienda establecer los mecanismos que permitan la identificación de nuevos activos de información, y también la cultura organizacional para tomar acciones correctivas frente a nuevas vulnerabilidades, amenazas o riesgos detectados; y con base en esa información tomar acciones preventivas.
3. Se recomienda seguir con la utilización de una metodología para gestionar los riesgos; ya que, de esta manera se puede lograr una reducción en los riesgos a los cuales son sometidos los activos de información y también se puede hacer lo mismo para nuevos riesgos que aparezcan.
4. Se recomienda formar y capacitar de manera periódica al personal en temas de seguridad de la información y así lograr que todos los involucrados o relacionados con los activos de información tengan los alcances de la implementación claros.
5. Se recomienda la revisión periódica de la implementación de la política de seguridad para verificar si existen cambios en los requisitos legales que impacten las políticas de seguridad de la información.
6. Se recomienda realizar una documentación de procesos para poder gestionar los mismos de manera óptima y hacer frente a cualquier cambio que se pueda dar en la organización. La documentación de procesos también nos permite la mejora de estos.

REFERENCIAS BIBLIOGRÁFICAS


Demipc. (2016). *"Características de los microprocesadores". Consultado el 8 de Diciembre 2016.*
*http://informaciondemipc.blogspot.pe/2009/12/caracteristicas-de-los.html.*

*Huanca. (2014) "IMPLEMENTACIÓN DE UNA MEJORA CONTINUA PARA UNA LAVANDERÍA EN EL ÁREA DE LAVADO AL SECO". Consultado el 11 de Diciembre 2016*
*http://www.repositorioacademico.usmp.edu.pe/bitstream/usmp/1050/1/huanca_sk.pdf*

*Díaz Paúl, (2016). "Sistema integrado con servicios web que brinde soporte a los procesos de gestión de proyectos de la empresa desarrolladora de software TAU" (Tesis de pre grado). Pontificia Universidad Católica Del Perú. Perú. EcuRed, (2016) Consultado el 22 de diciembre del 2016, de https://www.ecured.cu/Informática*

*Estrada, A. (2004), "Protocolos Tcp/Ip De Internet". México.*

*Ghersi Sandra, (2016). "Adopción de herramienta para el soporte a la gestión del portafolio de proyectos de PROCAL-PROSER" (Tesis de pre grado). Pontificia Universidad Católica Del Perú. Perú.*

*Godoy Diego, Belloni Edgardo, Kotynski Henry, Dos Santos Héctor y Sosa Eduardo, (2014). "Simulando Proyectos de Desarrollo de Software Administrados con Scrum" (Artículo científico). Universidad Gaston Zachary, Argentina.*

*Grillo Luzmila y La Rosa Gina, (2009). "Sistema Administrador De Requerimientos Y Planificador De Tareas" (Tesis de pre grado). Pontificia Universidad Católica del Perú. Perú.*

*Huesca Gabriel, (2011). "Auditoría Informática". México.: Universidad Autónoma de Baja California.*

*Instituto Tecnológico de Sonora (2016 ). Consultado el 22 de diciembre del 2016, de http://biblioteca.itson.mx/oa/dip_ago/introduccion_sistemas/p3.htm*

Maigua Gustavo, (2012). "*Buenas prácticas en la Dirección y Gestión de Proyectos Informáticos".* Editorial de la Universidad Tecnológica Nacional. Argentina.

Marante María, (2009). "*Planificación y seguimiento en proyectos de desarrollo y mantenimiento de software dirigido por la gestión de tiempos"* (Tesis de pre grado). Universidad Politécnica de Valencia. España.

Mateu Carles, (2004). *"Desarrollo de Aplicaciones Web" (1era Edición)*. Editorial UOC. España.

Mejía Carlos (2014). "*Indicadores de Efectividad y Eficacia"*. Consultado el 28 de diciembre del 2016, de http://www.ceppia.com.co/Herramientas/INDICADORES/Indicadores-efectividad-eficacia.pdf

Palacio Juan, (2007). "*Flexibilidad con Scrum"*. España.

Palacio Juan, (2014). "*Gestión de Proyectos Scrum Manager"*. España.

Pérez Julián, (2008). "*Definición.DE"*. Consultado el 28 de diciembre del 2016, de http://www. http://definicion.de/costo/

Portal Administración de empresas (s.f), Consultado el 12 de diciembre del 2016, de http://admindeempresas.blogspot.pe/2007/07/reingenieria.html

Ramírez Robert, (2015). "*Métodos para el desarrollo de aplicaciones móviles"*. Editorial UOC. España.

Gonzáles Gómez, J. I., Morini Marrero, S., & Do Nascimento, E. (2002). *Control Y Gestión del Área Comercial y de Producción de la PYME Una Aplicación práctica con : SP Factura Plus SP TPVplus Elite 2003.* (C. Iglesias, Ed.) La Caruña, España: Netbiblo,S.L.

Heredia Viveros, N. L. (2013). *Gerencia de Compras la Nueva Estrategia Competitiva.* Bogota D.C, Colombia: Ecoe Ediciones.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2003). *Metodología de la Investigación* (Tercera ed.). (M.-H. Interamericana, Ed.) México, D.F., México: McGraw-Hill Interamericana.

Hurtado de Barrera, J. (2000). *Metodología de Investigación Holística* (Tercera Edición ed.). Caracas: Editorial SYPAL.

Joehnk, M. D. (2005). *Fundamentos de Inveriones.* (D. Fayeman Aragon, Ed.) Madrid, España: Pearson Educacion, S.A.

Lambert, D. M., & Stock, J. R. (2001). *STRETEGIC LOGISTICS MANAGEMENT* (3 ed.). (Irvin, Ed.) ISBN.

Lee J., K., & Larry P., R. (2000). *Administracion de Operaciones : Estrategia y Análisis* (Quinta Edición ed.). (M. De Anta, Ed.) Naucalpan de Juarez, Mexico: Pearson Educacion, S.A.

Méndez Álvarez, C. (2001). *Metodología Diseño y Desarrolo del Proceso de Investigación.* Bogota, Colombia: Faen.

Mora, F., & Schupnik, W. (19 de Noviembre de 2001). Recuperado el 02 de 12 de 2016, de http://www.gestiopolis.com/analisis-de-rentabilidad-en-mercadeo/

Pérez Gómez, R. (2010). *Tecnica Contable.* (E. Tebar, Ed.) Madrid, España: Editex, S.A.

Revista de Investigación y Negocio, A. (2015). *Todo Sobre Existencias.* Lima: Instituto Pacífico.

Sanchez Bellesta, J. P. (2002). *Analisis de Rentabilidad de la Empresa*. (En linea, Editor) Recuperado el 02 de 12 de 2016, de Google: http://ciberconta.unizar.es/leccion/anarenta/analisisR.pdf

Siliceo Aguilar, A. (2004). *Capacitacion y Desarrollo de Personal* (Tercera Edición ed.). Balderas, Mexico D.F.: Limusa Noriega Editores.

Villar Castillo, J. C. (2006). *ADMINISTRACIÓN LOGÍSTICA* (Vol. Programa Especial De Profesionalizacion en Ciencias Administrativas). Lima, Perú: Universidad Inca Garcilaso de la Vega.

# ANEXOS

## MATRIZ DE CONSISTENCIA – ANEXO N°01

| Problema | Objetivos | Hipótesis | Variables | Instrumento |
|---|---|---|---|---|
| **PROBLEMA GENERAL**<br><br>¿De qué manera influye una política de seguridad para la base de datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME? | **OBJETIVO GENERAL**<br><br>Proponer una política de seguridad para la base de datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME. | **HIPOTESIS GENERAL**<br><br>$H_i$: La propuesta de una política de seguridad influye positivamente en la base de datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME. | **INDEPENDIENTE**<br><br>Política de Seguridad | **METODO**<br>El método es metodológico cuantitativo |
| | | | **DIMENSIONES** | **TIPO DE INVESTIGACIÓN**<br>Explicativo |
| | | | **DEPENDIENTE**<br><br>Base de Datos | **DISEÑO DE INVESTIGACIÓN**<br>Diseño pre Experimental con Pre test y post test |
| **PROBLEMAS ESPECÍFICOS**<br><br>¿De qué manera influye la revisión de la configuración en la base de datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME?<br><br>¿De qué manera influyen las pruebas de penetración en la base de datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME? | **OBJETIVOS ESPECIFICOS**<br><br>Proponer la revisión de la configuración en la base de datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME.<br><br>Proponer las pruebas de penetración en la base de datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME. | **HIPÓTESIS ESPECÍFICAS**<br><br>$H_1$: La revisión de la configuración protege a la base de datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME.<br><br>$H_2$: Las pruebas de penetración protegen a la base de datos OSSAB del ambiente de producción en el Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME. | **DIMENSIONES**<br><br>Productividad | **POBLACIÓN Y MUESTRA**<br>20<br>Gc:20 |
| | | | | **INSTRUMENTOS**<br>Prueba Pre test y Pos test |

## MATRIZ OPERACIONAL – ANEXO N°02

| VARIABLES | DIMENSIÓN | INDICADORES | ITEMS | VALORES CATEGORIAS |
|---|---|---|---|---|
| **I.: POLITICAS DE SEGURIDAD PARA LA BASE DE DATOS EN PRODUCCION** | **I.1. Configuración** | **I.1.1. Método ABC** | 1 ¿Aplica y reactualiza guías de mejoras de políticas?<br>2 ¿Considera que la toma decisiones es a partir de la información que le brinda el área de tecnología? | Seguridad |
| | | **1.1.2. Servidor de base de datos** | 3 ¿Revisa, controla el Ingreso y Salida del acceso a la base de datos?<br>4 ¿Sabe usted cuantas tiempo dura la conexión de cada usuario a la Base de Datos? | Seguridad |
| | **I.2. Pruebas** | **I.2.1. Revisión Continua** | 5 ¿Se promueve la participación activa de los colaboradores para el correcto uso de la información registrada en la base de datos?<br>6 ¿Considera que el registro de los datos registrados a la base de datos debe ser revisada diario?<br>7 ¿El descuadre de los datos registrados es verificado por la persona indicada? | Seguridad |
| | | **I.2.2. Revisión periódica** | 8 ¿La información cada cierto periodo es consolidad y validada?<br>9 ¿Cada que tiempo realizan conteos o chequeos de los datos registrados a la base de datos? | Seguridad |
| | | **I.2.2. Control de información** | 10 ¿considera que la organización y ubicación de la base de datos es la correcta?<br>11 ¿Revisa y controla su información registrada usando el conteo físico de la documentación? | Seguridad |
| | **I.3. Seguridad** | **I.3.1 políticas por implementar** | 12 ¿La implementación de políticas es coordinado y aprobado por el área encargada?<br>13 ¿Los trámites para la implementación tienen una fecha tope? | Seguridad |
| | | **I.3.2 Tiempo de implementación** | 14 ¿Considera importante la implementación de políticas para la base de datos?<br>15 ¿Considera importante la seguridad de la base de datos? | Seguridad |

| | | | | |
|---|---|---|---|---|
| **D.: RENTABILIDAD** | **D.1. ANALISIS RENDIMIENTO** | **D.1.1. Patrimonio** | 16 ¿Los fondos aportados por el los usuarios militares genera ganancias?<br>17 ¿Las seguridad para la base de datos genera satisfacción a los aportantes? | Seguridad |
| | | **D.1.2. Seguridad** | 18 ¿Cree usted que se mide el rendimiento de la seguridad?<br>19 ¿La estructura organizacional posee un perfil según sus necesidades? | Seguridad |
| | | **D.1.3. Información** | 20 ¿El registro de la información es la correcta?<br>21 ¿las políticas están alineadas en relación con las necesidades de la arquitectura tecnológica? | Seguridad |
| | **D.2. RENDIMIENTO LABORAL** | **D.2.1. Eficacia** | 22 ¿Se estimula la seguridad y protección de la información en la empresa?<br>23 ¿Se Alienta y ayuda al personal o colaborador en la empresa? | Seguridad |
| | | **D.2.2. Eficiencia** | 24¿Cree usted que los colaboradores son proactivos, optimistas y positivos?<br>25 ¿Cree usted que la empresa cuenta con personal perseverante y Transformador? | Seguridad |

## Anexo N°03: Instrumentos

# UNIVERSIDAD PRIVADA TELESUP

**CARRERAS DE: Ingeniería de Sistemas e Informática**

**ENCUESTA SOBRE "Política de seguridad de Base de Datos para el ambiente productivo OSSAB , en la empresa Organismo Especial de Fondo de Vivienda Militar del Ejercito ORES-FOVIME 2018"**

La presente Encuesta tiene por objetivo recopilar información sobre el manejo del control de la información de la Base de Datos del ambiente de producción OSSAB de la empresa.

**EMPRESA: ……**

**RECOMENDACIÓN:**
**Lea los enunciados detenidamente y marque con una equis (X) en casillero por pregunta.**
**Cada número equivale a:**
**5 = Siempre**
**4 = Casi Siempre**
**3 = A Veces sí a Veces no**
**2 = Casi Nunca**
**1 = Nunca**

### I. POLITICA DE SEGURIDAD PARA BASE DE DATOS

**I.1. POLITICA DE SEGURIDAD**

| N° | | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|
| | **I.1.1. REVISION CONTINUA** | | | | | |
| 1 | ¿Revisa, controla el Ingreso y Salida del acceso a la información del ambiente productivo de la base de datos OSSAB? | | | | | |
| 2 | ¿Se promueve la participación activa de las Buenas Prácticas del acceso a datos? | | | | | |
| 3 | ¿Considera que debería controlarse el ingreso y salida de Usuarios al sistema? | | | | | |
| | **I.1.2.REVISION PERIODICA** | | | | | |
| 4 | ¿Considera que las actividades se monitorean por perfil de usuario? | | | | | |
| 5 | ¿La información cada cierto periodo es consolidada y validada? | | | | | |
| | **I.1.3.PRECISION** | | | | | |
| 6 | ¿Genera confianza los accesos externos al sistema del ORES-FOVIME? | | | | | |
| 7 | ¿Considera que la toma decisiones es a partir de la información que le brinda el área de sistemas? | | | | | |

**I.2. BASE DE DATOS**

| N° | | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|
| | **I.2.1. ROTACION DE USUARIOS** | | | | | |
| 8 | ¿Considera que la inmovilización equipos genera pérdidas? | | | | | |
| 9 | ¿Utiliza algún proceso para que la información se convierta con rapidez en Efectivo? | | | | | |
| 10 | ¿El área de sistemas se encarga de la seguridad de la información? | | | | | |
| | **I.2.2. DURACIÒN** | | | | | |
| 11 | ¿Tiene alguna idea de cuánto tiempo dura un usuario externo conectado a la base de datos OSSAB? | | | | | |
| 12 | ¿Revisa minuciosamente la información que ingresa diariamente al sistema? | | | | | |
| 13 | ¿Cada cuánto tiempo realiza el cambio de su contraseña de acceso al sistema? | | | | | |
| | **I.2.3. EXACTITUD** | | | | | |
| 14 | ¿Considera como un activo esencial la información que está sujeto a amenazas y vulnerabilidades? | | | | | |
| 15 | ¿En la cláusula de su contrato existe un compromiso por parte de la institución de proteger su usuario y clave de acceso al sistema? | | | | | |

## 2. SEGURIDAD

**II.1. ANALISIS DE LA BASE DE DATOS**

| N° | | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|
| | **II.2.1. MECANISMOS** | | | | | |
| **16** | ¿Existe un mecanismo que tú conoces sobre los accesos de los visitantes de la Institución registrando la fecha y hora de entrada y salida de los mismos? | | | | | |
| **17** | ¿Realiza con frecuencia copias de seguridad de la base de datos OSSAB? | | | | | |
| | **II.2.2. COMPROMISO** | | | | | |
| **18** | ¿Has firmado un documento para mantener confidenciales las claves secretas de los sistemas de información que maneja? | | | | | |
| **19** | ¿Ha recibido capacitación en seguridad de la información en la institución? | | | | | |
| | **II.2.3. POLITICAS** | | | | | |
| **20** | ¿Conoce sobre política de seguridad de Base de Datos? | | | | | |
| **21** | ¿Conoce sobre el cumplimiento obligatorio del acceso al sistema? | | | | | |

**II.2. RENDIMIENTO BASE DE DATOS**

| N° | | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|
| | **II.3.1. RENDIMIENTO** | | | | | |
| **22** | ¿Se estimula el rendimiento y producción en la empresa? | | | | | |
| **23** | ¿Se Alienta y ayuda al personal o colaborador en la empresa? | | | | | |
| | **II.3.2. INFORMACION** | | | | | |
| **24** | ¿Cree usted que los colaboradores son proactivos, optimistas y positivos? | | | | | |
| **25** | ¿Cree usted que el área de sistemas del ORES-FOVIME se encarga de la seguridad de la información? | | | | | |

**MUCHAS GRACIAS**

## Anexo N° 04: Matriz e Instrumentos

**VALIDEZ DEL CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE INDEPENDIENTE: POLITICA DE SEGURIDAD PARA LA BASE DE DATOS OSSAB.**

| | Dimensiones / ítems | Pertine | | Relevanci | | Claridad | | Sugerencia |
|---|---|---|---|---|---|---|---|---|
| | I.POLTICA DE SEGURIDAD PARA LA BASE DE DATOS OSSAB | Si | No | Si | No | Si | No | |
| 1 | ¿Revisa, controla el Ingreso y Salida del acceso a la información del ambiente productivo de la base de datos | X | | X | | X | | |
| 2 | ¿Se promueve la participación activa de las Buenas Prácticas del acceso a datos? | X | | X | | X | | |
| 3 | ¿Considera que debería controlarse el ingreso y salida de Usuarios al sistema? | X | | X | | X | | |
| 4 | ¿Considera que las actividades se monitorean por perfil de usuario? | X | | X | | X | | |
| 5 | ¿La información cada cierto periodo es consolidada y validada? | X | | X | | X | | |
| 6 | ¿Genera confianza los accesos externos al sistema del ORES-FOVIME? | X | | X | | X | | |
| 7 | ¿Considera que la toma decisiones es a partir de la información que le brinda el área de sistemas? | X | | X | | X | | |
| 8 | ¿Considera que la inmovilización equipos genera pérdidas? | X | | X | | X | | |
| 9 | ¿Utiliza algún proceso para que la información se convierta con rapidez en Efectivo? | X | | X | | X | | |
| 10 | ¿El área de sistemas se encarga de la seguridad de la información? | X | | X | | X | | |
| 11 | ¿Tiene alguna idea de cuánto tiempo dura un usuario externo conectado a la base de datos OSSAB? | X | | X | | X | | |
| 12 | ¿Revisa minuciosamente la información que ingresa diariamente al sistema? | X | | X | | X | | |
| 13 | ¿Cada cuánto tiempo realiza el cambio de su contraseña de acceso al sistema? | X | | X | | X | | |
| 14 | ¿Considera como un activo esencial la información que está sujeto a amenazas y vulnerabilidades? | X | | X | | X | | |
| 15 | ¿En la cláusula de su contrato existe un compromiso por parte de la institución de proteger su usuario y clave de acceso al sistema? | X | | X | | X | | |

| | II.SEGURIDAD | Si | No | Si | No | Si | No | |
|---|---|---|---|---|---|---|---|---|
| 1 | ¿Los controles en la base de datos generan seguridad? | X | | X | | X | | |
| 2 | ¿la política de seguridad genera restricción para los datos ingresados? | X | | X | | X | | |
| 3 | ¿Cree usted que se controla ingreso y salida de los usuarios a la base de datos? | **X** | | **X** | | **X** | | |
| 4 | ¿La estructura organizacional posee un perfil según sus funciones? | X | | X | | X | | |
| 5 | ¿La política de seguridad está produciendo un control de usuarios de acceso a la base de datos? | X | | X | | X | | |
| 6 | ¿Los controles de la política en relación con las configuraciones actuales reducen riesgos en el acceso a la información de la Base de Datos OSSAB? | X | | X | | X | | |
| 7 | ¿Se Controla el ingreso y salida a la Base de Datos? | X | | X | | X | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **8** | ¿Se Influye y apoya al personal o participante en la empresa? | X | | X | | X | | |
| **9** | ¿Cree usted que los usuarios son proactivos, optimistas y positivos? | X | | X | | X | | |
| **10** | ¿Cree usted que la empresa cuenta con personal firme y convertidor? | X | | X | | X | | |

**Observaciones (precisar si hay suficiencia):_____**

**Opinión de aplicabilidad: Aplicable [ X ] Aplicable después de corregir [ ] No aplicable [ ]**

**Apellidos y nombres del juez validador. Dr/ Mg: Ing. Denis Christian Ovalle Paulino**

**DNI: 40234321**

**Especialidad del validador: DOCENTE METODOLOGO**

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

**Nota**: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Ing. Denis Christian Ovalle Paulino

10 de Marzo de 2017

**INSTRUMENTO QUE MIDE LA VARIABLE INDEPENDIENTE: POLITICA DE SEGURIDAD PARA LA BASE DE DATOS OSSAB.**

| | Dimensiones / ítems | Pertine | | Relevanci | | Claridad | | Sugerencia |
|---|---|---|---|---|---|---|---|---|
| | **I.POLTICA DE SEGURIDAD PARA LA BASE DE DATOS OSSAB** | **Si** | **No** | **Si** | **No** | **Si** | **No** | |
| 1 | ¿Revisa, controla el Ingreso y Salida del acceso a la información del ambiente productivo de la base de datos | X | | X | | X | | |
| 2 | ¿Se promueve la participación activa de las Buenas Prácticas del acceso a datos? | X | | X | | X | | |
| 3 | ¿Considera que debería controlarse el ingreso y salida de Usuarios al sistema? | X | | X | | X | | |
| 4 | ¿Considera que las actividades se monitorean por perfil de usuario? | X | | X | | X | | |
| 5 | ¿La información cada cierto periodo es consolidada y validada? | X | | X | | X | | |
| 6 | ¿Genera confianza los accesos externos al sistema del ORES-FOVIME? | X | | X | | X | | |
| 7 | ¿Considera que la toma decisiones es a partir de la información que le brinda el área de sistemas? | X | | X | | X | | |
| 8 | ¿Considera que la inmovilización equipos genera pérdidas? | X | | X | | X | | |
| 9 | ¿Utiliza algún proceso para que la información se convierta con rapidez en Efectivo? | X | | X | | X | | |
| 10 | ¿El área de sistemas se encarga de la seguridad de la información? | X | | X | | X | | |
| 11 | ¿Tiene alguna idea de cuánto tiempo dura un usuario externo conectado a la base de datos OSSAB? | X | | X | | X | | |
| 12 | ¿Revisa minuciosamente la información que ingresa diariamente al sistema? | X | | X | | X | | |
| 13 | ¿Cada cuánto tiempo realiza el cambio de su contraseña de acceso al sistema? | X | | X | | X | | |
| 14 | ¿Considera como un activo esencial la información que está sujeto a amenazas y vulnerabilidades? | X | | X | | X | | |
| 15 | ¿En la cláusula de su contrato existe un compromiso por parte de la institución de proteger su usuario y clave de acceso al sistema? | X | | X | | X | | |

| | **II.SEGURIDAD** | **Si** | **No** | **Si** | **No** | **Si** | **No** | |
|---|---|---|---|---|---|---|---|---|
| 1 | ¿Los controles en la base de datos generan seguridad? | X | | X | | X | | |
| 2 | ¿la política de seguridad genera restricción para los datos ingresados? | X | | X | | X | | |
| 3 | ¿Cree usted que se controla ingreso y salida de los usuarios a la base de datos? | **X** | | **X** | | **X** | | |
| 4 | ¿La estructura organizacional posee un perfil según sus funciones? | X | | X | | X | | |
| 5 | ¿La política de seguridad está produciendo un control de usuarios de acceso a la base de datos? | X | | X | | X | | |
| 6 | ¿Los controles de la política en relación con las configuraciones actuales reducen riesgos en el acceso a la información de la Base de Datos OSSAB? | X | | X | | X | | |
| 7 | ¿Se Controla el ingreso y salida a la Base de Datos? | X | | X | | X | | |
| 8 | ¿Se Influye y apoya al personal o participante en la empresa? | X | | X | | X | | |
| 9 | ¿Cree usted que los usuarios son proactivos, optimistas y positivos? | X | | X | | X | | |
| 10 | ¿Cree usted que la empresa cuenta con personal firme y convertidor? | X | | X | | X | | |

**Observaciones (precisar si hay suficiencia):**

**SI EXISTE SUFICIENCIA**

**Opinión de aplicabilidad:** **Aplicable [ X ]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

**Apellidos y nombres del juez evaluador: Mg. MIGUEL DE PRIEGO CARBAJAL, VICTOR MANUEL**

**DNI: 06722070**

**Especialidad del evaluador: DOCENTE TEMÁTICO**

**Mg. Miguel de Priego Carbajal, Victor**

**13 de Febrero.del 2017**

[1] **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
[2] **Pertinencia:** Si el ítem pertenece a la dimensión.
[3] **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
**Nota:** Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

# ANEXO Nº05

| MATRIZ DE DATOS | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| "POLITICA DE SEGURIDAD DE LA BASE DE DATOS OSSAB Y SU INFLUENCIA EN LA SEGURIDAD DE LA INFROMACION DEL ORES FOVIME 2006" | | | | | | | | | | | | | | | | | | | | | | | | | |
| N° de Encuestados | VARIABLE INDEPENDIENTE | | | | | | | | | | | | | | | VARIABLE DEPENDIENTE | | | | | | | | | |
| | p1 | p2 | p3 | p4 | p5 | p6 | p7 | p8 | p9 | p10 | p11 | p12 | p13 | p14 | p15 | p16 | p17 | p18 | p19 | p20 | p21 | p22 | p23 | p24 | p25 |
| 1 | 3 | 5 | 3 | 3 | 5 | 3 | 3 | 3 | 2 | 3 | 4 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 4 | 3 | 4 | 3 | 3 |
| 2 | 4 | 3 | 5 | 2 | 3 | 2 | 3 | 5 | 3 | 3 | 3 | 2 | 4 | 3 | 3 | 3 | 1 | 2 | 2 | 3 | 3 | 3 | 3 | 3 | 3 |
| 3 | 5 | 3 | 5 | 3 | 2 | 3 | 2 | 5 | 3 | 4 | 3 | 2 | 4 | 3 | 3 | 3 | 1 | 2 | 3 | 2 | 3 | 1 | 3 | 3 | 3 |
| 4 | 4 | 5 | 4 | 3 | 4 | 3 | 3 | 4 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 1 | 1 | 1 | 1 | 1 | 3 | 1 | 3 | 4 |
| 5 | 4 | 3 | 5 | 3 | 3 | 3 | 5 | 4 | 3 | 4 | 3 | 2 | 2 | 3 | 3 | 3 | 1 | 2 | 3 | 5 | 3 | 1 | 1 | 3 | 3 |
| 6 | 4 | 3 | 5 | 2 | 3 | 3 | 3 | 5 | 3 | 4 | 5 | 2 | 4 | 3 | 3 | 4 | 5 | 2 | 3 | 3 | 3 | 3 | 2 | 3 | 3 |
| 7 | 3 | 3 | 3 | 4 | 3 | 2 | 3 | 3 | 2 | 3 | 4 | 2 | 3 | 2 | 3 | 4 | 5 | 2 | 3 | 1 | 3 | 3 | 3 | 2 | 4 |
| 8 | 2 | 3 | 3 | 2 | 3 | 3 | 3 | 5 | 3 | 3 | 5 | 2 | 5 | 3 | 3 | 4 | 4 | 3 | 3 | 5 | 3 | 3 | 3 | 3 | 3 |
| 9 | 4 | 5 | 3 | 3 | 2 | 3 | 3 | 3 | 2 | 3 | 4 | 2 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 4 | 3 | 4 | 3 | 3 |
| 10 | 3 | 5 | 3 | 3 | 5 | 3 | 3 | 5 | 1 | 3 | 3 | 2 | 4 | 3 | 3 | 3 | 1 | 2 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 11 | 4 | 3 | 5 | 2 | 3 | 2 | 2 | 5 | 1 | 4 | 3 | 2 | 4 | 3 | 4 | 3 | 1 | 2 | 3 | 2 | 3 | 1 | 3 | 3 | 3 |
| 12 | 5 | 3 | 5 | 3 | 2 | 3 | 3 | 4 | 3 | 3 | 3 | 3 | 3 | 3 | 4 | 3 | 1 | 1 | 1 | 1 | 1 | 3 | 1 | 3 | 4 |
| 13 | 4 | 5 | 4 | 3 | 4 | 3 | 5 | 4 | 3 | 4 | 3 | 2 | 2 | 3 | 3 | 3 | 1 | 2 | 3 | 5 | 3 | 1 | 1 | 3 | 3 |
| 14 | 4 | 3 | 5 | 3 | 3 | 3 | 3 | 5 | 1 | 4 | 5 | 2 | 4 | 3 | 3 | 4 | 5 | 2 | 3 | 3 | 3 | 3 | 2 | 3 | 3 |
| 15 | 4 | 3 | 5 | 4 | 3 | 3 | 3 | 3 | 2 | 3 | 4 | 2 | 3 | 2 | 4 | 4 | 5 | 2 | 3 | 1 | 3 | 3 | 3 | 2 | 4 |
| 16 | 3 | 3 | 3 | 2 | 3 | 2 | 3 | 5 | 1 | 3 | 5 | 2 | 5 | 3 | 3 | 4 | 4 | 3 | 3 | 5 | 3 | 3 | 3 | 3 | 3 |
| 17 | 2 | 3 | 3 | 2 | 3 | 3 | 5 | 4 | 3 | 4 | 3 | 2 | 3 | 3 | 4 | 3 | 1 | 2 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 18 | 4 | 5 | 1 | 2 | 3 | 4 | 3 | 4 | 3 | 3 | 3 | 3 | 2 | 3 | 4 | 3 | 1 | 2 | 3 | 2 | 3 | 1 | 3 | 3 | 3 |
| 19 | 4 | 3 | 1 | 4 | 3 | 2 | 3 | 5 | 1 | 4 | 3 | 2 | 4 | 3 | 4 | 3 | 1 | 1 | 1 | 1 | 1 | 3 | 1 | 3 | 4 |
| 20 | 3 | 3 | 5 | 2 | 3 | 5 | 3 | 3 | 2 | 4 | 5 | 2 | 3 | 3 | 3 | 3 | 1 | 2 | 3 | 5 | 3 | 1 | 1 | 3 | 3 |
| 21 | 4 | 5 | 3 | 2 | 3 | 2 | 5 | 5 | 1 | 3 | 4 | 2 | 5 | 3 | 3 | 4 | 5 | 2 | 3 | 3 | 3 | 3 | 2 | 3 | 3 |
| 22 | 4 | 3 | 3 | 4 | 3 | 5 | 3 | 5 | 2 | 3 | 5 | 2 | 3 | 2 | 4 | 4 | 5 | 2 | 3 | 1 | 3 | 3 | 3 | 2 | 4 |
| 23 | 4 | 3 | 5 | 4 | 3 | 3 | 3 | 3 | 2 | 3 | 4 | 2 | 3 | 2 | 4 | 4 | 5 | 2 | 3 | 1 | 3 | 3 | 3 | 2 | 4 |
| 24 | 3 | 3 | 3 | 2 | 3 | 2 | 3 | 5 | 1 | 3 | 5 | 2 | 5 | 3 | 3 | 4 | 4 | 3 | 3 | 5 | 3 | 3 | 3 | 3 | 3 |
| 25 | 2 | 3 | 3 | 2 | 3 | 3 | 5 | 4 | 3 | 4 | 3 | 2 | 3 | 3 | 4 | 3 | 1 | 2 | 3 | 3 | 3 | 3 | 3 | 3 | 3 |
| 26 | 4 | 5 | 1 | 2 | 3 | 4 | 3 | 4 | 3 | 3 | 3 | 3 | 2 | 3 | 4 | 3 | 1 | 2 | 3 | 2 | 3 | 1 | 3 | 3 | 3 |
| 27 | 4 | 3 | 1 | 4 | 3 | 2 | 3 | 5 | 1 | 4 | 3 | 2 | 4 | 3 | 4 | 3 | 1 | 1 | 1 | 1 | 1 | 3 | 1 | 3 | 4 |
| 28 | 3 | 3 | 5 | 2 | 3 | 5 | 3 | 3 | 2 | 4 | 5 | 2 | 3 | 3 | 3 | 3 | 1 | 2 | 3 | 5 | 3 | 1 | 1 | 3 | 3 |
| 29 | 4 | 5 | 3 | 2 | 3 | 2 | 5 | 5 | 1 | 3 | 4 | 2 | 5 | 3 | 3 | 4 | 5 | 2 | 3 | 3 | 3 | 3 | 2 | 3 | 3 |
| 30 | 4 | 3 | 3 | 4 | 3 | 5 | 3 | 5 | 2 | 3 | 5 | 2 | 3 | 2 | 4 | 4 | 5 | 2 | 3 | 1 | 3 | 3 | 3 | 2 | 4 |

**Plan de Políticas de seguridad para la base de datos OSSAB – ANEXO Nª 06**

# POLITICA

## Política de Seguridad de la Información

**Versión 1.0**

Marzo 2017

**DOCUMENTO EXCLUSIVAMENTE DE USO INTERNO**

## Introducción

Las Políticas de Seguridad identifican responsabilidades y establecen los objetivos para una protección apropiada y consistente de los activos de información de la entidad.

**¿Qué es Seguridad de la Información?**
Es la protección de la información de una amplia gama de amenazas para asegurar la continuidad de la entidad, minimizar el riesgo para la misma y maximizar el retorno de inversión y de oportunidades.

La Información es un activo que, como otros activos importantes de la entidad, tiene valor para la organización y requiere como consecuencia una protección adecuada. Esto es muy importante en el creciente ambiente de interconectividad, y como resultado de este crecimiento la información está expuesta a un mayor rango de amenazas y vulnerabilidades.

**¿Por qué es necesaria la Seguridad de la Información?**
Las organizaciones y sus sistemas de información se enfrentan cada vez más con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

Cabe destacar que esta Política de Seguridad de la Información está fundamentada en un riguroso análisis de riegos realizada a medida para el Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME, explicado más adelante en el punto 6.2 del presente documento.

**Objetivos globales para establecer la seguridad de la información en el ORES-FOVIME**
La implementación de las políticas busca reducir el riesgo de que en forma accidental o intencional se divulgue, modifique, destruya o se use en forma indebida los activos de información. Al mismo tiempo las políticas ayudan a las áreas responsables de la administración de seguridad orientar y mejorar la administración de seguridad de los activos de información y proveer las bases para el monitoreo a través de toda la entidad.

1. **Objetivo de la Alta Dirección del ORES-FOVIME como soporte a los principios de la seguridad de la Información**
   La Alta Dirección del ORES-FOVIME tiene como objetivo mantener un esquema de seguridad que permita asegurar constantemente la confidencialidad, integridad y disponibilidad de su información, siendo ésta,

su activo más valioso. Para ello la entidad desea que todo el personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, temporales y terceras partes u otros) que brindan servicios a la misma, conozcan, participen y cumplan con los lineamientos, políticas, procedimientos y demás directivas estipuladas en el Sistema de Gestión de Seguridad de la Información (SGSI) diseñados e implementados para tal fin.

## 2. Alcances

La importancia de estas políticas es que están orientadas a garantizar el uso apropiado de los dispositivos tecnológicos (computadores de escritorio, portátiles, etc.) y de los demás servicios (Internet, Correo Electrónico, etc), brindando a todo el personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) que brindan servicios a la entidad, las pautas para la utilización apropiada de dichos recursos, permitiendo así minimizar los riesgos de una eventual pérdida de activos de información sensitivos para el Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME.

### 2.1. Alcance de la seguridad de la información

Para el Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME la seguridad de la información es aplicable a todos los activos de información durante su ciclo de vida.

Dicha seguridad está orientada a proteger los activos de información en todos los ambientes en los cuales ésta reside, y para asegurar los activos de información que residen en lugares externos (pe. Dependencias, proveedores de servicios, etc.), estos son sometidos a controles equivalentes para su protección.

### 2.2. Alcances de la Política de Seguridad de la Información

Estas Políticas aplican a todo el personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, temporales y

terceras partes u otros) que brindan servicios a la entidad, quienes están sujetos a los mismos requerimientos de seguridad, y tienen las mismas responsabilidades de seguridad de información que el personal de la entidad.

Todos están obligados a continuar protegiendo la información del Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME cumpliendo las políticas de seguridad después de terminar su relación con la entidad.

### 2.3. Cumplimiento y conformidad

El cumplimiento de las Políticas de Seguridad es obligatorio. Ninguna persona (funcionarios, servidores, CAS, locadores de servicios, personas naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) está exento del cumplimiento de estas políticas. Si un individuo u organización viola las siguientes disposiciones, por negligencia o intencionalmente, el Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME tomará las medidas correspondientes, tales como acciones administrativas, laborales, disciplinarias, legales, u otras.

## 3. Dominios de la Norma

**Política de Seguridad**: Constituye el presente documento, y es donde se estipulan las políticas con respecto a la seguridad de la Información para el Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME.

3.1. **Seguridad Organizacional**: Agrupa los temas de administración de la seguridad dentro de la entidad. (Roles, compromisos, autorizaciones, acuerdos, manejo con terceros)

3.2. **Administración de Activos de Información**: Habla del mantenimiento y protecciones apropiadas de todos los activos de información.

3.3. **Seguridad del Recurso Humano**: Temas para asegurar que todo el personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores,

contratistas, temporales o terceras partes u otros) entiendan sus responsabilidades y sean adecuados para los roles a desempeñar minimizando los riesgos relacionados con el recurso humano.

3.4. **Seguridad Física y Ambiental**: Hace referencia a prevenir accesos físicos no autorizados (perímetro), daños o interferencias a las instalaciones de la entidad y a su información.

## 4. Marco referencial

Los objetivos de control y la estructura de evaluación y gestión de riesgos fundamentan las políticas de seguridad de la información para la infraestructura tecnológica y de información del Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME.

### 4.1. Objetivos de control

#### 4.1.1. Protección de la información

Los activos de información serán protegidos con el nivel necesario en proporción a su valor y el riesgo de pérdida para la entidad. La protección debe acentuar la confidencialidad, integridad y disponibilidad de los activos de información.

#### 4.1.2. Protección de los recursos tecnológicos

Los recursos tecnológicos serán protegidos con el nivel necesario en proporción a su valor y el riesgo de pérdida para la entidad. Dichos recursos deben ser utilizados exclusivamente para desarrollar las actividades laborales establecidas para el personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) asegurando que su utilización se hará en forma adecuada, con el máximo de eficiencia y con ejemplar racionalidad.

#### 4.1.3. Autorización de usuarios

Todos los usuarios deben ser identificados independientemente con

permisos de acceso, específicamente e individualmente autorizados por razones básicas de operaciones. Los métodos de acceso de usuarios deben exigir un proceso robusto de autenticación, autorización apropiada y auditoría confiable.

4.1.4. **Responsabilidad**

Los usuarios y custodios de los activos de información del Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME son responsables por el uso apropiado, protección y privacidad de estos activos. Los sistemas informáticos del Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME generarán y mantendrán unas apropiadas pistas de auditoría para identificar usuarios, y documentar los eventos relacionados con eventos de seguridad.

4.1.5. **Disponibilidad**

Los activos de información deben estar disponibles para soportar los objetivos del Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME. Deben tomarse medidas adecuadas para asegurar el tiempo de recuperación de toda la información y el acceso por personas autorizadas.

4.1.6. **Integridad**

Los activos de información deben estar adecuadamente protegidos para asegurar su integridad y precisión. Las medidas de validación definidas permitirán detectar la modificación inapropiada, eliminación o adulteración de los activos de información.

4.1.7. **Confidencialidad**

Los activos de información deben mantenerse protegidos para asegurar su confidencialidad entre los usuarios autorizados para acceder a los mismos.

4.1.8. **Confianza**

Todo el personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) deben demostrar capacidad para reunir o exceder los requerimientos de seguridad del Organismo Especial del Fondo de Vivienda Militar del

Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME son compartidos con otras personas.

4.1.9. **Esfuerzo de Equipo**

Para que logre ser efectiva, la seguridad de la información debe ser un esfuerzo de equipo donde deben participar en forma activa todo el personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) que tengan interacción con la información o los sistemas de información de la entidad. Todos deben cumplir con las políticas de seguridad de información y más que eso, desempeñar un papel proactivo para su protección y divulgación de estas políticas.

4.1.10. **Soporte primario para la Seguridad de la Información**

El Oficial de Seguridad de la Información debe facilitar la administración y desarrollo de iniciativas sobre seguridad de información. El Oficial de Seguridad de la Información deberá proveer dirección y experiencia técnica para asegurar que la información del Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME se encuentre protegida

**5. Revisiones de seguridad en sistemas de Información**

En forma periódica el Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME debe efectuar las pruebas necesarias para evaluar el cumplimiento de las diferentes políticas de seguridad, lo mismo que para verificar el cumplimiento de los estándares de configuración en las diferentes plataformas técnicas e instalaciones de tecnología de información. Esta tarea será realizada por el Oficial de Seguridad de la Información o el responsable en la Unidad de Tecnología de la Información, según el caso.

**5.1. Propiedad de la información**

La información que es soportada por la infraestructura de tecnología informática del Organismo Especial del Fondo de Vivienda Militar del

Ejercito ORES-FOVIME pertenece a la entidad a menos que en una relación contractual se establezca lo contrario. Sin embargo, la facultad de otorgar acceso a la información es del responsable del área que genera esa información.

La información propiedad del Organismo Especial del Fondo de Vivienda Militar del Ejército ORES-FOVIME y sobre la cual tiene sus derechos, podrá ser suministrada a los entes de control pertinentes, cuando estos lo requieran, con previa autorización expresa y aprobada por los directivos de la entidad para estos fines.

Para efectos de control del flujo de la información de los procesos de la entidad, se asignarán responsables de la información, quienes deben asegurar y otorgar acceso a la información que genere su área, con el fin de lograr un adecuado ambiente de control y un buen nivel de segregación de funciones.

En caso de divulgación no autorizada de la información de propiedad del Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME, se realizarán las investigaciones pertinentes para establecer sanciones, las cuales serán evaluadas con el jefe inmediato del usuario involucrado y el Comité de Seguridad para lo cual utilizarán el concepto emitido por el Oficial de Seguridad de la Información sobre el hecho y su impacto en la entidad.

## 5.2. Estructura de evaluación y gestión de riesgos

### 5.2.1. La estructura de evaluación de riesgo

Se fundamenta en el principio de identificación de los procesos organizacionales críticos para el funcionamiento del Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME, y consiste en la separación e identificación de los activos de información que soportan dichos procesos sobre los cuales se determina un nivel de seguridad correspondiente a lo analizado en el momento de la evaluación.

Del resultado de ese análisis se ha creado y diseñado la presente Política de Seguridad de la Información.

5.2.2. **La gestión del riesgo**

Es una tarea que debe realizarse constantemente actualizando los mapas o niveles de riesgo cada vez que se cumpla un ciclo del SGSI o al presentarse un cambio importante en los sistemas de información críticos.

El Oficial de Seguridad de la Información se encargará de coordinar todas las tareas necesarias para la gestión del riesgo

## 6. Políticas

Estas Políticas cuentan con el apoyo de un Sistema de Gestión de Seguridad de la Información (SGSI), integrado entre otros, por normas, procedimientos y formatos los cuales están en constante revisión y actualización por cada ciclo del SGSI.

### *6.1. Política de Seguridad*

La Política de Seguridad de la Información (expresada en éste documento) especifica las pautas que deben ser cumplidas por parte de todo el personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros), con el fin de asegurar un adecuado nivel de confidencialidad, integridad y disponibilidad en su información.

### *6.2. Seguridad Organizacional*

6.2.1. **Oficial de Seguridad de la Información**

El Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME mantendrá dentro de su organización un Oficial de Seguridad de la Información, cuyas funciones estarán caracterizadas y definidas según la necesidad de la entidad.

### 6.2.2. Comité de Seguridad

Se establece el Comité de Seguridad, como el ente dentro de la entidad para atender los temas en materia de Seguridad de la Información que requieran de una definición o aprobación.

Además este Comité debe conocer y aprobar los planes de Seguridad de la Información. Cuando el Comité de Seguridad se reúna con el propósito de revisar temas de seguridad de la información se incluirá la participación del Oficial de Seguridad de la Información.

6.2.2. **Grupo de Seguridad Interdisciplinario**

El Oficial de Seguridad de la Información podrá convocar a diferente personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) para formar grupos interdisciplinarios que apoyen la definición e implementación de los diferentes temas de seguridad de la información.

6.2.3. **Coordinación de la seguridad**

El Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME deberá contar con un Oficial de Seguridad de la Información que asuma las tareas y responsabilidades que conlleva este rol, y que se expresan en el documento referido a Responsabilidades de la Gestión de la Seguridad.

6.2.4. **Seguridad con Terceros**

a) Todas las conexiones de personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) a la red interna del Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME, deben ser autorizadas, revisadas y monitoreadas por la Unidad de Tecnología de la Información, según sus requerimientos

b) Los contratos de desarrollo o mantenimiento de Software que se suscriban con personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros), deberán incluir el acuerdo para cumplir las políticas de seguridad de la Información establecidas por la entidad.

c. Además, los contratos para los cuales se transfiere la responsabilidad por la seguridad de la información a un tercero (o outsorcing), deben dejar en forma explícita el compromiso por parte de este, de la aplicación de los controles de seguridad necesarios en la medida en que el Organismo

6.2.5. **Acuerdos de Seguridad**

Todo el personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) y personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) que deban realizar labores dentro de la entidad, cuya labor involucre el manejo de información de la entidad ya sea por medios lógicos o físicos; deben conocer, entender, firmar y aceptar el correspondiente acuerdo de confidencialidad que para su caso aplique y que se expresa en los documentos: Acuerdo de Confidencialidad y usos de TI (para personal del ORES-FOVIME) y el Acuerdo de Confidencialidad – Terceros (para las otras personas).

Todas estas personas están obligadas a continuar protegiendo la información del cumpliendo las políticas de seguridad después de terminar su relación con la entidad.

6.2.6. **Responsabilidad por la información**

a) Cada conjunto de datos tendrá un usuario dueño y responsable de los datos que están en producción. Donde se entiende por dueño de la información al usuario que trabaja con la información y como responsable de la información al Director del área donde ésta se genera.

b) Es responsabilidad de la Unidad de Tecnología de la Información, mantener segura la información sistematizada de la entidad.

### 6.2.7. Segregación de Funciones

El MINISTERIO DE AGRICULTURA DEL PERÚ debe asegurar que los procesos se desarrollen a través de una correcta segregación de funciones que permita garantizar que la ejecución, la revisión, la autorización y el seguimiento se dan a diferentes niveles.

## 7. Administración de Activos de Información

### 7.1. Inventario de Activos

a) El MINISTERIO DE AGRICULTURA DEL PERÚ mantendrá todos sus activos de información referenciados e inventariados, y constantemente actualizará esta documentación.

b) Toda adquisición de cualquier naturaleza que haga la entidad en materia de hardware, software, servicios en temas informáticos e información debe tener un control a través de la Unidad de Tecnología de la Información.

c) Se debe realizar un control de todo hardware y software que sea recibido, en cuanto a su ubicación y protección, desde que se adquieren o arriendan, hasta su retiro de uso.

### 7.2. Clasificación de la información

a) Cada activo de información propiedad del MINISTERIO DE AGRICULTURA DEL PERÚ, debe estar asignado a un personal de la entidad (funcionarios, servidores, CAS, locadores de servicios y otros) quien se responsabilizará por el mismo.

b) Toda la información utilizada por el MINISTERIO DE AGRICULTURA DEL PERÚ y su personal (funcionarios, servidores, CAS, locadores de servicios y otros), debe ser clasificada y administrada de acuerdo a los niveles establecidos por la entidad y que se expresan en el documento referido a la Clasificación de la Información.

### 7.3. Seguridad del Recurso Humano

#### 7.3.1. Responsabilidades de los usuarios

a) Todo personal nuevo del MINAG (funcionarios, servidores, CAS, locadores de servicios y otros), que hayan aprobado los procesos de selección, deberán conocer, entender y asumir sus responsabilidades con respecto a la seguridad de la información, según el rol a desempeñar. Igualmente es responsabilidad de todo personal vinculado a la entidad con anterioridad a la elaboración de este documento, conocer, entender y asumir sus responsabilidades con respecto a la seguridad de la información, según el rol a desempeñar.

b) El incumplimiento de esta Política de Seguridad de la Información así como las normas, procedimientos y formatos que regulan el SGSI que conlleve a un incidente de seguridad, implicará un proceso disciplinario y/o las acciones legales correspondientes, dentro del marco legal vigente, por parte de la entidad para establecer la responsabilidad del usuario involucrado.

c) El término del contrato de trabajo con el MINISTERIO DE AGRICULTURA DEL PERÚ implica el cumplimiento de los procesos de entrega de activos de información y remoción de privilegios sobre la plataforma tecnológica de la entidad.

d) Todos los usuarios deben conocer y dar cumplimiento al manual de uso de la tecnología (uso del correo, uso de las impresoras, navegación en Internet, etc.) establecido por la Unidad de Tecnología de la Información del MINAG.

7.2.1. **Entrenamiento**

Todo el personal del MINAG (funcionarios, servidores, CAS, locadores de servicios y otros) será entrenado en los temas de seguridad necesarios para asegurar que se cumpla el esquema de seguridad, evitando su incumplimiento debido a falta de capacitación o desconocimiento del SGSI.

## 8. Seguridad Física y Ambiental

### 8.1. Controles de acceso perimetral

a) Todo el personal del MINAG (funcionarios, servidores, CAS, locadores de servicios y otros) deberán portar constantemente y en un lado visible su fotocheck que lo identifica como personal de la entidad.
b) Todas las demás personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) que hagan su ingreso a las instalaciones de la entidad deberán estar adecuadamente identificadas y anunciar su llegada a través del personal de vigilancia de las instalaciones. Cualquier elemento que entre o salga de las diferentes unidades orgánicas del Ministerio debe ser anunciado al personal de vigilancia para que este proceda a hacer el registro correspondiente.
c) Las puertas de acceso a las áreas de manipulación o administración de información confidencial o privada, deberán permanecer cerradas en todo momento.
d) Para el ingreso o salida de cualquier elemento deberá diligenciarse el formato de autorización que tiene establecida la entidad con el registro completo de la información que allí se solicita.
e) Todas las personas que ingresen a las áreas restringidas de la entidad, deberán cumplir los controles establecidos para el acceso específico a dichas áreas.

### 7.3. Controles ambientales

a) El MINISTERIO DE AGRICULTURA DEL PERÚ proporcionará el ambiente adecuado para la conservación de medios magnéticos y equipos.
b) El MINISTERIO DE AGRICULTURA DEL PERÚ grabará en video las actividades en áreas públicas (dentro de los confines de la entidad), puertas de acceso a áreas restringidas y zonas de manipulación de información confidencial o privada, con el fin de mantener un control de seguridad.

c. El MINISTERIO DE AGRICULTURA DEL PERÚ mantendrá en condiciones óptimas de limpieza, seguridad, mantenimiento y funcionalidad de cada uno de los elementos que forman parte del centro de cómputo y para el resguardo de los backups de la información, de acuerdo con las recomendaciones que sobre cada uno provea el fabricante.

c) Todo el personal del MINAG (funcionarios, servidores, CAS, locadores de servicios y otros) que utilice estaciones de trabajo para la realización de su labor, deberán acoger como práctica permanente el bloqueo de la pantalla al ausentarse de su puesto, así como mantener en orden sus papeles de trabajo, siempre pensando en la confidencialidad de la información.

d) Las estaciones de trabajo de los usuarios finales serán desactivadas automáticamente si superan un tiempo de inactividad determinada en cada caso, según el nivel de riesgo que corresponda, siendo necesario digitar nuevamente la clave de acceso en el momento que requiera continuar con la conexión.

### 7.4. Mantenimiento

El MINISTERIO DE AGRICULTURA DEL PERÚ establecerá esquemas de mantenimiento para toda su plataforma tecnológica que deberá ser cumplido dentro de las fechas programadas.

Cuando un medio magnético, propiedad del MINISTERIO DE AGRICULTURA DEL PERÚ, termine su ciclo de vida, deberá ser destruido de acuerdo a las exigencias de la Unidad de Tecnología de la Información.

Al disponer de un disco duro utilizado, ya sea para su entrega o reutilización, deberá pasar por un proceso adecuado de borrado determinado por la Unidad de Tecnología de la Información.

### 7.5. Cintoteca

La entidad contará con una cintoteca adecuada y segura para la custodia de la información.

La Cintoteca deberá cumplir con la normatividad relacionada a seguridad de áreas de procesamiento de datos (áreas restringidas)

### 7.6. Centro de Cómputo

La Unidad de Tecnología de la Información debe establecer los mecanismos de seguridad necesarios para la correcta protección del Centro de Datos (o centro de cómputo), de manera que se mantenga la confidencialidad y seguridad de la información que se procesa, así como la integridad de los equipos.

El MINISTERIO DE AGRICULTURA DEL PERÚ mantendrá las condiciones físicas y ambientales óptimas recomendadas para centros de cómputo así como controles automáticos para incendio y temperatura (humedad, monitoreo por el CCTV, etc)

### 7.7. Áreas Restringidas

El MINISTERIO DE AGRICULTURA DEL PERÚ clasificará sitios (áreas) que por su actividad, activos, manejo transaccional, etc., se deban manejar en forma restringida teniendo controles de acceso y registro de visitantes. Se consideran dentro de éstas por ejemplo: El centro de cómputo y el gabinete de comunicaciones.

### 7.7.1. *Administración de comunicaciones y operaciones*

### 7.8. Documentación operativa

a) Todos los procedimientos operativos del MINISTERIO DE AGRICULTURA DEL PERÚ estarán adecuadamente documentados, mantenidos y a disposición de los usuarios a quienes compete.

b) Es responsabilidad de la Unidad de Tecnología de la Información, mantener debidamente actualizada toda la documentación referente a la plataforma tecnológica de la entidad.

### 7.9. Control de Cambios

Cualquier cambio a la plataforma tecnológica del MINISTERIO DE AGRICULTURA DEL PERÚ (a excepción de las estaciones de trabajo) deberá ser completamente documentado y controlado por la Unidad de Tecnología de la Información.

Todos los cambios en el ambiente de producción deberán ceñirse a las regulaciones establecidas para la adecuada puesta en producción, por la Unidad de Tecnología de la Información.

## 8. Uso de la Tecnología

a) La Unidad de Tecnología de la Información definirá los criterios de utilización de los servicios de tecnología y los estándares adecuados para la óptima administración de los recursos.

b) Los recursos informáticos del MINISTERIO DE AGRICULTURA DEL PERÚ deben ser utilizados únicamente para propósitos propios de la entidad. (Para mayor referencia consultar directivas internas).

### 8.1. Acceso remoto

La entidad proporcionará tecnologías de acceso remoto a todo el personal del MINAG (funcionarios, servidores, CAS, locadores de servicios y otros), previa evaluación y autorización del área correspondiente. La Unidad de Tecnología de la Información garantizará un adecuado esquema de seguridad para los mismos.

### 8.2. Separación de ambientes

El MINISTERIO DE AGRICULTURA DEL PERÚ mantendrá identificados, controlados y aislados sus ambientes de desarrollo, calidad y producción, aplicando para cada uno los procedimientos específicamente estipulados por la entidad, para su operación o administración.

### 8.3. Capacidad y Desempeño

La plataforma tecnológica del MINISTERIO DE AGRICULTURA DEL PERÚ será continuamente monitoreada con el fin de establecer niveles de capacidad y desempeño, empleando las herramientas adecuadas y manteniendo actualizada la debida documentación.

## 8.3. Servicios de red

a) El MINISTERIO DE AGRICULTURA DEL PERÚ mantendrá un constante monitoreo sobre la red interna, implementando las herramientas que le permitan detectar, prevenir y recuperarse del código malicioso encontrado en su plataforma tecnológica.

b) El MINISTERIO DE AGRICULTURA DEL PERÚ se reserva el derecho de examinar toda la información almacenada o transmitida por sus sistemas de cómputo y de comunicación, y debe informar a todo el personal del MINAG (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) que no deben esperar privacidad asociada con la información que ellos almacenan o envían a través de estos sistemas.

c) La entidad mantendrá actualizada y con la debida aprobación de la Unidad de Tecnología de la Información, una lista de las categorías de acceso NO permitido para la navegación en Internet. En todas las ocasiones los intereses, el buen nombre y la seguridad de la entidad deben ser protegidos por todo el personal del MINAG (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) que presentan servicios a la entidad.

## 8.4. Servicios WEB

La entidad vigilará el cumplimiento de los compromisos de seguridad de la página www.minag.gob.pe, a través de la revisión periódica de los informes de vulnerabilidades entregados a la entidad.

### 8.3. Software

La entidad efectuará constantes revisiones al cumplimiento de las normas en materia de propiedad intelectual.

Todo el personal del MINAG (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) tienen PROHIBIDO instalar o utilizar software o productos sin licencias autorizadas por la entidad. Se exceptúan de esta política los productos de software con licencia de libre utilización o que sean soportados con certificado de propiedad de licencia de terceros. En todo caso, cualquier instalación de software debe ser solicitada y obtenida a través de la Unidad de Tecnología de la Información.

### 8.5. Computación móvil

a) Los equipos de cómputo (sin importar su propietario) utilizados fuera del MINISTERIO DE AGRICULTURA DEL PERÚ y en funciones propias de la entidad, deben ser exclusivamente utilizados para brindar apoyo a las actividades de la entidad y deben ser sujetos a un grado equivalente de protección igual al de los equipos que se encuentran dentro de las instalaciones del MINISTERIO DE AGRICULTURA DEL PERÚ. Se deben aplicar las siguientes pautas:

- El uso de equipos portátiles asignados al personal del MINAG (funcionarios, servidores, CAS, locadores de servicios y otros) deben atenerse a todas las recomendaciones de seguridad y, adicionalmente, deberán seguir las instrucciones emitidas por la Unidad de Tecnología de la Información.
- Las computadoras personales, para conectarse a la red del Ministerio, previamente deben pasar por una verificación y autorización por parte de la Unidad de Tecnología de la Información.
- Durante los viajes, los equipos y medios magnéticos no deben dejarse desatendidos en lugares públicos. Las computadoras portátiles se deben llevar como equipaje de mano.

- Los equipos portátiles son vulnerables al robo, pérdida o acceso no autorizado durante los viajes. Se les deben proporcionar una forma apropiada de protección al acceso (Ej. Contraseñas de encendido, encriptación, etc.) con el fin de prevenir el acceso no autorizado.
- Las instrucciones del fabricante concernientes a la protección del equipo se deben seguir en todo momento (Ej.: para protegerse contra la exposición de campos electromagnéticos muy fuertes).

b) La utilización de elementos removibles de almacenamiento (Cintas con copias de respaldo, DVD's, memorias USB, CD's reescribibles, discos duros portátiles, etc.) por parte de los usuarios, deberá cumplir estrictamente los lineamientos establecidos por la Unidad de Tecnología de la Información mediante pautas recomendadas por parte del Oficial de Seguridad de la Información. La administración (custodia, reutilización y destrucción) adecuada de estos elementos, tanto para su conservación como la destrucción, cuando fuera necesario, estará determinada por los procedimientos establecidos en la Unidad de Tecnología de la Información.

c) El ingreso y/o salida de los equipos de cómputo y elementos removibles de almacenamiento (Cintas con copias de respaldo, DVD's, memorias USB, CD's reescribibles, discos duros portátiles, etc.), que SI pertenecen al MINISTERIO DE AGRICULTURA, deberá ser previamente autorizado por la Unidad de Tecnología de la Información y registrado por la Unidad de Logística y el Personal de Seguridad.

d) El ingreso y/o salida de los equipos de cómputo y elementos removibles de almacenamiento (Cintas con copias de respaldo, DVD's, memorias USB, CD's reescribibles, discos duros portátiles, etc.) que NO pertenecen al MINISTERIO DE AGRICULTURA, deberá ser previamente autorizado por la Unidad de Tecnología de la Información y registrado por el Personal de Seguridad.

**9. Backups**

Toda la información del MINISTERIO DE AGRICULTURA DEL PERÚ debe ser respaldada por medio de copias de seguridad siguiendo el procedimiento adecuado según el componente. Esto incluye la información de las estaciones de trabajo que cada responsable de área considere necesario, previa coordinación con el responsable de la Unidad de Tecnología de la Información para incluirlos en el procedimiento de backup.

a) Es responsabilidad de cada personal del MINAG (funcionarios, servidores, CAS, locadores de servicios y otros) ubicar en una unidad de red la información referida únicamente al MINISTERIO DE AGRICULTURA DEL PERÚ que requiera ser respaldada por la Unidad de Tecnología de la Información.
b) Ningún tipo de información referida al MINISTERIO DE AGRICULTURA DEL PERÚ puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo. Para estos casos, es responsabilidad de cada usuario replicar la información en los directorios públicos que residen en los servidores.
c) Deben existir al menos dos copias de la información, una de las cuales deberá permanecer fuera de las instalaciones de la entidad, con excepción de aquellos archivos que provienen de entidades externas, o que en razón de cambios en la tecnología, no puedan ser duplicados.
d) Es responsabilidad de la Unidad de Tecnología de la Información, definir los periodos de retención y la frecuencia de los Backups que garanticen la continuidad de las operaciones y la consulta histórica de su información.
e) Es responsabilidad de la Unidad de Tecnología de la Información el mantenimiento adecuado de las versiones de las aplicaciones en el medio de almacenamiento utilizado en su momento que le permita atender requerimientos legales o internos.

f) Toda restauración de datos en producción debe ser autorizada por la Unidad de Tecnología de la Información.

f) Es responsabilidad de cada unidad orgánica y del personal mantener depurada la información de sus archivos públicos, como mejor práctica para la optimización del uso de los recursos que entrega la entidad a su personal.

### 8.6. Control de código Malicioso

a) El Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME contará permanentemente con un sistema efectivo de antivirus que será administrado bajo la responsabilidad de la Unidad de Tecnología de la Información.

b) Los usuarios deberán cumplir con las mejores prácticas establecidas por el Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME con respecto al uso del Antivirus.

c) Es responsabilidad de todo el personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros), revisar que todos los medios magnéticos extraíbles sean chequeados con un antivirus provisto por la entidad antes de procesarlos en los computadores personales o servidores de la entidad.

d) Es responsabilidad de la Unidad de Tecnología de la Información, mantener en buen funcionamiento los sistemas que le permitan prevenir, detectar y corregir ingresos o intentos de ingresos no autorizados.

### 8.7. Revisión y monitoreo de Logs

El Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME realizará un monitoreo permanente de la red a través de los diferentes logs establecidos y configurados a conveniencia de la entidad. Estos logs serán revisados y analizados de acuerdo a las tareas programadas dentro de la Unidad de Tecnología de la Información.

8.8. **Responsabilidad Operativa**

a) Dentro del personal de la Unidad de Tecnología de la Información debe existir un responsable de la seguridad de los backups.
b) El Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME, a través de la Unidad de Tecnología de la Información se responsabilizará de la seguridad de la información en los equipos centrales de cómputo, quien adoptará las mejores prácticas en materia de control de acceso a la información de acuerdo a la tecnología usada.
c) El Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME, a través de la Unidad de Tecnología de la Información, asegurará la mejor selección (técnica) de los proveedores de servicios, para los elementos y equipos que forman parte del centro de cómputo.
d) Es responsabilidad de la Unidad de Tecnología de la Información brindar la información al ente regulador de la entidad sobre las actividades de desarrollo y mantenimiento de los aplicativos, y es potestativo del ente de control su participación en los grupos de trabajo.

**8.8. Telefonía**

La entidad contará con el servicio telefónico local, nacional, internacional y de celulares, con lo cual autorizará su uso de manera particular a todo el personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) y a personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) que lo requieran según sus funciones.

8.8.1. ***Control de Acceso***

**8.9. Administración de usuarios**

a) Las cuentas que no hayan sido utilizadas en los últimos noventa días deben ser eliminadas o inhabilitadas dependiendo del caso.

b) Está prohibido intentar ingresar a los servicios de cómputo y comunicaciones con la cuenta de otro personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) o de otras personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros).

d) La Unidad de Tecnología de la Información del Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME definirá el esquema de usuarios para la administración y uso de cada plataforma tecnológica, utilizando los criterios de mínimo riesgo e impacto para la entidad.

e) El nivel de acceso debe ser definido por funciones específicas dentro de cada aplicación y para cada usuario.

f) Cada personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) tendrá un código único de identificación ante el sistema y será responsable de todo registro a su nombre.

g) La creación, eliminación y revisión de privilegios de los usuarios de la red y las aplicaciones del Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME deberán ser regularmente revisados según las actividades programadas de la Unidad de Tecnología de la Información.

h) El Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME clasificará las cuentas de usuario de acuerdo a los niveles de acceso autorizados y requeridos para la operación o administración de los sistemas de la entidad.

i) Las unidades correspondientes deberán enviar mensualmente a la Unidad de Tecnología de la Información, la lista actualizada de altas, bajas, vacaciones, incapacidades, licencias, consultorías, servicios, etc. de todo el personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas,

consultores, contratistas, temporales o terceras partes u otros), a fin de llevar un control de las cuentas de usuario correspondientes según sea el caso.

### 8.10. Contraseñas

a) Cada personal del ORES-FOVIME funcionarios, servidores, CAS, locadores de servicios y otros) debe tener asociada una contraseña que cumpla con las características de contraseñas seguras referida en el documento Administración de Contraseñas de Usuarios. No está permitido que las demás personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) utilicen contraseñas asignadas al personal de la entidad.

b) El Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME mantendrá definido para todos sus sistemas de información un esquema de construcción de contraseñas fuertes que debe ser cumplida por todo el personal del MINAG (funcionarios, servidores, CAS, locadores de servicios y otros).

c) Las contraseñas deberán permanecer enmascaradas en todos los medios tecnológicos en los cuales son digitadas.

d) Es responsabilidad directa del personal del ORES-FOVIME(funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) el velar por la confidencialidad y buen uso de su contraseña.

e) No se deben almacenar contraseñas en formato legible en archivos tipo “batch”, scripts de logon automáticos, macros de software, teclas de función de terminales, computadores sin control de acceso, archivos de texto o en sitios donde personas no autorizadas puedan descubrirlos y utilizarlos.

**Controles de acceso de red**

Ninguna persona que labore en la Unidad de Tecnología de la Información tendrá acceso a los datos en producción, en modalidad diferente a la de consulta, a excepción del Administrador de la Base de Datos o cuando se realice por expresa solicitud y autorización del responsable de la Unidad de Tecnología de la Información.

a) El personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) no tendrán acceso de escritura a los datos de producción por fuera de los sistemas de información, a excepción del Administrador de Base de Datos.

b) Es responsabilidad de la Unidad de Tecnología de la Información contar con los mecanismos que permitan definir los atributos de acceso definidos por el usuario dueño de los datos.

c) La Unidad de Tecnología de la Información garantizará a la entidad que el personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) y demás personas (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) reportadas como ausentes por motivo de vacaciones, incapacidades, licencias, término del servicio, etc., no podrá tener acceso a la red interna de la institución, salvo que se justifique y se realice por expresa solicitud y autorización del responsable de la Unidad de Tecnología de la Información.

d) La Unidad de Tecnología de la Información contará con personas responsables de la seguridad de acceso a los datos, de acuerdo a sus funciones en las diferentes plataformas.

e) Para cubrir eventualidades causadas por ausencia imprevista (incapacidades y fuerza mayor) del personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) que tiene a cargo operaciones críticas, se recurrirá a mantener creados pero

inhabilitados, usuarios de Backup que permitan en forma rápida restaurar el servicio afectado. El Oficial de Seguridad de la Información revisará en forma periódica la utilización de estos perfiles.

### 8.11. Controles de acceso a aplicaciones

Las aplicaciones incluirán un adecuado control de acceso basado en el análisis de las funciones que la aplicación tiene desarrolladas y las autorizaciones por grupos de usuarios, roles y perfiles.

### *8.12. Adquisición, mantenimiento y desarrollo de sistemas de información*

#### 8.12.1. Requerimientos de seguridad

a) Las nuevas aplicaciones que se pondrán en operación en la entidad deben cumplir los requerimientos de seguridad mínimos establecidos para asegurar confidencialidad, integridad y disponibilidad en la información que manejan.

b) La Unidad de Tecnología de la Información es responsable de mantener a disposición de la entidad la infraestructura tecnológica más conveniente de acuerdo a sus requerimientos y lo que ofrece el mercado.

#### 8.12.2. Datos para pruebas

El Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME mantendrá por separado sus ambientes de producción, desarrollo y calidad, y en cada uno de ellos mantendrá únicamente los elementos que se consideren adecuados con el fin de mitigar los riesgos.

Es responsabilidad de la Unidad de Tecnología de la Información asegurar que los datos dispuestos para la realización de calidad y desarrollo cuenten con la debida protección para minimizar los riesgos con respecto a la confidencialidad.

**Análisis de Vulnerabilidades**

Es responsabilidad de la Unidad de Tecnología de la Información mantener un esquema de pruebas de vulnerabilidad a los componentes de la red dependiendo del análisis de riesgos.

8.12.3. **Administración de sistemas de información**

El Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME deberá cumplir el esquema general de ciclo de vida de los proyectos, de acuerdo a la metodología basada en la NTP 12207, que para el efecto elaboró la Unidad de Tecnología de la Información, esto es tanto para el mantenimiento de aplicaciones en producción, calidad ó desarrollos nuevos.

8.12.4. **Cifrado**

En los medios y transmisiones electrónicas que el Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME determine, se deberán mantener esquemas de cifrado que cumplan los requerimientos específicos establecidos para tal fin. Para esto creará una política específica que regule el uso de dicho esquema.

### *8.13. Administración de Incidentes de Seguridad*

8.13.1. **Reporte de Incidentes y eventos de seguridad**

a) Todo el personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) debe reportar cualquier incidente de seguridad que detecte, al Oficial de Seguridad de la Información lo antes posible de la forma establecida en el procedimiento correspondiente a Administración de Incidentes.

b) El alcance fundamental es que cualquier personal del ORES-FOVIME (funcionarios, servidores, CAS, locadores de servicios y otros) pueda identificar, clasificar y reportar de manera sencilla los incidentes de seguridad, manteniendo abierta la posibilidad de reportar los incidentes en forma oportuna.

Todos estos incidentes y eventos de seguridad serán monitoreados y cuantificados a través del Sistema de Gestión de la Seguridad de la Información (SGSI), el cual al ser un sistema cíclico recibe información de los incidentes y eventos sucedidos ayudando a identificar cuales son los que más se repiten o de gran impacto para la entidad; logrando que el sistema mejore constantemente, implementando controles más avanzados o adicionales, y así limitar la frecuencia, daño y costos de

#### 8.13.2. **Administración de incidentes de seguridad**

El Oficial de Seguridad de la Información debe realizar el debido estudio y seguimiento de todos los incidentes de seguridad, valiéndose de la asistencia de todos los usuarios involucrados cuando éste lo requiera.

Es responsabilidad del Oficial de Seguridad de la Información mantener actualizadas las estadísticas de mantenimiento de emergencia, clasificadas en técnicas y de usuario, siendo éstas reportadas mensualmente al responsable de la Unidad de Tecnología de la Información.

Es responsabilidad de la Unidad de Tecnología de la Información divulgar las estadísticas de mantenimientos de emergencia, clasificados en técnicas y de usuario a las instancias que determine la entidad.

### *8.14. Administración de la continuidad de operaciones*

#### 8.14.1. **Planeación del Plan de Continuidad de Operaciones**

El Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME diseñará y mantendrá vigente un Plan de Continuidad de Operaciones que atienda los requerimientos de Seguridad de la Información en la entidad según el análisis de riesgos determinado para tal fin, el cual deberá estar catalogado por niveles (1,2,3) de acuerdo con el grado de contingencia que se deba atender, por ejemplo: Grado 1, contingencias menores que se atienden con el personal dentro de las instalaciones. Grado 2, que no se permita el ingreso al edificio, grado 3, por desastre.

La entidad realizará pruebas periódicas y mantenimiento al Plan de Continuidad de Operaciones por lo menos UNA vez en el año. Ocurrencias futuras.

La entidad contará con un contrato de custodia externa de la información, como parte del plan de continuidad de operaciones.

## *8.15. Cumplimiento*

### 8.15.1. **Protección Legal**

El Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME conserva el derecho de retirar de los sistemas de información cualquier material que pueda ser considerado ofensivo o potencialmente ilegal.

### 8.15.2. **Normatividad**

Es responsabilidad del dueño de la información, definir los periodos de retención y la frecuencia de los Backups que garanticen el cumplimiento legal y los propios.

Las políticas de seguridad de la información del Organismo Especial del Fondo de Vivienda Militar del Ejercito ORES-FOVIME fueron diseñadas para ajustarse o exceder, sin contravenir, las medidas de protección establecidas en las leyes y regulaciones; si el personal del MINAG (funcionarios, servidores, CAS, locadores de servicios y otros) u otra persona (naturales, jurídicas, consultores, contratistas, temporales o terceras partes u otros) considera que alguna política de seguridad de la información está en conflicto con las leyes y regulaciones existentes, lo debe reportar en forma inmediata al Oficial de Seguridad de la Información de la entidad.

## Principales Modificaciones por versión del Presente Documento

**Historial de Revisión**

| Versión | Autor | Fecha | Descripción de Revisión |
|---|---|---|---|
| 0.1 | Maria Villar – Telemática | 10-03-2017 | Versión Inicial |
| 1.0 | Manuel Camacho – ORES-FOVIME<br>Carlos Chois – ORES-FOVIME<br>Carlos Vega - ORES-FOVIME<br>Adrián Rodríguez. – ORES-FOVIME | 09-02-2009 | Versión Final 1.0 |

## Este documento ha sido revisado por:

| It | Revisor |
|---|---|
| 1. | Carmen Salardi – ORES-FOVIME Jessica Urrello – ORES-FOVIME Carlos Chois – ORES-FOVIME<br>Carlos Vega – ORES-FOVIME Manuel Camacho - ORES-FOVIME<br>Adrián Rodríguez. – ORES-FOVIME<br>Dianne Vergara – M&T Consulting<br>Eric Morán – M&T Consulting |

## Este documento ha sido aprobado por:

| | Expertos en el Tema | | |
|---|---|---|---|
| **It.** | **Nombre** | **Firma** | **Fecha Autorización** |
| 1. | ORES-FOVIME – Carlos Federico Leyton Muñoz, Ministro |  | |

| | | | |
|---|---|---|---|
| 2. | ORES-FOVIME – José Mercedes Sialer Pasco, Viceministro | | |
| 3. | ORES-FOVIME – Carmen Lucy Salardi Bramont, Directora de la Oficina de Administración | | |
| 4. | ORES-FOVIME – Carlos Chois Pimentel, Director de la Unidad de Tecnología de la Información | | |

## EVIDENCIAS – ANEXO Nª 07

Reunión con el Consejo Directivo del ORES-FOVIME

Consejo Directivo

Reunión con los Jefes de Áreas

**Anexo 11:** Personal evaluando la seguridad de sus proyectos

Coordinación con los usuarios de la Sección de telemática SETEL

Encuesta al personal involucrado

**Anexo 11.**

Personal que accede a préstamos hipotecarios ORES-FOVIME

Colas de personal para préstamos hipotecarios y refinanciamiento

Capacitación al personal para el uso de usuario y clave del sistema

Capacitación al personal que tiene acceso a la base de datos OSSAB

Sala de servidores (antes)


Sala de servidores (después)