**UNIVERSIDAD NACIONAL**

**JOSÉ FAUSTINO SÁNCHEZ CARRIÓN**

**FACULTAD DE INGENIERÍA INDUSTRIAL,**

**SISTEMAS E INFORMÁTICA**

ESCUELA PROFESIONAL

DE INGENIERÍA INFORMÁTICA

# ELABORACION DE MODELO DE SEGURIDAD PARA EL MANEJO DE INFORMACION EN EL ORGANO DE CONTROL INSTITUCIONAL, MUNICIPALIDAD PROVINCIAL DE HUAURA – HUACHO

# TESIS


**AUTOR:**

BACH. OLORTEGUI LAGUNA, YASSER ANGEL

**ASESOR:**

Ing. CARLOS MANUEL CRUZ CASTAÑEDA

Registro CIP: 93335


**HUACHO - PERÚ**

**2019**

## ASESOR Y MIEMBROS DE JURADO

**Ing. Alejandro Manuel Salazar Santibáñez**
**Presidente**
**CIP N° 26580**

**Ing. Erlo Wilfredo Lino Escobar**
**Secretario**
**CIP N° 31652**

**Ing. Eddy Iván Quispe Soto**
**Vocal**
**CIP N° 91455**

**Ing. Carlos Manuel Cruz Castañeda**
**Asesor**
**CIP N° 93335**

## DEDICATORIA

*A Dios por darme sabiduría y permitirme llegar a este nivel intelectual.*

*A mis padres por ser guías en el sendero de cada acto que realizo hoy, mañana y siempre.*

*A todos mis maestros que con sus ejemplos de superación inspiran a sus discípulos.*

***El autor***

## AGRADECIMIENTO

Aprovecho este espacio para expresar mi más profundo y sincero agradecimiento a todas aquellas personas que con su ayuda han colaborado en la realización del presente trabajo de investigación.

Un especial agradecimiento al Ing. Carlos Manuel Cruz Castañeda, Asesor de Tesis, por la orientación, supervisión del proyecto de investigación. A los integrantes de la **Órgano de control Institucional**, período 2017, por la oportunidad de realizar la presente investigación en la Municipalidad Provincial de Huaura Huacho. Por su disposición en atenderme cada vez que solicitaba sus ayudas y conocimientos que me brindaron.

**El Autor.**

## INDICE GENERAL


PORTADA i
ASESOR Y MIEMBROS DE JURADO ii
DEDICATORIA iii
AGRADECIMIENTO iv
INDICE GENERAL v
INDICE DE FIGURAS viii
INDICE DE TABLAS ix
RESUMEN – ABSTRACT x
INTRODUCCIÓN xi
**1.** PLANTEAMIENTO DEL PROBLEMA 1
**1.1.** DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA 1
**1.2.** FORMULACIÓN DEL PROBLEMA 2
**1.2.1.** PROBLEMA GENERAL 2
**1.2.2.** PROBLEMAS ESPECÍFICOS 2
**1.3.** OBJETIVOS DE LA INVESTIGACIÓN 2
**1.3.1.** OBJETIVO GENERAL 2
**1.3.2.** OBJETIVOS ESPECÍFICOS 3
**1.4.** JUSTIFICACIÓN E IMPORTANCIA DE LA INVESTIGACIÓN 3
**1.4.1.** JUSTIFICACIÓN 3
**1.4.2.** IMPORTANCIA 4
**1.5.** DELIMITACIÓN DE LA INVESTIGACIÓN 4
**1.5.1.** DELIMITACIÓN GEOGRÁFICA 4
**1.5.2.** DELIMITACIÓN TEMPORAL 4
**1.5.3.** DELIMITACIÓN DE RECURSOS 5
**1.6.** VIABILIDAD 5
**2.** MARCO TEÓRICO 6
**2.1.** DESCRIPCIÓN DE LA INSTITUCIÓN EN ESTUDIO 6
**2.1.1.** **ANTECEDENTES** **6**
**2.1.2.** **MISIÓN** **6**
**2.1.3.** **VISIÓN** **7**
**2.1.4.** OFICINA DE INFORMÁTICA 7
**2.2.** ANTECEDENTES DE LA INVESTIGACIÓN 8
INTERNACIONALES: 8
NACIONALES: 9
**2.3.** BASES TEÓRICAS 11
**2.3.1.** **AUDITORÍA** **11**
**2.3.1.1.** CLASIFICACIÓN DE AUDITORÍA: 12
**2.3.1.2.** *Auditoría* de Seguridad Informática 13

**2.3.2.** SEGURIDAD INFORMÁTICA 15
**2.3.2.1.** Elementos de la Seguridad Informática 15
**2.3.2.2.** Clasificación de la Seguridad Informática 17
**2.3.2.3.** Razones para la Seguridad Informática 20
**2.3.3.** NTP-ISO/IEC 27001: 2014 - ESTANDAR RELACIONADO CON LA SEGURIDAD DE LA INFORMACIÓN 27
**2.4.** DEFINICIÓN DE TÉRMINOS BÁSICOS 34
**2.5.** FORMULACIÓN DE HIPÓTESIS 37
**2.5.1.** HIPÓTESIS GENERAL 37
**2.5.2.** HIPÓTESIS ESPECÍFICA 37
**2.6.** OPERACIONALIZACIÓN DE VARIABLES E INDICADORES 38
**2.6.1.** VARIABLE INDEPENDIENTE 1 38
**2.6.2.** VARIABLE INDEPENDIENTE 2 38
**3.** METODOLOGÍA 40
**3.1.** DISEÑO METODOLÓGICO 40
**3.1.1.** TIPO DE INVESTIGACIÓN 40
**3.1.2.** NIVEL 40
**3.1.3.** ENFOQUE 40
**3.2.** POBLACIÓN 41
**3.2.1.** POBLACIÓN 41
**3.2.2.** MUESTRA 41
**3.3.** TÉCNICAS E INSTRUMENTOS DE RECOLEC. DE DATOS 41
**3.3.1.** TÉCNICAS A EMPLEAR 41
**3.3.2.** DESCRIPCIÓN DE LOS INSTRUMENTOS 42
**3.4.** TÉCNICAS PARA EL PROCESAMIENTO DE LA INFORMAC. 42
**4.** RESULTADOS 43
**4.1.** GESTIÓN Y PROPUESTAS 43
**4.2.** POLÍTICAS DE MEJORAS PARA ENCARGADOS DE LA INFORMATICA 45
**4.3.** RESULTADOS METODOLÓGICOS 45
**4.3.1.** VALIDEZ DEL INSTRUMENTO 45
**4.3.2.** CONFIABILIDAD DEL INSTRUMENTO 47
**4.3.3.** TABLAS Y GRÁFICOS ESTADÍSTICOS 49
**4.3.4.** CONTRASTACIÓN DE HIPÓTESIS 63
**5.** CONCLUSIONES Y RECOMENDACIONES 68
**5.1.** CONCLUSIONES: 68
**5.2.** RECOMENDACIONES. 69
**6.** FUENTES BIBLIOGRÁFICAS 70
ANEXO A. (Matriz de Consistencia)
ANEXO B. (3 Juicios de Expertos)
ANEXO C. (Encuesta o Cuestionario)
ANEXO D. (Matriz de Alpha de Cronbach)

***INDICE DE FIGURAS***

***Figura 01. Triada de la seguridad.*** ***16***
***Figura 02. Ejemplo de Acceso a un sistema.*** ***18***
***Figura 03. Conexiones de ordenadores en red.*** ***22***
***Figura 04. Tarjetas de Crédito.*** ***22***
***Figura 05. Ataque de interrupción.*** ***23***
*Figura 06. Ataque de interceptación.* *24*
*Figura 07. Ataque de modificación.* *24*
*Figura 08. Ataque de fabricación.* *25*
*Figura 9. Modelo PDCA (ciclo Demming).* *34*
*Figura N° 10: Inventariado de recursos informáticos en las fechas establecida* *49*
*Figura N° 11: Recursos informáticos: propiedad de la Municipalidad.* *50*
*Figura N° 12: Arregla su computadora por su propia cuenta.* *51*
*Figura N° 13: Conocimiento de funciones de desempeños.* *52*
*Figura N° 14: Capacitaciones de trabajadores para la seguridad Informática.* *53*
*Figura N° 15: Acceso a los sistemas de información de la municipalidad.* *54*
*Figura N° 16: Monitoreo: privilegios de acceso a los usuarios.* *55*
*Figura N° 17: Acceso a internet a través de su celular.* *56*
*Figura N° 18: Copias de seguridad al alcance de los demás trabajadores.* *57*
*Figura N° 19: Acceso a la sala de servidores personal no autorizado.* *58*
*Figura N° 20: Cualquier trabajador puede llevarse información en usb, etc.* *59*
*Figura N° 21: Gerencia pide información al departamento de informática (tiempo).* *60*
*Figura N° 22: Copias de seguridad - están disponibles.* *61*
*Figura N° 23: Todos los encargados del área de informática pueden modificar, eliminar o cambiar la información en la base de datos.* *62*

**INDICE DE TABLAS**


Tabla 01: Calificación de los Expertos 46
Tabla 02: Calificación de los Expertos 47
Tabla 03: Alpha de Cronbach aplicado al Instrumento 48
Tabla 04: Escala de confiabilidad 48
Tabla 05: ¿Se realiza el inventariado de recursos informáticos en las fechas establecidas? 49
Tabla 06: ¿Los recursos informáticos son propiedad de la municipalidad? 50
Tabla 07: ¿Ha intentado arreglar su computadora por su propia cuenta? 51
Tabla 08: ¿Conoce usted la función que debe desempeñar? 52
Tabla 09: ¿Se dictan capacitaciones a los trabajadores para la seguridad Informática? 53
Tabla 10: ¿Accede a los sistemas de información de la municipalidad? 54
Tabla 11: ¿Monitorean constantemente los privilegios de acceso a los usuarios? 55
Tabla 12: ¿Tiene acceso a internet a través de su celular? 56
Tabla 13: ¿Las copias de seguridad están al alcance de los demás trabajadores? 57
Tabla 14: ¿Puede entrar a la sala de servidores personal no autorizado 58
Tabla 15: ¿Cualquier trabajador puede llevarse información en USB, cd, etc? 59
Tabla 16: ¿Cuándo la gerencia pide información al departamento de informática, se le brinda a tiempo? 60
Tabla 17: ¿Cuándo se requiere utilizar las copias de seguridad, están disponibles? 61
Tabla 18: ¿Todos los encargados del área de informática pueden modificar, eliminar o cambiar la información en la base de datos? 62
Tabla N° 19 de contingencia X1 * RESUMEN_Y (agrupado) 63
Tabla N° 20: Pruebas de chi-cuadrado 64
Tabla N° 21 de contingencia X2 * RESUMEN_Y (agrupado) 65
Tabla N° 22 Pruebas de chi-cuadrado 65
Tabla N° 23 de contingencia X3 * RESUMEN_Y (agrupado) 66
Tabla N° 24 Pruebas de chi-cuadrado 66
Tabla N° 25 de contingencia RESUMEN_X (agrupado) * RESUMEN_Y (agrupado) 67
Tabla N° 26 Pruebas de chi-cuadrado 67
Tabla N° 27 Resumen de la Prueba de Hipótesis Estadística 68

**ELABORACION DE MODELO DE SEGURIDAD PARA EL MANEJO DE INFORMACION EN EL ORGANO DE CONTROL INSTITUCIONAL, MUNICIPALIDAD PROVINCIAL DE HUAURA – HUACHO**

**ELABORATION OF SECURITY MODEL FOR THE HANDLING OF INFORMATION IN THE INSTITUTIONAL CONTROL ORGAN, PROVINCIAL MUNICIPALITY OF HUAURA - HUACHO**

**OLORTEGUI LAGUNA, YASSER ANGEL**[1]

## RESUMEN

**Objetivo:** Diseñar un Sistema Informático basado en la ISO 27001, que permita al Órgano de Control Institucional de la Municipalidad Provincial de Huaura – Huacho tener seguridad en el manejo de la información. **Métodos:** La Población estuvo constituida por los 07 trabajadores del Órgano de Control Institucional de la Municipalidad Provincial. Se utilizó la Técnica de *Encuesta,* para aplicar el Test que mide el grado de conocimiento del Sistema de seguridad. Con este indicador de alfa de Cronbach se indica que el Cuestionario tiene un 90% de validez. **Resultados**: Se realizó el análisis de fiabilidad en el programa estadístico SPSS Statistics 22.0 al instrumento aplicado a todos los trabajadores del Órgano de Control y Área de Informática (07 trabajadores). Se obtuvo una fiabilidad de 0,739 (ver Tabla 03), este instrumento estuvo conformado por 14 items, distribuidos para la variable independiente: Seguridad Informática**,** en 3 dimensiones (Gestión de activos informáticos, Seguridad de Recursos Humanos y Control de Accesos) y para la variable dependiente: Alineamiento de Políticas de Seguridad Informática, 3 dimensiones (Confidencialidad, Disponible e Integro). **Conclusión:** Se concluye que si los usuarios de los sistemas de información ya sean expertos o inexpertos no están enterados de los métodos y elementos que componen la seguridad informática y los aplican en conjunto no se podrá cumplir la seguridad informática, podemos confirmar nuestra idea principal de investigación la cual menciona que: La seguridad en tecnologías de información se ve amenazada cuando se desconocen los métodos de seguridad informática.

**Palabras claves:** Sistema Informático, Seguridad para el Manejo de Información.

## ABSTRACT

**Objective**: Design a Computer System based on ISO 27001, which allows the Institutional Control Body of the Provincial Municipality of Huaura - Huacho to have security in the handling of information. **Methods**: The Population was constituted by the 07 workers of the Organ of Institutional Control of the Provincial Municipality. The Survey Technique was used to apply the Test that measures the degree of knowledge of the Security System. With this Cronbach alpha indicator it is indicated that the Questionnaire is 90% valid. **Results**: Reliability analysis was performed in the statistical program SPSS Statistics 22.0 to the instrument applied to all workers of the Control Body and Computer Area (07 workers). A reliability of 0,739 was obtained (see Table 03), this instrument consisted of 14 items, distributed for the independent variable: Computer Security, in 3 dimensions (Computer Asset Management, Human Resources Security and Access Control) and for the dependent variable: Alignment of IT Security Policies, 3 dimensions (Confidentiality, Available and Complete). **Conclusion**: It is concluded that if the users of the information systems, whether expert or inexperienced, are not aware of the methods and elements that make up computer security and apply them together, computer security can not be met, we can confirm our main idea of research which mentions that: The security in information technologies is threatened when the methods of computer security are unknown.

**Keywords**: Computer System, Security for Information Management.

# INTRODUCCIÓN

En el transcurrir del presente siglo, el mundo se encuentra inmerso en constantes cambios y problemas globales que demandan profesionales capaces de desarrollar al máximo sus potencialidades en la búsqueda de soluciones y alternativas teóricas y metodológicas que permitan conocer, interpretar y transformar la realidad hacia el desarrollo humano con compromiso social.

La investigación constituye un proceso de búsqueda de alternativas para la generación, innovación y elaboración de soluciones ante cualquier realidad en la que le toque desenvolverse. La investigación, como actividad y capacidad, cada vez se generaliza y se constituye en una exigencia en todos los niveles del saber.

En ese sentido, la investigación es una experiencia que posibilita reconocerse partícipe del problema y de la solución o de la posibilidad de proponer alternativas viables y efectivas a las necesidades humanas.

En concordancia al contexto emergente y realidad problemática referida en líneas anteriores se desarrolló el estudio sobre "Modelo de Seguridad para el manejo de información en el Órgano de Control Institucional Municipalidad Provincial de Huaura – Huacho"; para mejorar el sistema de seguridad y control del servicio informático con la idea central de proteger la información, poder monitorear y aplicar políticas de seguridad de control que mitiguen la probabilidad de ocurrencia de pérdidas de información.

El estudio estuvo orientado a mejorar la protección de información, identificar la vulnerabilidad, riesgos, dar una propuesta de solución utilizando instrumentos metodológicos que conlleven a probar la relación de una necesidad de tener un modelo de para el manejo de la información en la Municipalidad de Huaura – Huacho.

En el capítulo 1, se desarrolla el marco de la realidad problemática formulada sobre las bases de revisiones bibliográficas, estudios exploratorios y técnicas adecuadas para el enfoque del problema.

En el capítulo 2, denominado marco teórico, se detalla sobre la institución en estudio y se mencionan estudios nacionales y extranjeros que fueron tomados en cuenta; así mismo se exponen las bases teóricas científicas de las variables enfocadas (Modelo de

Auditoría – Seguridad Informática).

En el capítulo 3, denominado marco metodológico, se precisan los elementos principales del protocolo de investigación como: hipótesis, variables, tipo de investigación, diseño, método de estudio, población y muestra, técnicas de acopio de datos y método de análisis de datos.

En el capítulo 4, denominado resultados, se presentan los hallazgos explorados y expresados en tablas estadísticas, gráficos y medidas de resumen. Complementado con interpretaciones y prueba de hipótesis, de acuerdo a los objetivos generales y específicos establecidos previamente. Enseguida se discuten los resultados destacando nuestra opinión sobre la validez de los resultados y estableciendo la relación con los antecedentes y las teorías precisados en el estudio.

En la parte final del informe se formulan de manera puntual las conclusiones más relevantes, se plantean recomendaciones dirigidas a la institución en estudio y a personas que trabajan en el quehacer informático para resolver algunos problemas. Y en la sección de anexos se adjuntan las evidencias que contribuyen a lograr la credibilidad del estudio.

El Autor.

# 1. PLANTEAMIENTO DEL PROBLEMA

## 1.1. DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

Con el paso del tiempo, se puede evidenciar que la mayor parte de las organizaciones, sin importar el tamaño, logran acumular gran cantidad de datos de sus empleados, proyectos de investigación, su situación financiera, entre otros. El volumen más grande de estos datos, es recolectado, procesado, almacenado y puesto a la disposición de sus trabajadores, usuarios, como información visible y disponible a través de la tecnología de la informática.

Es preocupante entonces, como muchas entidades pueden perder información importante y también echarse a perder proyectos importantes, decisiones estratégicas, estados financieros, entre otros, sin haber permitido que se volviera pública de forma no autorizada. Es por esto, que desde el punto de vista de la investigación, proteger la Información confidencial es un requisito muy importante.

En la oficina de Informática de la Municipalidad Provincial de Huaura - Huacho, tienen el control de todos los movimientos de información de la municipalidad; esta entidad tiene una directiva en políticas de seguridad sobre Administración de la Red de la Municipalidad Provincial de Huaura– Huacho, declarada el 2012, pero cuenta con poco personal en informática y solo se encargan de Administrar la Seguridad de la Red dejando de lado otros aspectos que incluyen la seguridad informática que implica salvaguardar la información importante de la municipalidad, es por ello que cada día se ven en la necesidad de seguir alineándose a las políticas de seguridad, por ello la importancia de un modelo de seguridad en el manejo de la información en el Órgano de Control Institucional de la entidad y poder monitorear como se están cumpliendo las políticas de seguridad Informática y encontrar los puntos donde hace falta implementarlas. Ya que un ataque simple o un descuido puede originar daños catastróficos a una entidad como en este caso el Órgano de Control Institucional de la municipalidad provincial de Huaura - Huacho si es que no cuenta con controles que mitiguen la probabilidad de ocurrencia de estos.

## 1.2. FORMULACIÓN DEL PROBLEMA

### 1.2.1. PROBLEMA GENERAL

¿Cómo el diseño de un modelo de la Auditoría Informática basado en la ISO 27001, permitirá al Órgano de Control Institucional de la Municipalidad Provincial de Huaura – Huacho tener seguridad en el manejo de información de dicho Órgano de Control Institucional?

### 1.2.2. PROBLEMAS ESPECÍFICOS

- ¿En qué medida el diseño de un Sistema Informático basado en la ISO 27001, con una buena Gestión de activos Informáticos, permitirá el alineamiento de Políticas de Seguridad para el manejo de la información de dicho Órgano de Control Institucional?

- ¿De qué manera el diseño de un modelo de un Sistema Informático basado en la ISO 27001, con una buena seguridad relacionada con los Recursos Humanos, permitirá el buen manejo de información en el Órgano de Control Institucional?

- ¿Cómo el diseño de un modelo de un Sistema Informático basado en la ISO 27001, con un buen Control de Accesos, permitirá tener Seguridad para el buen manejo de información en base a políticas de seguridad informática?

## 1.3. OBJETIVOS DE LA INVESTIGACIÓN

### 1.3.1. OBJETIVO GENERAL

Diseñar un Sistema Informático basado en la ISO 27001, que permita al Órgano de Control Institucional de la Municipalidad Provincial de Huaura – Huacho tener seguridad en el manejo de la información de dicho Órgano de Control Institucional

### 1.3.2. OBJETIVOS ESPECÍFICOS

- Diseñar un Sistema Informático basado en la ISO 27001 con una buena Gestión de activos Informáticos, que permita alinearse a las políticas de Seguridad Informática en la Municipalidad Provincial Huaura-Huacho.

- Diseñar un Sistema Informático basado en la ISO 27001 con una buena seguridad relacionada con los Recursos Humanos, que permita alinearse a las políticas de Seguridad Informática en el Órgano de Control Institucional de la Municipalidad Provincial Huaura-Huacho.

- Diseñar un Sistema Informático basado en la ISO 27001 con un buen Control de Accesos, que permita alinearse a las políticas de Seguridad Informática en el Órgano de Control Institucional de la Municipalidad Provincial Huaura-Huacho.

# 2. MARCO TEÓRICO

## 2.1. DESCRIPCIÓN DE LA INSTITUCIÓN EN ESTUDIO

### 2.1.1. ANTECEDENTES

La antigua Provincia de Chancay estaba conformada (según Ley transitoria de Municipalidades del 29-XII-1856) por los distritos de Huacho, Huaral, Chancay, Sayán, Supe, Barranca, Pativilca, Paccho y Checras. Debido al crecimiento poblacional y al desarrollo económico, los distritos de Huaral y Chancay pasaron a conformar la Provincia de Huaral (Ley Nº 21488 del 11-V-1976); mientras que Barranca, Pativilca y Supe (Ley Nº 23939 del 01-X-1984) pasaron a conformar la provincia de Barranca. De esa manera la provincia quedó prácticamente reducida a la cuenca del río Huaura (el distrito de Ámbar fue anexado por Ley Nº 8003 del 14-II-1935, antes formó parte de la provincia de Cajatambo) pero conservando su antigua denominación, por lo que por ley Nº 24886 del 26-V-1988 se cambió su denominación por Provincia de Huaura.

### 2.1.2. MISIÓN

Entidad del estado que cumple con la Integración Territorial en la Provincia de Huaura, promotora del Desarrollo Humano sostenible, con capacidad para el cumplimiento de sus fines, promueve la adecuada prestación de Servicios Públicos Locales, Gobierno incluyente que desarrolla las Políticas y Planes de Desarrollo Concertado en un espacio de reflexión y debate, promueve el Desarrollo Integral Solidario para viabilizar el crecimiento Económico, la Justicia Social y la Sostenibilidad Ambiental, Propiciando la defensa de la ciudadanía para las mejores condiciones de vida de su población.

### 2.1.3. VISIÓN

Huaura al 2021 es una provincia integrada con sus distritos, con sus principales circuitos viales asfaltados y seguros, con desarrollo integral solidario, sostenido y sustentablemente, con manejo y gestión de cuenca hidrográfica del río Huaura y el litoral marítimo, articulado al mundo globalizado. Sus ciudadanas y ciudadanos organizados, inspirados en principios y valores democráticos, donde el rol de la ciudadanía contribuye al desarrollo de la provincia, sus autoridades y líderes actúan con integridad moral, son comprometidos, concertadores, participativos, eficientes y honestos, con vocación deservicio, logran el desarrollo institucional de sus organizaciones.

### 2.1.4. ORGANO DE CONTROL INSTITUCIONAL

El Órgano de Control Institucional, es el órgano de control interno integrante del Sistema Nacional de Control, encargado de realizar el control a las unidades orgánicas de la Municipalidad Provincial de Huaura, así como de sus órganos desconcentrados y descentralizados que no cuenten con su propio órgano de control conforme a la Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, el Reglamento de los Órganos de Control Institucional aprobado por Resolución de Contraloría y demás normas reglamentarias, directivas y lineamientos que disponga la Contraloría General de la República.

**FUNCIONES:**

- Ejercer el control interno posterior a los actos, procedimientos administrativos de la Municipalidad, sobre la base de los lineamientos y cumplimiento del Plan Anual de Control, a que se refiere al artículo 7° de la Ley, y el control externo al que se refiere el artículo 8° de la Ley, por encargo de la Contraloría Genera.
- Verificar el cumplimiento de las disposiciones legales y normativas internas aplicables a la Municipalidad.

- Fomentar, ejecutar y evaluar el Plan Anual de Control previamente aprobado, en coordinación con la Contraloría General de la República.

### 2.1.5. OFICINA DE INFORMÁTICA

La Oficina de Informática de la Municipalidad Provincial de Huaura – Huacho; dependía de la Subgerencia de Secretaría General, (actualmente en esta gestión 2015, se llama Subgerencia de Tecnologías, Sistemas de Información y Estadística, depende de la Gerencia de Planeamiento y Presupuesto) es la encargada de controlar todos los movimientos de información de la municipalidad; esta entidad tiene una directiva en políticas de seguridad sobre Administración de la Red de la Municipalidad Provincial de Huaura – Huacho, declarada el 2012, pero solo se encargan de Administrar la Seguridad de la Red dejando de lado otros aspectos que incluyen la seguridad informática que implica salvaguardar la información importante de la municipalidad.

**FUNCIONES**

- Planeación, programación, diseño e implementación del Sistema Informático Municipal a través de los terminales de trabajo, garantizando la confiabilidad, exactitud y oportunidad de resultados en beneficio de la institución.
- Velar por la seguridad de los equipos y del soporte técnico, sobre la automatización de datos en el proceso administrativo de la Municipalidad.
- Conducción y supervisión de actividades en la ejecución de los sistemas mecanizados y desarrollar actividades de programación.

## 2.2. ANTECEDENTES DE LA INVESTIGACIÓN

### INTERNACIONALES:

**Cadme C., Duque D. (2012)** Realizaron una tesis titulada "Auditoría de Seguridad Informática ISO 27001 para la empresa de alimentos ITALIMENTOS CIA. LTDA" Para optar el título de Ingeniero de Sistemas, Universidad Politécnica Salesiana - Cuenca, su objetivo: Realizar una Auditoría para alinear la empresa con la ISO 27001 para garantizar la seguridad, rendimientos y privacidad de los sistemas y máquinas de la empresa; para esto hizo un análisis exhaustivo que describió la situación actual de la empresa concluyendo con las propuestas de solución que tuvo su auditoria. (Ecuador),

**Reyes M. (2011)** Realizó una tesis titulada "Propuestas para impulsar la seguridad informática en materia de educación" Para optar por el título de Ingeniero en Computación, Universidad Nacional Autónoma de México; su objetivo: Comprender el desarrollo de la seguridad informática en México y su relación con el mundo, concluyendo con una propuesta de un plan de acción para impulsar la seguridad informática en cuanto a educación y desarrollo tecnológico desde las universidades: que tengan acceso a internet y adquieran los conocimientos adecuados para crear una nueva cultura sobre tecnologías y seguridad informática. (México),

**Martínez V. (2010)** Realizó una tesis titulada "Concientización en Seguridad de la Información, La Estrategia para Fortalecer el Eslabón más débil de la Cadena" Para optar por el título de Especialista en Dirección Estratégica de Empresas, Fundación Universitaria Iberoamericana; su objetivo: Elaborar un programa de concienciación en Seguridad de la Información que pueda ser usado por las empresas, para garantizar un tratamiento seguro de la Información sensible y confidencial de la compañía, evitando se vuelva pública de una manera no autorizada; concluyendo: La información es uno de los activos más importantes para la compañía, y por lo tanto, se le debe dar un tratamiento seguro haciendo que la información se convierta en el eje central sobre el cual gira la seguridad, definiendo acciones de protección y mecanismos de control para garantizar al negocio, la confiabilidad de dicha información. (Colombia),

**Monzón C. (2009)** Realizó una tesis titulada "Auditoria de Seguridad de Redes Inalámbricas de Área Local Wireless Local Área Network (WLAN)" Para optar por el título de licenciatura en informática, Universidad Mayor de San Andrés, su objetivo es: desarrollar un modelo de gestión para la auditoria de redes inalámbricas de área local con la finalidad de verificar la vulnerabilidad y riesgos en las redes inalámbricas de computadoras; la metodología utilizada está en base al método científico; concluyendo: que la investigación ofrece instrumentos para el relevamiento de la información y para la evaluación de la información recolectada que están de acuerdo al modelo de seguridad propuesto. (Bolivia).

**NACIONALES:**

**Villarroel, Y. (2013**) Realizó una tesis titulada "Proceso de Seguridad de la Información y Comunicación dentro del Control Interno según el Marco Coso II – ERM", Para optar el Título de Ingeniero Informático, Pontificia Universidad Católica del Perú; su objetivo: ubicar los principales aspectos

Involucrados en información y comunicaciones que podrían ser objeto de revisión dentro del control interno u otras auditorías relacionadas, analizar los riesgos y establecer las estrategias que los mitiguen, cumplir con la leyes y normativas, minimizar pérdidas operacionales, exponer claramente la filosofía y enfoque de la gestión de riesgos corporativos de la empresa, reforzar o modificar la cultura de una empresa,

**Ampuero C. (2011)** Realizó una tesis titulada "Diseño de un Sistema de Gestión de Seguridad de Información para una Compañía de Seguros" Para optar por el título de Ingeniero Informático, Pontificia Universidad Católica del Perú; su objetivo: desarrollar un sistema de gestión de seguridad de Información para ayudar al área de TI de una compañía de seguros, concluyendo: es importante contar con un Sistema de Gestión de Seguridad de la Información para poder asegurar, a un nivel aceptable, la información de la compañía y, dado que se trata de una compañía de seguros peruana, poder cumplir con las regulaciones de la SBS cumpliendo con el contenido de la circular G-140 y evitar así que la compañía incumpla con las regulaciones de la superintendencia,

**Córdova N. (2008)** Realizó una tesis titulada "Plan de Seguridad Informática para una Entidad Financiera" Para optar el título de Ingeniero de Sistemas, Universidad Nacional Mayor de San Marcos; su objetivo: es realizar un diagnóstico de la situación actual en cuanto a la seguridad de la información que el banco ABC actualmente administra y diseñar un plan de seguridad de la información que permita realizar operaciones seguras; concluyendo: que para desarrollar con éxito un programa efectivo de seguridad consiste en recordar que las políticas de seguridad son un grupo de documentos interrelacionados y presentando su plan de desarrollo,

**Villena M. (2006)** Realizó una tesis titulada "Sistema de Gestión de Seguridad de Información para una Institución Financiera" Para optar el título de Ingeniero Informático, Pontificia Universidad Católica del Perú; su

Objetivo: establecer los principales lineamientos para poder implementar de manera exitosa, un adecuado modelo de sistema de gestión de seguridad de información (SGSI) para una empresa financiera; concluyendo: que lo importante es la protección de la información para los procesos de negocio, se debe esperar de la alta gerencia su participación continua.

## 2.3. BASES TEÓRICAS

### 2.3.1. SEGURIDAD

**Alexander (2007),** Define a la seguridad como aquellas reglas técnicas y actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, perdida o daño, ya sea de manera personal, grupal o empresarial, por esta razón la información es el elemento principal a proteger, resguardar y recuperar en ls Instituciones.

**Hernández E (2003),** Señala que un sistema informático es seguro si se puede confiar en él y si se comporta de acuerdo a lo esperado. La seguridad en los sistemas informáticos en un conjunto de soluciones técnicas, métodos y planes con el objetivo de que la información que trata los sistemas informáticos sea protegida así como establecer un plan de seguridad en el cual se definan las necesidades y objetivos en cuestión de seguridad.

**Echenique (2008),** dice qué; con frecuencia la palabra auditoría se ha empleado incorrectamente y se le ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas. Por eso se ha llegado a usar la frase “tiene auditoría” como sinónimo de que, desde antes de realizarse, ya se encontraron fallas y por lo tanto se está haciendo auditoría. El concepto de auditoría es más amplio; no solo detecta errores: es un examen que se realiza con objeto de evaluar la eficiencia y eficacia de una sección o de un organismo, y determinar cursos alternativos de acción para mejorar la organización, y lograr los objetivos propuestos.

### *2.3.1.1.* CLASIFICACIÓN DEL CONTROL:

**Muñoz, C (2010),** escribió que se clasifica en:

#### Control Externo

La principal característica de este tipo de auditoría es que la realizan auditores totalmente ajenos a la empresa, por lo menos en el ámbito profesional y laboral, esto permite que el auditor externo utilice su libre albedrío en la aplicación de los métodos, técnicas y herramientas de auditoría con las cuales hará la evaluación de las actividades y operaciones de la empresa que audita y, por lo tanto, la emisión de resultados será absolutamente independiente.

Generalmente, estas auditorías externas son realizadas por grandes empresas y despachos independientes de auditores, los cuales, casi siempre gozan de gran popularidad y prestigio dentro del ambiente profesional. El mercado en el cual tienen mayor demanda y aplicación, estas auditorías es el ámbito contable, fiscal y financiero de las instituciones, así como aquellas actividades específicas que demandan una auditoría externa a la empresa cuando existen condiciones especiales que se pretenden evaluar.

#### Control Interno

En la realización de estos tipos de evaluación, el auditor que lleva a cabo la auditoría labora en la empresa donde se realiza la misma y, por lo tanto, de alguna manera, está involucrado en su operación normal, debido a esto, el auditor puede tener algún tipo de independencia con las autoridades de la institución, lo cual puede llegar a influir en el juicio que emita sobre la evaluación de las áreas de la empresa.

### 2.3.1.2. Control de Seguridad Informática

**Piattini, M (2001),** escribió que Una Auditoría de Seguridad Informática es el estudio que comprende el análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, los servidores y las redes de comunicaciones.

Durante una Auditoría de Seguridad Informática se realizan los siguientes tipos de auditorías expuestos posteriormente: Auditoría de la seguridad lógica y Auditoría de las comunicaciones.

Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables quienes deben establecer medidas preventivas de refuerzo, siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

Dentro de las Control de Seguridad Informática existen dos tipos principales en función del ámbito desde el que se comprueba la seguridad:

- **Control de seguridad interna.** En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno.

- **Control de seguridad perimetral.** En este tipo de análisis, el perímetro de la red local es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores.

La Auditoría de Seguridad Informática consta de las siguientes fases:

- **Enumeración de redes, topologías y protocolos.** Esta fase de reconocimiento pretende extraer la mayor información valiosa posible acerca de la red que va a ser auditada. Es fundamental el uso de herramientas de detección de equipos en esta fase.

- **Análisis de servicios y aplicaciones.** Esta fase consiste en detectar qué servicios están activos en qué puertos, y qué software junto con su versión están ejecutando. Para obtener está información, se utilizan técnicas, que mediante el uso de paquetes malformados extraen la información deseada.

- **Detección, comprobación y evaluación de vulnerabilidades.** En esta fase se hace uso de las Bases de Datos existentes con información acerca de vulnerabilidades en software anticuado. Por lo tanto, lo que se hace es comprobar que el software detectado en la fase anterior no es vulnerable.

- **Análisis de las comunicaciones.** Esta fase suele constar de una comprobación de si la red es vulnerable a ataques de tipo Man-in-the-Middle. Por lo general la mayoría de redes suele ser débil a estos ataques, y en caso de que lo sea, se realiza un análisis más exhaustivo de las comunicaciones existentes.

  Este análisis exhaustivo consiste en verificar si se utilizan protocolos de comunicación seguros mediante conexiones cifradas o por el contrario viajan las claves en texto plano por la red.

Finalmente si se obtienen contraseñas cifradas también existe la posibilidad de intentar descifrarlas para verificar que el nivel de seguridad de las mismas es el adecuado.

- **Medidas específicas de corrección**. Finalmente se redacta un informe con los datos extraídos de la auditoría y con recomendaciones sobre las medidas de corrección que deberían ser adoptadas.

### 2.3.2. SEGURIDAD INFORMÁTICA

**Monzón, C (2009).** Dice: Definir el concepto de Seguridad Informática no es algo fácil, se puede decir que la Seguridad Informática consiste en que un sistema se comporte como el usuario espera que lo haga, y a su vez mantenerlo libre de amenazas y riesgos. Por más de dos décadas se ha manejado que la seguridad se logra a partir de tres conceptos, conocidos como la triada de la seguridad: Confidencialidad, Integridad y Disponibilidad.

#### 2.3.2.1. Elementos de la Seguridad Informática

**Confidencialidad**

Consiste en mantener la información secreta a todos, excepto a aquellos que tienen autorización para verla. Cuando la información de naturaleza confidencial ha sido accedida, usada, copiada o revelada, por una persona que no está autorizada, entonces se presenta una ruptura de confidencialidad. La confidencialidad es un requisito para mantener la privacidad de las personas.

La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto.

**Integridad**

Significa que se debe asegurar que la información no ha sido alterada por medios no autorizados o desconocidos. Un ataque no debe ser capaz de sustituir información legítima por falsa.

**Disponibilidad**

Significa que todos aquellos elementos que sirven para el procesamiento de la información, así como los que sirven para facilitar la seguridad, estén activos y sean alcanzables siempre que se quiera.


***Figura 01. Triada de la seguridad.***

### 2.3.2.2. Clasificación de la Seguridad Informática

**Cervigón, A; Alegre, M (2011).** Escribieron que: Cuando hablamos de la seguridad en un sistema informático, podemos encontrar diversos tipos de seguridad, dependiendo de la naturaleza material de los elementos que utilicemos o de si se ocupan de evitar el ataque o incidente o recuperar el sistema una vez que este se haya producido.

#### Seguridad Activa y Pasiva

La seguridad se divide en seguridad activa y pasiva, dependiendo de los elementos utilizados para la misma, así como de la actuación que van a tener en la seguridad de los mismos.

#### Activa

Se entiende por seguridad activa todas aquellas medidas que se utilizan para detectar amenazas, y en caso de su detección generar los mecanismos adecuados para evitar el problema.

Ejemplos de seguridad activa los podemos encontrar en el empleo de contraseñas o claves de acceso, uso de antivirus, cortafuegos o firewall.

Una contraseña, cuanto más compleja sea, más segura y más difícil será descubrirla o desencriptarla, es decir, mayor fortaleza tendrá. Su longitud (8 caracteres como mínimo) y el uso conjunto de letras mayúsculas, números y caracteres especiales hacen que la seguridad de la contraseña sea mayor. No es conveniente para la seguridad de la contraseña el uso del mismo nombre de usuario, del nombre o apellido real, ni de palabras que vienen en el diccionario.

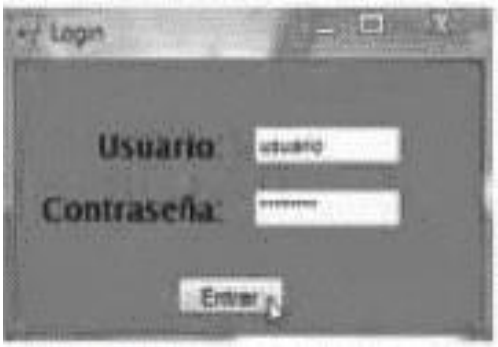


***Figura 02. Ejemplo de Acceso a un sistema.***

**Pasiva**

Está formada por las medidas que se implantan para, una vez producido el incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema; por ejemplo teniendo siempre al día copias de seguridad de los datos.

**Seguridad Física y Lógica**

**Cervigón, A; Alegre, M (2011).** Dijeron: Desde el punto de vista de la naturaleza de la amenaza, podemos hablar de seguridad a nivel físico o material o seguridad lógica o software.

**Física**

Se utiliza para proteger el sistema informático utilizando barreras físicas y mecanismos de control. Se emplea para proteger físicamente el sistema informático.

Las amenazas físicas se pueden producir provocadas por el hombre, de forma accidental o voluntaria, o bien por factores naturales.

Dentro de las provocadas por el ser humano, encontramos amenazas de tipo:

- Accidentales, como borrado accidental, olvido de la clave, etc.

- Deliberadas: como robo de la clave, robo de datos confidenciales, entre otros.

Dentro de las provocadas por factores naturales, podemos encontrar: incendios, inundaciones, etc.

Ejemplos de seguridad física del sistema informático pueden ser el uso de UPS, guardias de seguridad del edificio, alarmas, cámaras de seguridad, sistemas antincendios, extintores, climatizadores, etc.

La mayor parte de los sistemas de seguridad física se pueden encuadrar dentro de la seguridad pasiva y los de la seguridad lógica en la seguridad activa, aunque existen excepciones, como por ejemplo los controles de acceso a un edificio, climatizador, disipador de calor de los procesadores, entre otros.

**Lógica**

La seguridad lógica se encarga de asegurar la parte software de un sistema informático, que se compone de todo lo que no es físico, es decir los programas y los datos.

La seguridad lógica se encarga de controlar que el acceso al sistema informático, desde el punto de vista software, se realice correctamente y por usuarios autorizados, ya sea desde dentro del sistema informático, como desde fuera, es decir, desde una red externa, usando una VPN, la web (protocolos http, https), transmisión de ficheros (ftp), entre otros.

Dentro de la seguridad lógica, tenemos una serie de programas, o software, como el sistema operativo, que se debe encargar de controlar el acceso de los procesos o usuarios a los recursos del sistema.

Para ello debe tomar distintas medidas de seguridad. Cada vez los sistemas operativos controlan más la seguridad del equipo informático ya sea por parte de un error, por uso incorrecto del sistema operativo o del usuario, o bien por un acceso no controlado físicamente o a través de la red, o por un programa malicioso, como los virus, phishing, etc.

Es casi imposible que sea totalmente seguro, pero se pueden tomar ciertas medidas para evitar daños a la información o a la privacidad de esta. Uno de los principales peligros de un sistema informático le puede venir por internet, también por compartir información con otro equipo por la red o a través de un archivo infectado que entre en el sistema mediante una memoria secundaria, como un dispositivo de almacenamiento USB, DVD, DISCO DURO externo entre otros.

#### 2.3.2.3. Razones para la Seguridad Informática

**Cervigón, A; Alegre, M (2011).** Escribieron que: Preservar la información y la integridad de un sistema informático es algo muy importante para una empresa u organización, por lo que en pérdidas económicas y de tiempo podría suponer, sin olvidarnos del peligro que podría acarrear el acceso al sistema de un usuario no autorizado.

Igualmente, es también importante para un usuario que emplee su ordenador en el ámbito doméstico, por lo que podría

suponer el perder documentos o fotos personales, sin olvidarnos del inconveniente que supondría el no poder disponer de su equipo durante un tiempo determinado o el coste de intentar recuperar la información perdida.

Por todo lo anterior se considera muy importante la seguridad informática, que se puede definir como un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y confidencialidad de la información en un sistema informático e intentar reducir las amenazas que pueden afectar al mismo.

Dentro de la seguridad informática podemos encontrar elementos y técnicas tanto hardware, como software, así como dispositivos físicos y medios humanos.

Actualmente existen un gran número de razones para aplicar y afianzar la seguridad informática.

En los sistemas informáticos actuales prácticamente no existe el concepto de ordenador aislado como sucedía en ordenadores anteriores a la actual, sino que es extraño que un sistema informático que no esté dentro de una red de ordenadores para compartir recursos e información, así como acceso a internet, con lo cual las amenazas les pueden llegar desde el interior, así como desde el exterior, y al estar conectados en red, un ataque a un equipo, puede afectar a todo el conjunto.

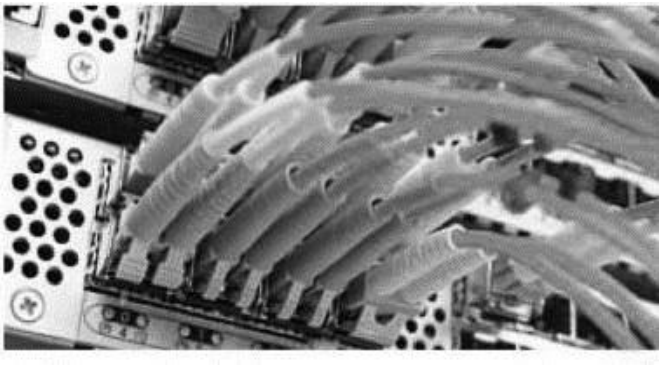

***Figura 03. Conexiones de ordenadores en red.***

Además cada día, es más frecuente realizar cualquier gestión a través de la web, ya sea de tipo personal, económica, administrativa, etc. Para estos tipos de gestiones se puede utilizar una clave de acceso, un certificado digital, o bien el DNI electrónico, entre otros, pero hay que tener cuidado y utilizar sistemas de protección cuando se envía información confidencial, como por ejemplo, el número de la tarjeta de crédito, a través de una red de ordenadores, en especial si se hace en lugares públicos.

***Figura 04. Tarjetas de Crédito.***

## Amenaza, Vulnerabilidad y Riesgo

### Amenaza

**Editex S.A (2010)**. Publicó que: En sistemas de información se entiende por amenaza la presencia de uno o más factores de diversa índole (personas, máquinas o sucesos) que de tener la oportunidad atacarían al sistema produciéndole daños aprovechándose de su nivel de vulnerabilidad. Hay diferentes tipos de amenazas de las que hay que proteger al sistema, desde las físicas como cortes eléctricos, fallos del hardware o riesgos ambientales hasta los errores intencionados o no de los usuarios, la entrada de software malicioso (virus: troyanos, gusanos) o el robo, destrucción o modificación de la información.

En función del tipo de alteración, daño o intervención que podrían producir sobre la información, las amenazas se clasifican en cuatro grupos:

- **De interrupción.** El objetivo de la amenaza es deshabilitar el acceso a la información; por ejemplo, destruyendo componentes físicos como el disco duro, bloqueando el acceso a los datos, o cortando o saturando los canales de comunicación.

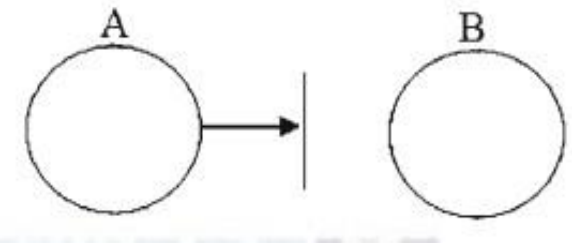


***Figura 05. Ataque de interrupción.***

- **De interceptación.** Personas, programas o equipos no autorizados podrían acceder a un determinado recurso del sistema y captar información confidencial de la organización, como pueden ser datos, programas o identidad de personas.

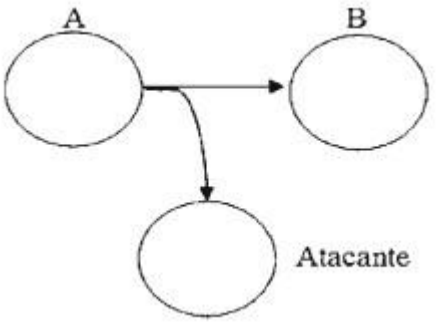


***Figura 06. Ataque de interceptación.***

- **De modificación.** Personas, programas o equipos no autorizados no solamente accederían a los programas y datos de un sistema de información sino que además los modificarían. Por ejemplo, modificar la respuesta enviada a un usuario conectado o alterar el comportamiento de una aplicación instalada.

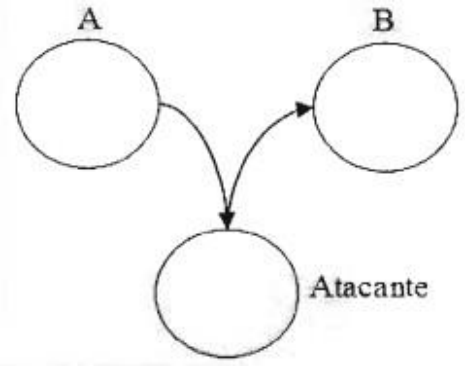


***Figura 07. Ataque de modificación.***

- **De fabricación.** Agregarían información falsa en el conjunto de información del sistema.

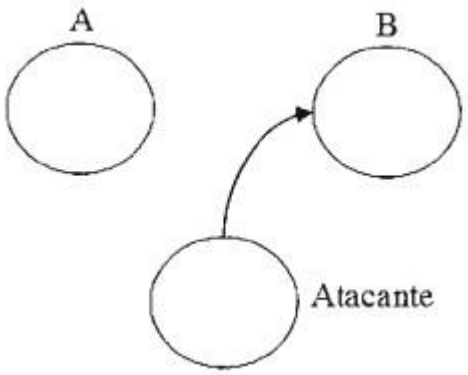


***Figura 08. Ataque de fabricación.***

Según su origen las amenazas se clasifican en:

- **Accidentales.** Accidentes meteorológicos, incendios, inundaciones, fallos en los equipos, en las redes, en los sistemas operativos o en el software, errores humanos.

- **Intencionales.** Son debidas siempre a la acción humana, como la introducción del software malicioso "malware" (aunque este penetre en el sistema por algún procedimiento automático, su origen es siempre humano), intrusión informática (con frecuencia se produce previa a la introducción de malware en los equipos), robos, hurtos. Las amenazas intencionadas pueden tener su origen en el exterior de la organización o incluso en el personal de la misma.

**Vulnerabilidad**

La vulnerabilidad es la debilidad de un recurso o grupo de recursos que son aprovechados por una o varias amenazas, es

una situación creada por la falta de uno o varios controles que eviten la amenaza, que afecta el entorno informático.

Probabilidades que existen de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a las amenazas. Por ejemplo, los datos son vulnerables a la acción de los hackers, mientras que una instalación eléctrica es vulnerable a un cortocircuito. Al hacer el análisis de riesgos hay que tener en cuenta la vulnerabilidad de cada activo.

**Riesgo**

Se denomina riesgo a la probabilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad y cuando no existe amenaza para la misma.

Ante un determinado riesgo, una organización puede optar por tres alternativas distintas:

- Asumirlo sin hacer nada. Esto solamente resulta lógico cuando el prejuicio esperado no tiene valor alguno o cuando el coste de aplicación de medidas superaría al de la reparación del daño.
- Aplicar medidas para disminuirlo o anularlo.
- Transferirlo (por ejemplo, contratando un seguro).

El riesgo se cuantifica como el resultado de multiplicar la probabilidad de que la amenaza se produzca, por el daño potencial de esta, se expresa en forma de ecuación:

**Riesgo = Probabilidad * Daño Potencial**

Es necesario tomar medidas de protección para la seguridad de las empresas sin importar si son grandes o pequeñas.

### 2.3.3. NTP-ISO/IEC 27001: 2014 - ESTANDAR RELACIONADO CON LA SEGURIDAD DE LA INFORMACIÓN

**INDECOPI (2014)**

Se aprobó la Norma Técnica Peruana, mediante la Resolución 129-2014/CNB-INDECOPI, en donde se aprueba la NTP-ISO/IEC 27001:2014 (Tecnología de la Información, Técnicas de Seguridad), habiéndose hecho efectiva al publicarse en el Diario oficial "El Peruano" el día 02 de Diciembre de 2014.

La NTP-ISO/IEC 27001:2014 (Tecnología de la Información, Técnicas de Seguridad. Sistemas de Gestión de la Información), reemplaza a la NTP-ISO/IEC 27001:2008, dejándola sin efecto..

**ISO 27001 – 2014**

Esta Norma Técnica Peruana promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, mantener y mejorar la efectividad de un ISMS (Information Security Management Systems**)** en la organización.

Una organización debe identificar y administrar varias actividades con el fin de funcionar efectivamente. Cualquier actividad que administre y use recursos para lograr la transformación de entradas en salidas, puede ser considerada un proceso. Con frecuencia la salida de un proceso se convierte en la entrada del proceso siguiente.

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación e interacciones de estos procesos y su administración se define como un “enfoque de proceso”.

El enfoque de proceso alienta a sus usuarios a enfatizar la importancia de:

a) Entender los requisitos de seguridad de información de negocios y la necesidad de establecer políticas y objetivos para la seguridad de la información.

b) Implementar y operar controles en el contexto de administrar el riesgo total del negocio de una organización.

c) Monitorear y revisar el desempeño y efectividad del ISMS.

d) Mejoramiento continuo basado en la medición de objetivos.

El modelo conocido como "Planear-Hacer-Verificar-Actuar" (CICLO DEMMING) - PDCA (Plan-Do-Check-Act), por sus siglas en inglés, puede aplicarse a todos los procesos ISMS.

## CONTENIDO DE LA NORMA ISO 27001

### 1. Introducción

La norma/estándar UNE ISO/IEC 27001: del "Sistema de Gestión de la Seguridad de la Información" es la solución de mejora continua más adecuada para evaluar los riesgos físicos (incendios, inundaciones, sabotajes, vandalismos, accesos indebidos e indeseados) y lógicos (virus informáticos, ataques de intrusión o denegación de servicios) y establecer las estrategias y controles.

### 2. Objeto

En el objeto de la Norma ISO 27001 se propone abarcar hasta qué punto puede ayudar este tipo de estándar en la organización que se va a auditar.

## 3. Referencias Normativas

La NTP-ISO/IEC 27001:2014 (Tecnología de la Información, Técnicas de Seguridad. Sistemas de Gestión de la Información), reemplaza a la NTP-ISO/IEC 27001:2008, dejándola sin efecto.

## 4. Términos y Definiciones

Para los fines de esta Norma Técnica Peruana, se aplican los siguientes términos y definiciones:

**Activo:** Algo que presenta valor para la organización.

**Disponibilidad:** Garantizar que los usuarios garantizados tengan acceso a la información y activos asociados cuando sea necesario.

**Confidencialidad:** Garantizar que la información sea accesible únicamente para quienes tengan acceso autorizado.

**Seguridad de la información:** Preservar la confidencialidad, integridad y disponibilidad de la información, además también pueden ser involucradas otras características como la autenticación, responsabilidad, no-repudio y fiabilidad.

**Evento de la seguridad de la información:** Ocurrencia identificada en un sistema, servicio o red indicando una posible brecha de la política de seguridad de la información o falla de las salvaguardas o una situación desconocida previa que puede ser relevante.

**Incidente de la seguridad de la información:** Una serie de eventos no deseados que tienen una probabilidad significativa

de comprometer operaciones del negocio y amenazar la seguridad de la información.

**Sistema de gestión de seguridad de la información – ISMS:** Es la parte del sistema integral de gestión, basado en un enfoque del riesgo del negocio para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

**Integridad:** Salvaguardar la exactitud e integridad de la información y activos asociados.

**Riesgo residual:** Riesgo remanente después de un tratamiento del riesgo.

**Aceptación del riesgo:** Decisión de aceptar el riesgo.

**Análisis del riesgo:** Uso sistemático de información para identificar amenazas y estimar el riesgo.

**Estimación del riesgo:** Proceso total de análisis y evaluación del riesgo.

**Evaluación del riesgo:** Proceso de comparación del riesgo estimado frente al criterio del riesgo para determinar el significado del riesgo.

**Gestión de riesgo:** Actividades coordinadas para dirigir y controlar el riesgo en una organización.

**Tratamiento del riesgo:** Proceso de selección e implantación de controles para minimizar el riesgo.

**Declaración de aplicabilidad:** Documento que describe los objetivos de control y los controles que son relevantes y aplicables al ISMS de la organización.

## 5. Sistema de gestión de la seguridad de la Información

En este sistema se abarca todo acerca de la seguridad de la información en la parte específica de la gestión, que interviene en ésta política y encontrar la solución más adecuada para la auditoria.

- Establecimiento y administración del ISMS.
- Implementar y operar el ISMS.
- Monitorear y revisar el ISMS.
- Mantener y mejorar el ISMS.

## 6. Responsabilidad de la Dirección

La dirección debe estar atenta a lo que ocurra con las auditorias, ya que con ello pueden tomar medidas para poder prevenir posibles fallos en la seguridad informática.

## 7. Auditorías internas de SGSI

El objetivo primordial de este tipo de auditoria de SGSI es averiguar si hay algo que se está realizando mal, de manera objetiva, el auditor debe ser una persona capacitada y atenta en lo que está ocurriendo en la empresa.

## 8. Revisión del SGSI por la Dirección

Este paso es muy importante, ya que la dirección también debe formar parte del proyecto, para lo cual se realizan reuniones planificadas para dar puntos de vista y recomendaciones.

## 9. Mejora de SGSI

Mediante la mejora continua del SGSI, se evitaran que se produzcan errores y para ello se desarrollaran medidas preventivas, que representan una forma de corregir las cosas antes que se generen problemas.

## 10. ANEXO A. Resumen de controles.

Para este caso el anexo se va a cumplir, es el anexo A. Éste anexo es, probablemente, el anexo más nombrado de todas las normas de gestión, el objetivo del anexo A, contiene los siguientes puntos:

- A.5 Política de la seguridad.
- A.7 Gestión de activos.
- A.8 Seguridad relacionada con el personal
- A.9 Seguridad física y entorno.
- A11 Control de acceso.
- A13 Estrategias de solución.

**CICLO DEMMING**

- **Planificar**

Incluyen determinar metas, objetivos y determinar métodos para alcanzar las metas es:

- Definición de políticas y objetivos.
- Determinación del alcance.
- Valoración de activos.
- Análisis de Riesgo.

- Gestionar riesgos.
- Seleccionar controles ISO 1779:2005.

- **Hacer**

Incluyen asegurar la educación y el entrenamiento e implementar el trabajo, estas son:

- Definir e implementar Plan de Gestión de Riesgo.
- Implementar controles sancionados y sus indicadores.
- Implementar sistema de gestión.

- **Chequear**

Consiste en verificar los efectos de la implementación, estos son:

- Revisión gerencial.
- Desarrollar procesos de monitorización.
- Revisar regularmente el SGSI.
- Revisar los niveles de riesgo.
- Auditar internamente el SGSI.

- **Actuar**

Consiste en tomar la acción apropiada estos son:

- Implementar las mejoras.
- Adoptar acciones preventivas y correctivas.
- Comunicar acciones y resultados.
- Verificar que las mejoras cumplan el objetivo.

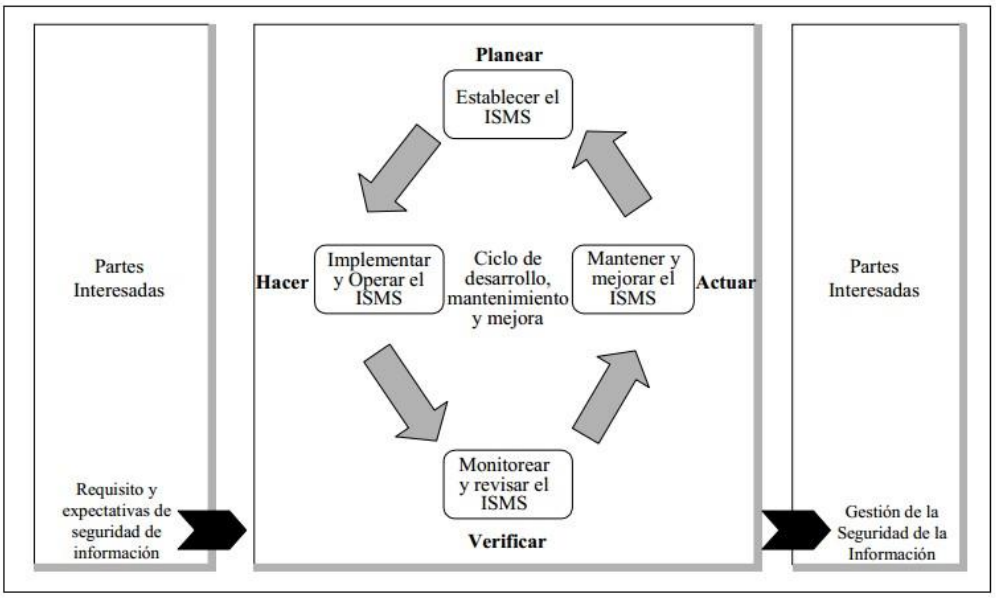


***Figura 9. Modelo PDCA (ciclo Demming).***

## 2.4. DEFINICIÓN CONCEPTUALES (TÉRMINOS BÁSICOS)

- **ANTIVIRUS: Programas** para detectar y desinfectar virus en un sistema operativo.

- **APLICACIONES:** Servicios disponibles para un usuario.

- **CONTROL:** Oír, revisar cuentas, examen de gestión para saber el estado de alguna organización.

- **BASE DE DATOS:** Colección de información organizada de forma que un programa de ordenador pueda seleccionar rápidamente los fragmentos de datos que necesite. Una base de datos es un sistema de archivos electrónico.

- **CIFRADA:** Transcrita en letras o símbolos alguna información que se quiere ocultar.

- **CONEXIÓN: Enlace**, empalme. Acción y efecto de conectar y conectarse.

- **CONFIDENCIALIDAD:** Mantener información secreta, privada.

- **COPIAS DE SEGURIDAD:** Hacer copias de documentos, archivos y otra información importante.

- **DESENCRIPTARLA:** Traducir a un lenguaje común información oculta.

- **DIRECTIVA:** Conjunto de Instrucciones.

- **DISPONIBILIDAD:** Elementos disponibles, alcanzables siempre que se requiera.

- **EMISIÓN:** Acción y efecto de emitir, poner en circulación.

- **FIREWALL:** Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

- **(FTP):** En informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red.

- **HACKERS:** Persona con grandes conocimientos de informática que se dedica a acceder ilegalmente a sistemas informáticos ajenos y a manipularlos.

- **HARDWARE: Conjunto** de elementos físicos o materiales que constituyen una computadora o un sistema informático.

- **INTEGRIDAD:** Asegurar que alguna información no sea alterada.

- **INTRUSIÓN:** Que se ha introducido sin derecho ni permiso.

- **MALWARE:** Código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario.

- **MAN-IN-THE-MIDDLE:** Es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.

- **PHISHING:** Tipo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta.

- **PREVENTIVAS:** Preparar, prevenir, advertir, disponer con anticipación las cosas necesarias para un fin.

- **PROTOCOLO:** Conjunto de reglas y normas que permiten que dos o más entidades de un sistema de comunicación se comuniquen entre ellos para transmitir información por medio de cualquier tipo de variación de una magnitud física.

- **PUERTOS:** Es una forma genérica de denominar a una interfaz a través de la cual los diferentes tipos de datos se pueden enviar y recibir.

- **RED:** Es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas.

- **RIESGO:** Contingencia o proximidad de un daño.

- **SERVIDORES: Es** un nodo que forma parte de una red, provee servicios a otros nodos denominados clientes.

- **SOFTWARE:** Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

- **TOPOLOGIAS:** La forma en que está diseñada la red, sea en el plano físico o lógico.

- **UPS:** Es una fuente de suministro eléctrico que posee un batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica.

- **VPN:** Es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet.

## 2.5. FORMULACIÓN DE HIPÓTESIS

### 2.5.1. HIPÓTESIS GENERAL

El diseño de un Sistema Informático basado en la ISO 27001, si permite la seguridad para el manejo de información en el Órgano de Control Institucional en la Municipalidad Provincial de Huaura – Huacho.

### 2.5.2. HIPÓTESIS ESPECÍFICA

- El diseño de un Sistema Informático basado en la ISO 27001, con una buena Gestión de Activos Informáticos, si permite alinearse a las políticas de Seguridad Informática en la Oficina de Control Institucional de la Municipalidad Provincial Huaura-Huacho.

- El diseño de un Sistema Informático basado en la ISO 27001, con una buena Seguridad relacionada con los Recursos Humanos, si permite alinearse a las políticas de Seguridad Informática en la Oficina de Control Institucional de la Municipalidad Provincial Huaura-Huacho.

- El diseño de un Sistema Informático basado en la ISO 27001, con un buen Control de Accesos, si permite alinearse a las políticas de Seguridad Informática en la Oficina de Control Institucional de la Municipalidad Provincial Huaura-Huacho.

# 3. METODOLOGÍA

## 3.1. DISEÑO METODOLÓGICO

La investigación es de un diseño no experimental, pues la variable independiente no se va a manipular deliberadamente; es decir se observan hechos que ya se han presentado en el área del fenómeno estudiado.

### 3.1.1. TIPO DE INVESTIGACIÓN

La investigación es de tipo transversal, porque se recopilan datos en un tiempo único o en un momento dado (2018).

### 3.1.2. NIVEL

La investigación es descriptiva, porque se especificará las bondades del diseño de un modelo de auditoría informática basado en ISO 27001. Buscando incidir en el alineamiento de las Políticas de Seguridad Informática en la Municipalidad Provincial de Huaura – Huacho.

Correlacional, que tiene como propósito describir las variables y analizar su incidencia e interrelación en un momento dado. Se examinó la situación actual de la Municipalidad Provincial de Huaura - Huacho, se identificó problemas y se recolectó información acerca de las posibles alternativas de solución.

### 3.1.3. ENFOQUE

Para desarrollar la investigación se sigue el modelo Cuantitativo y Aplicado debido a las siguientes características:

- Porque se ponderaron los datos del cuestionario que se realizó en los Órganos de administrativos de la Municipalidad Provincial de Huaura - Huacho. (Cuantitativa).

- Se busca de la utilización de teorías, conocimientos que pueda modificar, reformar o cambiar el aspecto de la realidad. (Aplicada).

## 3.2. POBLACIÓN Y MUESTRA.

### 3.2.1. POBLACIÓN

La población, objeto de investigación está constituida por los trabajadores de la Oficina de Control Institucional de la Municipalidad Provincial de Huaura, que tienen acceso a toda la información requerida para la Seguridad de dicha Información y acceso a los diferentes sistemas de información de la Municipalidad, a los que se realizó la encuesta; siendo 7 personas (2018).

### 3.2.2. MUESTRA

La muestra es la misma población por ser finita. Los datos se recolectaron mediante una encuesta, al ser aplicado sobre las variables independientes, recogí su medida para luego ser decodificada y así permitir realizar el análisis.

## 3.3. OPERACIONALIZACIÓN DE VARIABLES E INDICADORES

### 3.3.1 VARIABLE 1

**Variable independiente:** SISTEMA INFORMATICO

Es la evaluación de políticas de seguridad en general para tener segura la información en el Órgano de Control de la Municipalidad.

| Dimensiones | Indicadores |
|---|---|
| Gestión de activos informáticos | Inventario de activos<br>Propiedad de los inventarios<br>Uso de activos |
| Seguridad de recursos humanos | Roles de los trabajadores<br>Concientización Derechos<br>de acceso |
| Control de accesos | Gestión de privilegios<br>Control de conexión a redes |

### 3.3.1 VARIABLE 2

**Variable dependiente:** SEGURIDAD PARA EL MANEJO DE INFORMACION

Es alinear las políticas internas de Seguridad de la Municipalidad con la NTP para mejorar su seguridad en el manejo de información.

| Dimensiones | Indicadores |
|---|---|
| **Confidencial** | Copias de seguridad<br>Acceso a información<br>Acceso a la sala de servidores |
| **Disponible**. | Información a tiempo<br>Copias de seguridad |
| **Integro** | Alterar información |

## 3.4. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

### 3.4.1. TÉCNICAS A EMPLEAR

Las técnicas para la obtención de la información que se necesitó para el desarrollo de esta investigación fueron:

- Observación.
- Análisis documental
- Entrevista
- Encuestas

### 3.4.2. DESCRIPCIÓN DE LOS INSTRUMENTOS

**Observación:** Se aplica para observar todo lo relacionado con el área informática y los sistemas de la organización con el propósito de percibir, examinar, o analizar los eventos que se presentan en el desarrollo de las actividades del área o de un sistema que permita evaluar el cumplimiento de las funciones, operaciones y procedimientos.

**Análisis Documental:** Con la finalidad de obtener un fundamento del problema de investigación para el presente trabajo de estudio, se revisará las fuentes escritas (textos, tesis, etc.) vinculadas al tema de estudio.

**Entrevista:** Se entrevistará al jefe del Órgano de Control y al Jefe del Área de Informática de la Municipalidad Provincial de Huaura - Huacho, también a algunos trabajadores de la entidad para poder averiguar todos los inconvenientes que se presentan.

**Encuesta:** Se elaborará un cuestionario de preguntas tipo Likert que serán respondidas por los trabajadores del Órgano de Control y otros trabajadores de la Municipalidad Provincial Huaura – Huacho.

## 3.5. TÉCNICAS PARA EL PROCESAMIENTO DE LA INFORMACIÓN

Para analizar los datos recogidos con los instrumentos anteriores, se utilizará la estadística descriptiva para el procesamiento de datos, haciendo uso del programa SPSS, que nos permitirá la comprobación de la hipótesis respectiva.

# 4. RESULTADOS

## 4.1. GESTIÓN Y PROPUESTAS

Este trabajo de investigación referente a modelos de Seguridad para el manejo de información, me parece importante dedicarlo a la investigación de factores de protección informática, mostrando y describiendo los métodos de protección, conociendo los tipos y medios de ataque a nuestro sistema de información.

Las empresas tienen riesgo de perder información, esto podría detener su operación, deteniendo procesos de producción o administrativos, para ello es necesario proteger el funcionamiento de la información, existen diferentes maneras o métodos de proteger un sistema de información, todas estas partes del sistema de seguridad deben trabajar en conjunto para asegurar la informática de la empresa.

La seguridad informática existe solo si se juntan todos los elementos y métodos que la hacen posible ya que cualquier método utilizado por sí solo no puede abarcar todos los puntos vulnerables de los sistemas de información, así lo da a entender, Hallberg (2003, p.97). “La seguridad informática solo brinda áreas de oportunidad, en los sistemas informáticos y no brinda por si sola seguridad en la información de la organización, la seguridad informática, no puede por sí misma proporcionar la protección para su información”. De acuerdo con el autor, es porque se pretende mostrar los puntos de protección en una empresa que usa una red de datos local para compartir y automatizar su información.

Se pretende describir por que las empresas cuidan la información, de qué manera lo hacen, que es la seguridad informática, conceptualizando una teoría general de la seguridad lógica, física e ingeniería social, y mediante ejemplos básicos y prácticos que hablen de seguridad lógica, es decir, como instalar un antivirus, un firewall y un sistema de actualizaciones de sistema operativo Windows, para proteger la información.

Se describe los puntos más importantes en la seguridad informática, como ya se dijo como lo son firewall, antivirus, conductas del usuario, seguridad informática física, ingeniería social, esto para crear una idea completa de los factores que tienen que ver con la seguridad informática.

Para lograr defender al sistema de información es necesario cubrir dos temas determinantes: Formar y Concientizar, la primera es explicar a los usuarios como consigue un hacker engañarle y como reconocer un ataque, es decir que se limite a utilizar el sistema como herramienta de trabajo, es decir, no compartir con nadie accesos, como usuarios y contraseñas, ya que son para uso personal. Concientizar, es probarles que este tipo de ataques es cada vez más frecuente y es por lo general el primer recurso que se utiliza cuando se quiere corromper la seguridad.

Además es necesario retroalimentar esta información y recordar periódicamente a los usuarios, esta medida es recomendada por muchos autores sobre seguridad de la información ya que respalda el trabajo previo de la ingeniería social, por eso es recomendable informar constantemente a los usuarios, (Jean-Marc Royer, 2001, p368) “La sensibilización respecto a los riesgos informáticos debe realizarse de forma recurrente, todos los años es necesario volver a formar al personal, ya que con el tiempo, no viendo ninguna alerta se instala una rutina y la atención se relaja”.

En el presente proyecto de fin de carrera se ha realizado una investigación de las normas y estándares internacionales (ISO 21007), rescatándose los aspectos más saltantes de cada norma y estándar, relacionados a la información.

## 4.2. POLÍTICAS DE MEJORAS PARA LOS ENCARGADOS DE LA INFORMÁTICA

- Apoyar la implementación de un modelo de seguridad para el manejo de la información y alentar al cumplimiento de los estándares, procedimientos y controles apropiados para los sistemas de información.
- Realizar sus funciones con objetividad, debida diligencia y celo profesional, de acuerdo con las normas y mejores prácticas profesionales.
- Servir a los intereses de las partes relevantes de manera diligente, leal y honesta, manteniendo altos estándares de conducta y carácter, y no ser parte de ninguna actividad deshonrosa para la profesión.
- Mantener la privacidad y confidencialidad de la información obtenida en el transcurso de sus funciones a menos que la autoridad legal requiera su divulgación. Dicha información no deberá ser usada para beneficio personal ni divulgada a las partes que no correspondan.
- Mantener la competencia en sus respectivos campos y acordar realizar sólo aquellas actividades que de modo razonable puedan esperar cumplir con competencia profesional.
- Informar a las partes apropiadas los resultados del trabajo realizado; revelando todos los hechos significativos de los que tengan conocimiento.
- Apoyar la educación profesional de los interesados para mejorar su comprensión en seguridad y control de sistemas de información.

## 4.3. RESULTADOS METODOLÓGICOS

### 4.3.1. VALIDEZ DEL INSTRUMENTO

La validez del instrumento (Ver Anexo B – Instrumento para la toma de datos) de la presente investigación, se realizó por medio del juicio de expertos, en donde ellos evaluaron y a criterio propio calificaron el contenido del cuestionario empleado. Los expertos que realizaron fueron los siguientes:

Experto 1: Dr. Sosa Palomino, Alcibíades Flamencio- CIP N° 60431

Experto 2: Ing. Barrenechea Alvarado, Julio C. – CIP N° 98989

Experto 3: Mg. Morales Escobar, Delvis Beder – CIP N° 107525

Las calificaciones para los criterios de validación, que se mencionan en la hoja de juicio de experto (Ver Anexo B – Juicio de Expertos) con respecto al contenido del instrumento, se muestran en la siguiente tabla:

**Tabla 01: Calificación de los Expertos**

| N° PREGUNTA Y ALTERNATIVAS | EXPERTOS | | | TA |
|---|---|---|---|---|
| | E1 | E2 | E3 | |
| Pregunta N° 1 y sus alternativas | 1 | 1 | 1 | **3** |
| Pregunta N° 2 y sus alternativas | 1 | 0 | 1 | **2** |
| Pregunta N° 3 y sus alternativas | 1 | 1 | 1 | **3** |
| Pregunta N° 4 y sus alternativas | 1 | 1 | 0 | **2** |
| Pregunta N° 5 y sus alternativas | 1 | 1 | 1 | **3** |
| Pregunta N° 6 y sus alternativas | 1 | 1 | 1 | **3** |
| Pregunta N° 7 y sus alternativas | 1 | 1 | 1 | **3** |
| Pregunta N° 8 y sus alternativas | 0 | 1 | 1 | **2** |
| Pregunta N° 9 y sus alternativas | 1 | 1 | 1 | **3** |
| Pregunta N° 10 y sus alternativas | 1 | 0 | 1 | **2** |
| Pregunta N° 11 y sus alternativas | 1 | 1 | 1 | **3** |
| Pregunta N° 12 y sus alternativas | 1 | 1 | 1 | **3** |
| Pregunta N° 13 y sus alternativas | 1 | 1 | 1 | **3** |
| Pregunta N° 14 y sus alternativas | 1 | 1 | 1 | **3** |
| **Totalmente de Acuerdo (TA) =** | **13** | **12** | **13** | **38** |

Dónde: 1 = Totalmente de Acuerdo (TA)
0 = Totalmente en Desacuerdo (TD)

FUENTE: Elaboración propia

**CÁLCULO DEL COEFICIENTE DE VALIDEZ:**

$$\text{Validez} = \frac{\text{Total de Acuerdo}}{\text{Total de Acuerdo (TA)} + \text{Total de Desacuerdo (TD)}}$$

$$\text{Validez} = \frac{38}{38+4} = 0{,}90 = 90\%$$

FUENTE: Elaboración propia

Con una validez general de **90%** según la escala de validez el instrumento tiene excelente validez; Modelo de Seguridad para el manejo de Información (Ver Tabla 02), de acuerdo al criterio de los expertos.

**Tabla 02: Calificación de los Expertos**

| ESCALA | INDICADOR |
|---|---|
| 0.00 – 0.53 | Validez nula |
| 0.54 – 0.64 | Validez baja |
| 0.65 – 0.69 | Válida |
| 0.70 – 0.80 | Muy válida |
| 0.81 – 0.94 | Excelente validez |
| 0.95 – 1.00 | Validez perfecta |

Fuente: Herrera, 1988

### 4.3.2. CONFIABILIDAD DEL INSTRUMENTO

Se realizó el análisis de fiabilidad en el programa estadístico SPSS Statistics 22.0 al instrumento aplicado a todos los trabajadores del Órgano de Control y Área de Informática (07 trabajadores) de la Municipalidad Provincial de Huaura –Huacho.

Se obtuvo una fiabilidad de 0,739 (ver Tabla 03), este instrumento estuvo conformado por 14 items, distribuidos para la **variable independiente: Seguridad Informática,** en 3 dimensiones (Gestión de activos informáticos, Seguridad de Recursos Humanos y Control de Accesos) y para la **variable dependiente: Alineamiento de Políticas de Seguridad Informática**, 3 dimensiones (Confidencialidad, Disponible e Integro).

**Tabla 03: Alpha de Cronbach aplicado al Instrumento**

| Alpha de Cronbach | N° de elementos |
|---|---|
| 0.739 | 14 |

Fuente: Elaboración propia

Esto quiere decir que el instrumento tiene una valoración de muy confiable según la escala de Herrera (1998), como se muestra a continuación en la tabla 04.

**Tabla 04: Escala de confiabilidad**

| ESCALA | INDICADOR |
|---|---|
| 0.00 – 0.53 | Confiabilidad nula |
| 0.54 – 0.64 | Confiabilidad baja |
| 0.65 – 0.69 | Confiable |
| 0.70 – 0.80 | Muy confiable |
| 0.81 – 0.94 | Excelente confiabilidad |
| 0.95 – 1.00 | Confiabilidad perfecta |

Fuente: Herrera, 1988

### 4.3.3. TABLAS Y GRÁFICOS ESTADÍSTICOS

**Tabla 05: ¿Se realiza el inventariado de recursos informáticos en las fechas establecidas?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | nunca | 2 | 28,6 | 28,6 | 28,6 |
| | a veces | 5 | 71,4 | 71,4 | 100,0 |
| | Total | 7 | 100,0 | 100,0 | |

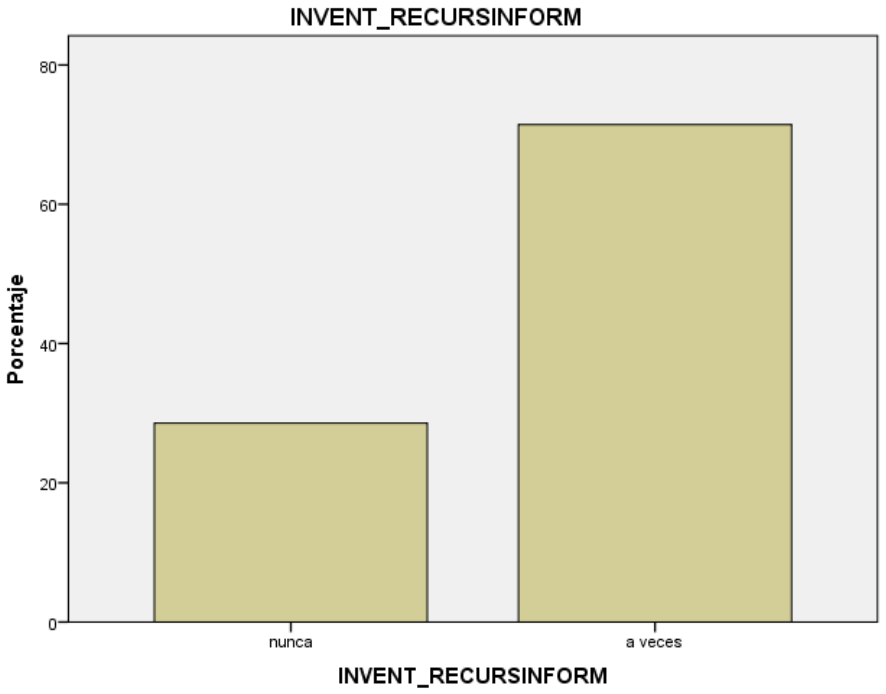


**Figura N° 10: Inventariado de recursos informáticos en las fechas establecidas.**

**Interpretación:**

Se debe dar siempre el inventariado, pero resulta que en la mayoría de casos se da a veces, seguido por nunca.

**Tabla 06: ¿ Los recursos informáticos son propiedad de la Municipalidad?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | a veces | 2 | 28,6 | 28,6 | 28,6 |
| | siempre | 5 | 71,4 | 71,4 | 100,0 |
| | Total | 7 | 100,0 | 100,0 | |

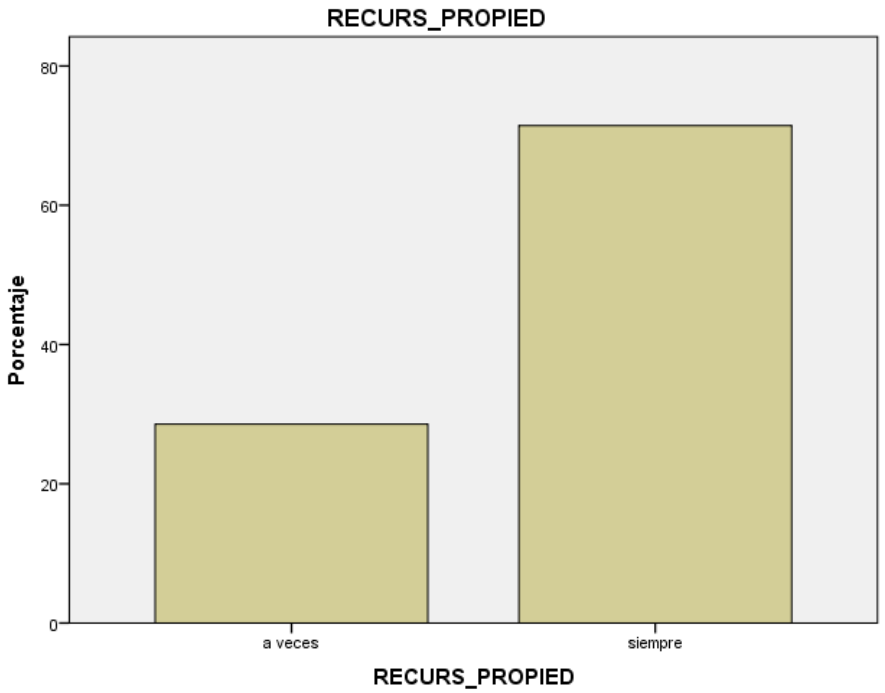


**Figura N° 11: Recursos informáticos: propiedad de la Municipalidad.**

**Interpretación:**

Si debe ser siempre propiedad de la municipalidad, pero se nota que a veces no lo es.

**Tabla 07: ¿Ha intentado arreglar su computadora por su propia cuenta?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | nunca | 4 | 57,1 | 57,1 | 57,1 |
| | a veces | 2 | 28,6 | 28,6 | 85,7 |
| | siempre | 1 | 14,3 | 14,3 | 100,0 |
| | Total | 7 | 100,0 | 100,0 | |

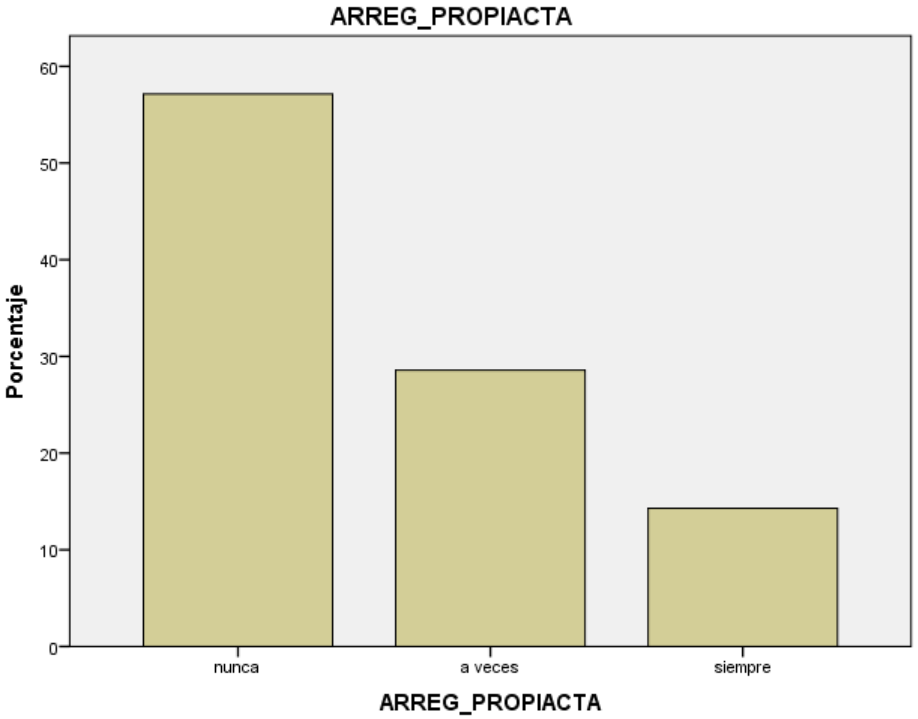


**Figura N° 12: Arregla su computadora por su propia cuenta.**

**Interpretación:**

En la mayoría de veces nunca se arregla la computadora por propia cuenta.

**Tabla 08: ¿Conoce usted la función que debe desempeñar?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | a veces | 4 | 57,1 | 57,1 | 57,1 |
| | siempre | 3 | 42,9 | 42,9 | 100,0 |
| | Total | 7 | 100,0 | 100,0 | |

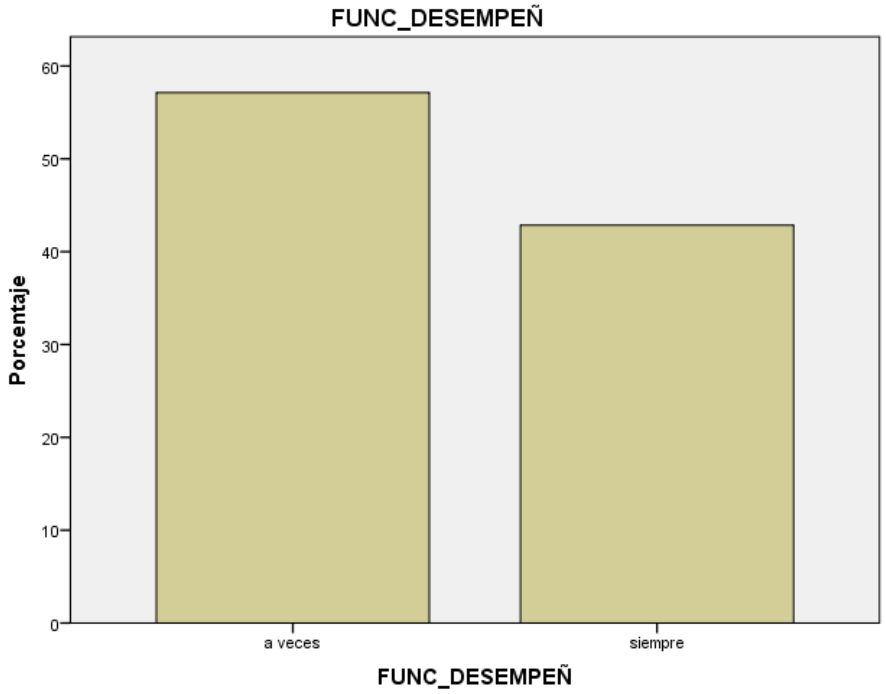


**Figura N° 13: Conocimiento de funciones de desempeños.**

**Interpretación:**

Sucede que deberíamos saber siempre nuestras verdaderas funciones, pero a veces se llevó la mayor parte.

**Tabla 09: ¿Se dictan capacitaciones a los trabajadores para la seguridad Informática?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | nunca | 2 | 28,6 | 28,6 | 28,6 |
| | a veces | 4 | 57,1 | 57,1 | 85,7 |
| | siempre | 1 | 14,3 | 14,3 | 100,0 |
| | Total | 7 | 100,0 | 100,0 | |

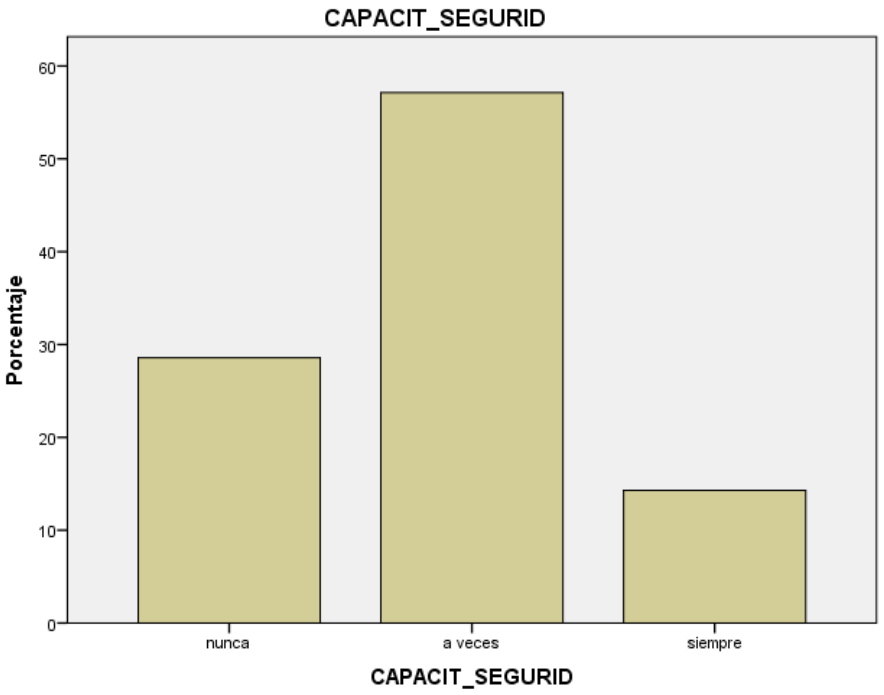


**Figura N° 14: Capacitaciones de trabajadores para la seguridad Informática.**

**Interpretación:**

Las capacitaciones deberán ser constantes (siempre) pero sucede que en la mayoría de casos se da a veces.

**Tabla 10: ¿Accede a los sistemas de información de la municipalidad?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | nunca | 1 | 14,3 | 14,3 | 14,3 |
| | a veces | 5 | 71,4 | 71,4 | 85,7 |
| | siempre | 1 | 14,3 | 14,3 | 100,0 |
| | Total | 7 | 100,0 | 100,0 | |

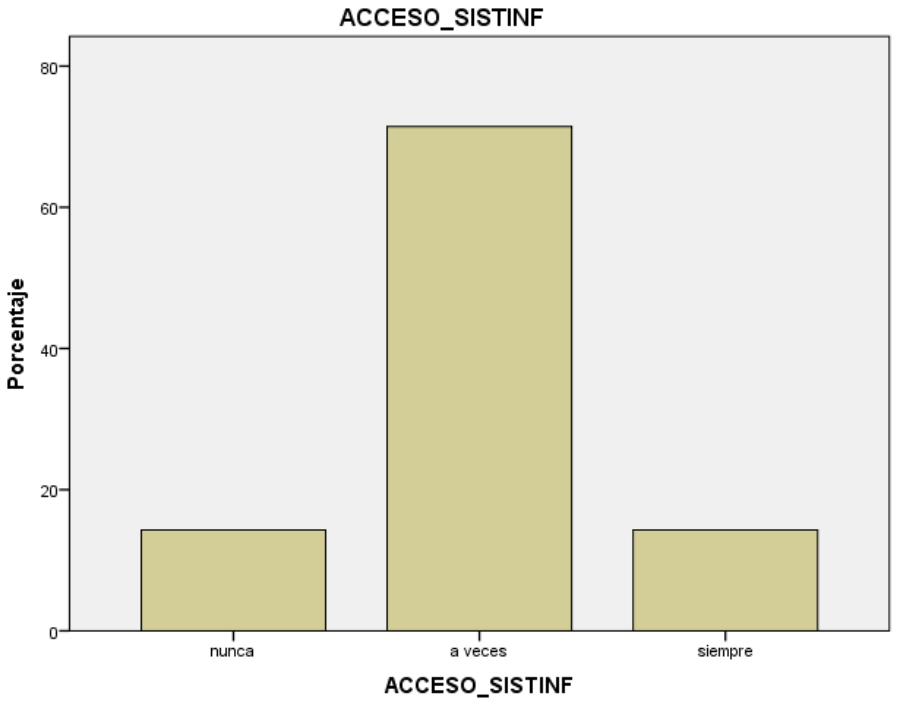


**Figura N° 15: Acceso a los sistemas de información de la municipalidad.**

**Interpretación:**

Conforme se requiera tendremos acceso a los sistemas de información (a veces), aunque no es homogéneos otros dijeron nunca o siempre.

**Tabla 11: ¿Monitorean constantemente los privilegios de acceso a los usuarios?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | nunca | 2 | 28,6 | 28,6 | 28,6 |
| | a veces | 4 | 57,1 | 57,1 | 85,7 |
| | siempre | 1 | 14,3 | 14,3 | 100,0 |
| | Total | 7 | 100,0 | 100,0 | |

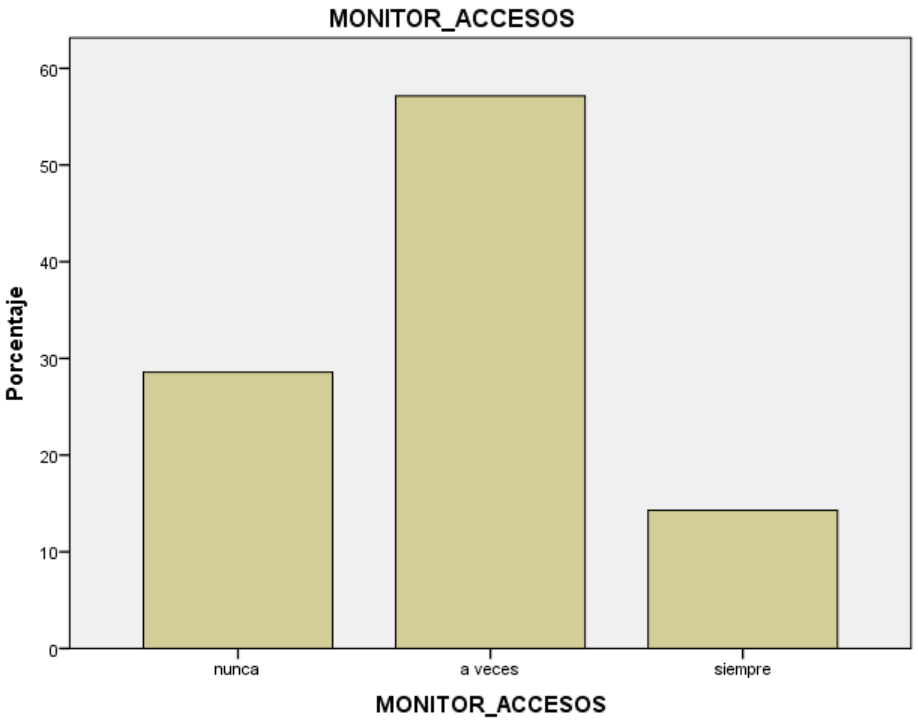


**Figura N° 16: Monitoreo: privilegios de acceso a los usuarios.**

**Interpretación:**

En la mayoría de los casos se da a veces, aunque otros dicen nunca o siempre.

**Tabla 12: ¿Tiene acceso a internet a través de su celular?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | a veces | 7 | 100,0 | 100,0 | 100,0 |

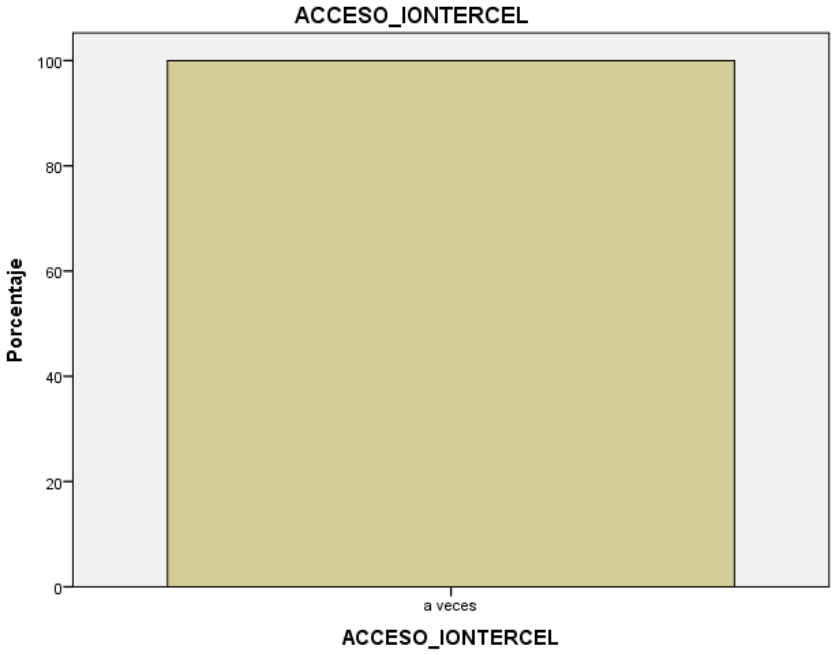


**Figura N° 17: Acceso a internet a través de su celular.**

**Interpretación:**

Todos señalaron a veces, dejando sin efecto las otras 2 posibilidades.

**Tabla 13: ¿Las copias de seguridad están al alcance de los demás trabajadores?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | nunca | 2 | 28,6 | 28,6 | 28,6 |
| | a veces | 4 | 57,1 | 57,1 | 85,7 |
| | siempre | 1 | 14,3 | 14,3 | 100,0 |
| | Total | 7 | 100,0 | 100,0 | |

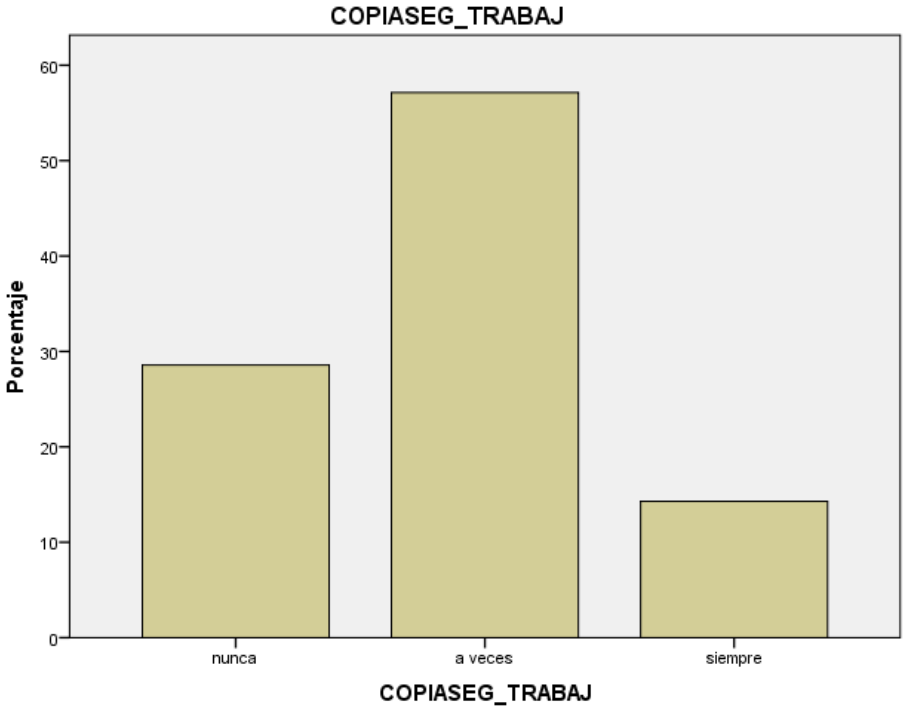


**Figura N° 18: Copias de seguridad al alcance de los demás trabajadores.**

**Interpretación:**

No debería ocurrir, pero dijeron que a veces es el caso mas fuerte.

**Tabla 14: ¿Puede entrar a la sala de servidores personal no autorizado?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | nunca | 4 | 57,1 | 57,1 | 57,1 |
| | a veces | 3 | 42,9 | 42,9 | 100,0 |
| | Total | 7 | 100,0 | 100,0 | |


**Figura N° 19: Acceso a la sala de servidores personal no autorizado.**

**Interpretación:**

Debería quedar consolidado el nunca, pero suele sucedes a veces tener acceso a la sala de servidores.

**Tabla 15: ¿Cualquier trabajador puede llevarse información en USB, cd, etc?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | nunca | 4 | 57,1 | 57,1 | 57,1 |
| | a veces | 3 | 42,9 | 42,9 | 100,0 |
| | Total | 7 | 100,0 | 100,0 | |

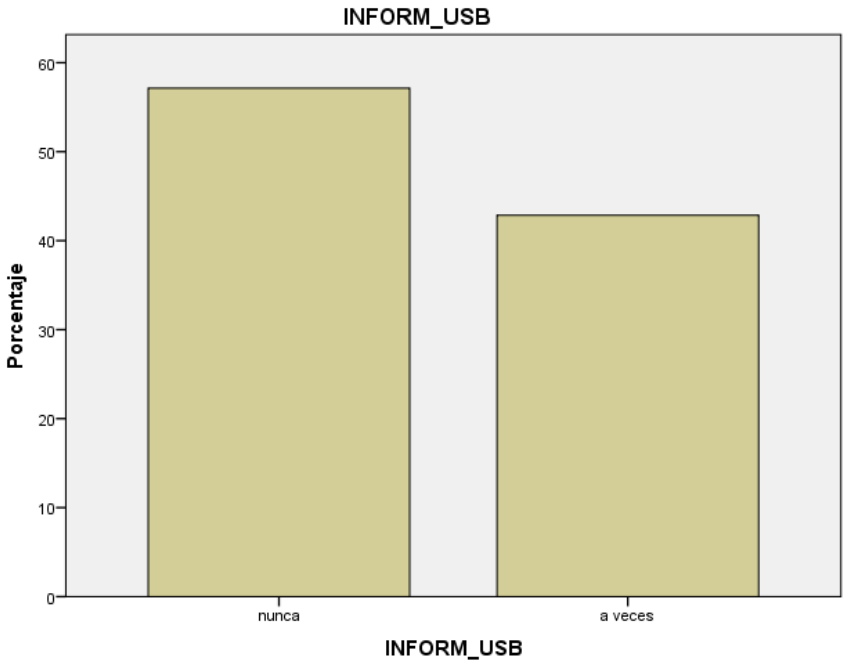


**Figura N° 20: Cualquier trabajador puede llevarse información en USB, cd, etc.**

**Interpretación:**

En la mayoría de veces nunca, y se nota que a veces sale información.

**Tabla 16: ¿Cuándo la gerencia pide información al departamento de informática, se le brinda a tiempo?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | a veces | 5 | 71,4 | 71,4 | 71,4 |
| | siempre | 2 | 28,6 | 28,6 | 100,0 |
| | Total | 7 | 100,0 | 100,0 | |

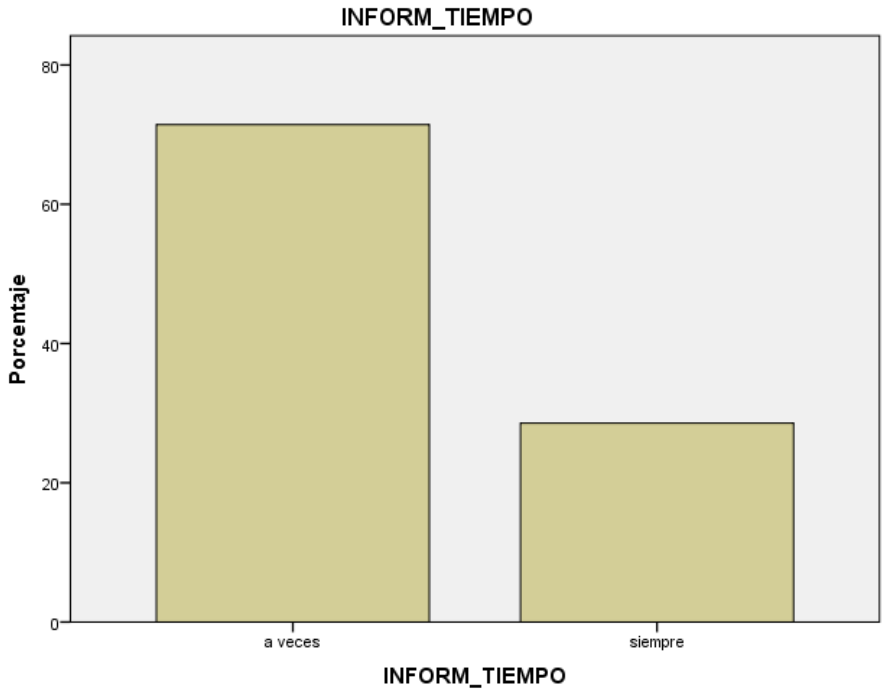


**Figura N° 21: Gerencia pide información al departamento de informática, (tiempo).**

**Interpretación:**

Aceptable el resultado, aunque debería ser lógico que siempre y a tiempo se debe atender a la Gerencia.

**Tabla 17: ¿Cuándo se requiere utilizar las copias de seguridad, están disponibles?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | nunca | 1 | 14,3 | 14,3 | 14,3 |
| | a veces | 5 | 71,4 | 71,4 | 85,7 |
| | siempre | 1 | 14,3 | 14,3 | 100,0 |
| | Total | 7 | 100,0 | 100,0 | |

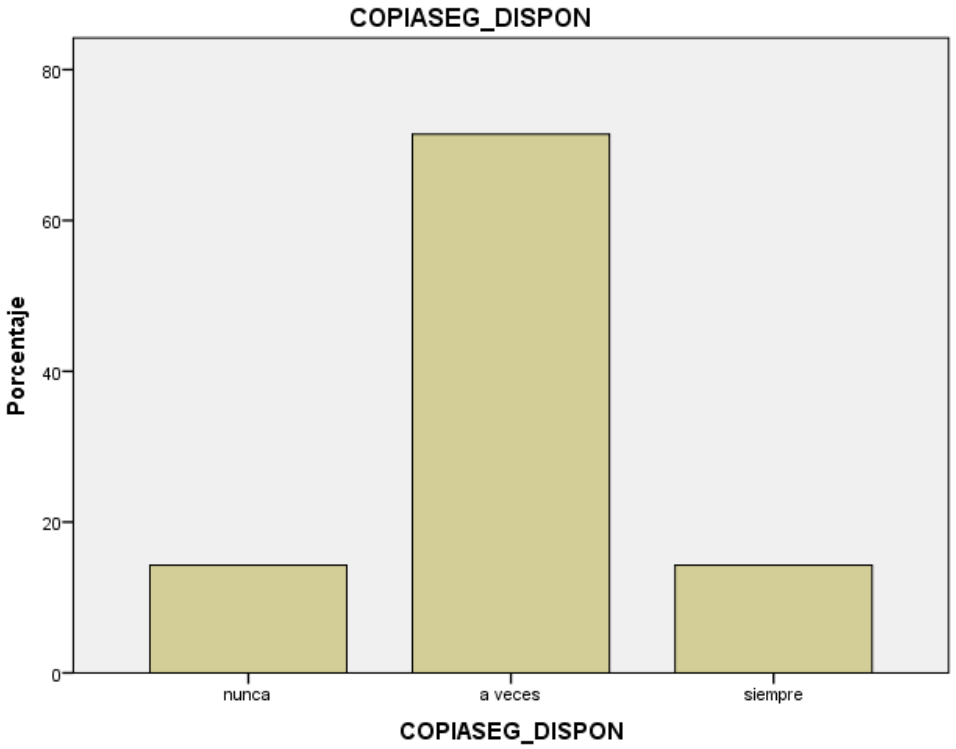


**Figura N° 22: Copias de seguridad - están disponibles.**

**Interpretación:**

En la mayoría de casos se da a veces (aunque debería ser siempre lo más lógico).

**Tabla 18: ¿Todos los encargados del área de informática pueden modificar, eliminar o cambiar la información en la base de datos?**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válidos | nunca | 3 | 42,9 | 42,9 | 42,9 |
| | a veces | 4 | 57,1 | 57,1 | 100,0 |
| | Total | 7 | 100,0 | 100,0 | |

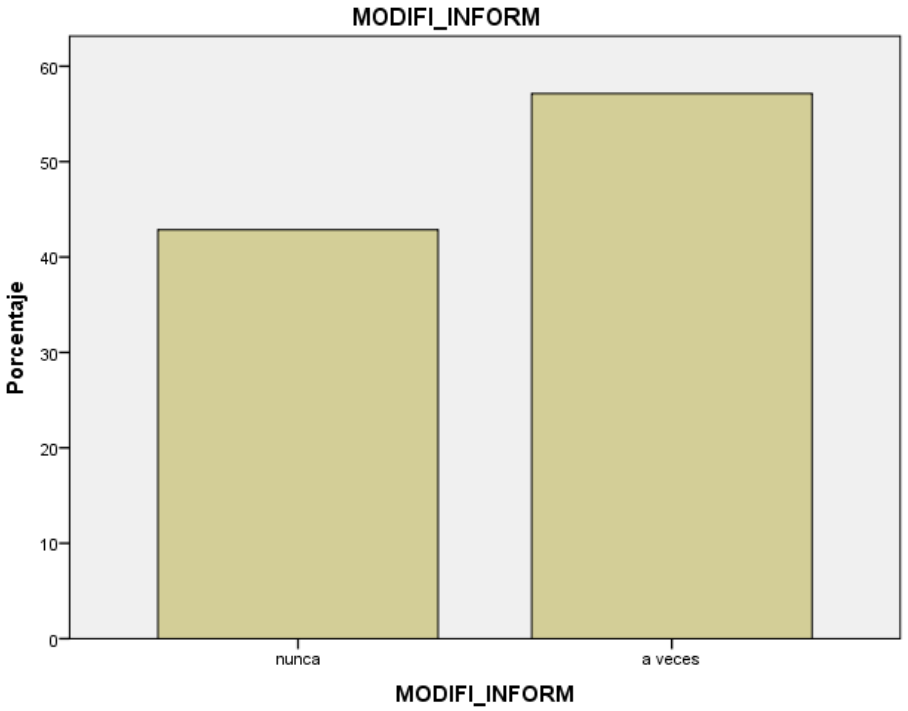


**Figura N° 23: Todos los encargados del área de informática pueden modificar, eliminar o cambiar la información en la base de datos.**

**Interpretación:**

Estaría de acuerdo con nunca, pero se nota que a veces todos podrían modificar, cambiar o eliminar información valiosa.

### 4.3.4. CONTRASTACIÓN DE HIPÓTESIS

En la realización de la contratación de hipótesis se empleó la data obtenida del cuestionario Modelo de Auditoría ISO 21007 y Seguridad Informática, donde se obtuvo las respuestas a las 14 preguntas planteadas, contestadas según escala de Likert, siendo (1) nunca, (2) a veces y (3) siempre.

## 1. PRUEBA DE HIPÓTESIS DE INDICADORES X1 – Y

**Hn:** El diseño de un Sistema Informático basado en la ISO27001, con un buen Control de accesos, NO permita alinearse a las políticas de Seguridad Informática en el Órgano de Control Institucional de la Municipalidad Provincial Huaura-Huacho.

**Ha:** El diseño de un Sistema Informático basado en la ISO27001, con un buen Control de accesos, permita alinearse a las políticas de Seguridad Informática en la Órgano de Control Institucional de la Municipalidad Provincial Huaura-Huacho.

**Tabla N° 19 de contingencia X1 * RESUMEN_Y (agrupado)**

Recuento

| | | RESUMEN_Y (agrupado) | | Total |
|---|---|---|---|---|
| | | nunca | a veces | |
| GESTIÓN ACTIVOS | nunca | 8 | 0 | 8 |
| | a veces | 0 | 4 | 4 |
| | siempre | 2 | 0 | 2 |
| | Total | 10 | 4 | 14 |

Variab. Independiente: X
Seguridad Informática

X1:
Valoración de la 1ra. Dimensión de la V.I. (Gestión de activos Informáticos)

Variab. Dependiente: Y
Alineamiento de Políticas de Seguridad Informática
RESUMEN_Y (agrupado):
Valoración del promedio de las tres dimensiones de la V.D. (Y1, Y2 y Y3)

**Tabla N° 20: Pruebas de chi-cuadrado**

| | Valor | gl | Sig. asintótica (bilateral) |
|---|---|---|---|
| Chi-cuadrado de Pearson | 14,000[a] | 2 | ,001 |
| Razón de verosimilitudes | 16,752 | 2 | ,000 |
| Asociación lineal por lineal | 1,800 | 1 | ,180 |
| N de casos válidos | 14 | | |

a. 5 casillas (83,3%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es ,57.

Interpretación:

Como el Nivel de Significación de muestra es **0.001**, menor al **0.05**, se Rechaza la Hipótesis Nula y en su lugar Acepta la Hipótesis Alternativa, es decir, El diseño de un Sistema Informático basado en la ISO 27001, con un buen control de accesos, permita alinearse a las políticas de Seguridad Informática en el Órgano de Control Institucional de la Municipalidad Provincial Huaura-Huacho.

## 2. PRUEBA DE HIPÓTESIS DE INDICADORES X2 – Y

**Hn:** El diseño de un Sistema Informático basado en la ISO 27001, con una buena seguridad relacionada con los Recursos Humanos, NO permita alinearse a las políticas de Seguridad Informática en el Órgano de Control Institucional de la Municipalidad Provincial Huaura-Huacho.

**Ha:** El diseño de un Sistema Informático basado en la ISO 27001, con una buena seguridad relacionada con los Recursos Humanos, permita alinearse a las políticas de Seguridad Informática en el Órgano de Control Institucional de la Municipalidad Provincial Huaura-Huacho.

**Tabla N° 21 de contingencia X2 * RESUMEN_Y (agrupado)**

Recuento

| | | RESUMEN_Y (agrupado) | | Total |
|---|---|---|---|---|
| | | nunca | a veces | |
| SEGUR-REC_HUM | a veces | 8 | 0 | 8 |
| | siempre | 2 | 4 | 6 |
| Total | | 10 | 4 | 14 |

Variab. Independiente: X
Sesuridad Informática

X2:
Valoración de la 2da. Dimensión de la V.I. (Seguridad de Recursos Humanos)

Variab. Dependiente: Y
Alineamiento de Políticas de Seguridad Informática
RESUMEN_Y (agrupado):
Valoración del promedio de las tres dimensiones de la V.D. (Y1, Y2 y Y3)

**Tabla N° 22 Pruebas de chi-cuadrado**

| | Valor | gl | Sig. asintótica (bilateral) | Sig. exacta (bilateral) | Sig. exacta (unilateral) |
|---|---|---|---|---|---|
| Chi-cuadrado de Pearson | 7,467[a] | 1 | ,006 | | |
| Corrección por continuidad[b] | 4,557 | 1 | ,033 | | |
| Razón de verosimilitudes | 9,113 | 1 | ,003 | | |
| Estadístico exacto de Fisher | | | | ,015 | ,015 |
| Asociación lineal por lineal | 6,933 | 1 | ,008 | | |
| N de casos válidos | 14 | | | | |

a. 3 casillas (75,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 1,71.

b. Calculado sólo para una tabla de 2x2.

Interpretación:

Como el Nivel de Significación de muestra es **0.006**, menor al **0.05**, se Rechaza la Hipótesis Nula y en su lugar Acepta la Hipótesis Alternativa, es decir, El diseño de un Sistema Informático basado en la ISO 27001, con una buena seguridad relacionada con los Recursos Humanos, permite alinearse a las políticas de Seguridad Informática en el Órgano de Control Interno de la Municipalidad Provincial Huaura-Huacho.

## 3. PRUEBA DE HIPÓTESIS DE INDICADORES X3 – Y

**Hn:** El diseño de un Sistema Informático basado en la ISO 27001, con un buen Control de Accesos Informáticos, NO permite alinearse a las políticas de Seguridad Informática en el Órgano de Control Institucional de la Municipalidad Provincial Huaura-Huacho.

Ha: El diseño de un Sistema Informático basado en la ISO 27001, con un buen Control de Accesos Informáticos, permite alinearse a las políticas de Seguridad Informática en el Órgano de Control Institucional de la Municipalidad Provincial Huaura-Huacho.

**Tabla N° 23 de contingencia X3 * RESUMEN_Y (agrupado)**

Recuento

| | | RESUMEN_Y (agrupado) | | Total |
|---|---|---|---|---|
| | | nunca | a veces | |
| CONTROL DE ACCESOS | nunca | 4 | 0 | 4 |
| | a veces | 4 | 4 | 8 |
| | siempre | 2 | 0 | 2 |
| Total | | 10 | 4 | 14 |

Variab. Independiente: X
Seguridad Informática

X3:
Valoración de la 3ra. Dimensión de la V.I. (Control de accesos)

Variab. Dependiente: Y
Alineamiento de Políticas de Seguridad Informática

RESUMEN_Y (agrupado):
Valoración del promedio de las tres dimensiones de la V.D. (Y1, Y2 y Y3)

**Tabla N° 24 Pruebas de chi-cuadrado**

| | Valor | gl | Sig. asintótica (bilateral) |
|---|---|---|---|
| Chi-cuadrado de Pearson | 4,200[a] | 2 | ,122 |
| Razón de verosimilitudes | 5,661 | 2 | ,059 |
| Asociación lineal por lineal | ,260 | 1 | ,610 |
| N de casos válidos | 14 | | |

a. 5 casillas (83,3%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es ,57.

Interpretación:

Como el Nivel de Significación de muestra es **0.122**, mayor al **0.05**, se Acepta la Hipótesis Nula y en su lugar Rechaza la Hipótesis Alternativa, es decir, El diseño de un Sistema Informático basado en la ISO 27001, con un buen Control de Accesos, NO permite alinearse a las políticas de Seguridad Informática en el Órgano de Control Institucional de la Municipalidad Provincial Huaura-Huacho.

## 4. PRUEBA DE HIPÓTESIS DE INDICADORES X – Y

**Tabla N° 25 de contingencia RESUMEN_X (agrupado) * RESUMEN_Y (agrupado)**

Recuento

| | | RESUMEN_Y (agrupado) | | Total |
|---|---|---|---|---|
| | | nunca | a veces | |
| RESUMEN_X (agrupado) | nunca | 6 | 0 | 6 |
| | a veces | 4 | 4 | 8 |
| Total | | 10 | 4 | 14 |

Variab. Independiente: X
Auditoría Informática

RESUMEN_X (agrupado):
del promedio de las tres dimensiones de la V.I. (X1, X2 y X3)

Variab. Dependiente: Y
Alineamiento de Políticas de Seguridad Informática

RESUMEN_Y (agrupado): Valoración
Valoración del promedio de las tres dimensiones de la V.D. (Y1, Y2 y Y3)

**Tabla N° 26 Pruebas de chi-cuadrado**

| | Valor | gl | Sig. asintótica (bilateral) | Sig. exacta (bilateral) | Sig. exacta (unilateral) |
|---|---|---|---|---|---|
| Chi-cuadrado de Pearson | 4,200[a] | 1 | ,040 | | |
| Corrección por continuidad[b] | 2,107 | 1 | ,147 | | |
| Razón de verosimilitudes | 5,661 | 1 | ,017 | | |
| Estadístico exacto de Fisher | | | | ,085 | ,070 |
| Asociación lineal por lineal | 3,900 | 1 | ,048 | | |
| N de casos válidos | 14 | | | | |

a. 3 casillas (75,0%) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 1,71.

b. Calculado sólo para una tabla de 2x2.

Interpretación:

Como el Nivel de Significación de muestra es **0.040**, menor al **0.05**, se Rechaza la Hipótesis Nula y en su lugar Acepta la Hipótesis Alternativa, es decir, El diseño de un Sistema Informático basado en la ISO 27001, permite el alineamiento de las Políticas de Seguridad Informática en el Órgano de Control Institucional de la Municipalidad Provincial de Huaura – Huacho.

## RESUMEN, ANÁLISIS E INTERPRETACIÓN DE LA PHE

**Tabla N° 27**

| CONTRASTACIONES | DECISIÓN | |
|---|---|---|
| | **H. NULA** | **H. ALTERNATIVA** |
| Buena gestión de activos / Seguridad Informática | . . . . . | Se Acepta |
| Buena seguridad con los Relac. Human./ Seguridad Informática | . . . . . | Se Acepta |
| Buen control de accesos/ Seguridad Informática | Se Acepta | . . . . . |

Sobre los Indicadores establecidos en nuestra Investigación, se encuentra que entre ellos existe varios resultados **de Relación y No Relación**, es decir con una Probabilidad del **95%,** en la primera y segunda prueba de hipótesis, se tiene la Aceptación de la Hipótesis Alternativa, mientras que en la tercera prueba se tiene la Aceptación de la Hipótesis Nula, lo que nos conduce a una Aceptación por mayoría de las Hipótesis Alternativas.

**POR LO TANTO:**

En las tres pruebas de hipótesis, se encuentra que en su mayoría se Acepta la Hipótesis Alternativa, dando paso al Rechazo de la Hipótesis Nula, con lo que se confirma la ACEPTACIÓN DE LA HIPÓTESIS PRINCIPAL, es decir que El diseño de un Sistema Informático basado en la ISO 27001, con una buena Gestion de Activos Informáticos si se relaciona con las Políticas de Seguridad Informática en el Organo de Control Institucional de la Municipalidad Provincial de Huaura – Huacho.

# 5. CONCLUSIONES Y RECOMENDACIONES

## 5.1. CONCLUSIONES:

- En general concluimos que si los usuarios de los sistemas de información ya sean expertos o inexpertos no están enterados de los métodos y elementos que componen la seguridad informática y los aplican en conjunto no se podrá cumplir la seguridad informática y podemos confirmar nuestra idea principal de investigación la cual menciona que: La seguridad en las tecnologías de la información se ve amenazada cuando se desconocen los métodos de seguridad informática.
- Para desarrollar el presente proyecto de tesis se aplicó los conocimientos de los cursos de Seguridad de la Información, Sistemas de Información, Sistemas de Control y Auditoria de Sistemas de Información, Administración de las Funciones Informáticas, Seguridad Computacional, Temas Avanzados en Tecnología de la Información, entre otros. Además se cumplió con el objetivo de desarrollar un proyecto de fin de carrera en un año académico.
- Del problema principal, El diseño de un Sistema Informático basado en la ISO 27001, modelo que identifica los riesgos, las amenazas y las vulnerabilidades que afectan y dañan la información confidencial del Órgano de Control Institucional de la Municipalidad, mostrando y describiendo los métodos de protección, conociendo los tipos y medios de ataque a nuestro sistema de información; permite alinearse a las Políticas de Seguridad Informática en la Municipalidad Provincial de Huaura – Huacho.
- Del objetivo general, El diseño de un Modelo de Sistema Informático basado en la ISO 27001, se relaciona con las Políticas de Seguridad Informática en el Órgano de Control Institucional de la Municipalidad Provincial de Huaura – Huacho; pues el modelo, forma (explica a los usuarios las vulnerabilidades que son expuestas la información) y concientiza (probar que si es dañino para la información).

- De la hipótesis general, a través de la prueba chi cuadrado de Pearson, dado que la probabilidad "p" (el Nivel de Significación) muestra un **0.040**, siendo menor al **0.05**, entonces se rechaza la $H_0$, es decir, El diseño de un modelo de Sistema Informático basado en la ISO 27001, permite el alineamiento de las Políticas de Seguridad Informática en el Órgano de Control Institucional de la Municipalidad Provincial de Huaura – Huacho.

## 5.2. RECOMENDACIONES.

- Se recomienda que los usuarios de los sistemas de información ya sean expertos o inexpertos estén enterados de los métodos y elementos que componen la seguridad informática y aplicándolos en conjunto se podrá cumplir con la seguridad informática, así se podrá confirmar nuestra idea principal de investigación la cual menciona que: La seguridad en las tecnologías de la información se ve amenazada cuando se desconocen los métodos de seguridad informática.
- Es de necesidad el diseño y la inmediata implementación del Sistema Informático basado en la ISO 27001, pues este modelo que identifica los riesgos, las amenazas y las vulnerabilidades solucionaran y resguardaran la información confidencial del Órgano de Control Institucional de la Municipalidad, mostrando y describiendo los métodos de protección, conociendo los tipos y medios de ataque a nuestro sistema de información; alineándose a las Políticas de Seguridad Informática en la Municipalidad Provincial de Huaura – Huacho.
- Debe considerarse como prioritario diseño de un Modelo de Sistema Informático basado en la ISO 27001, relacionado a las Políticas de Seguridad Informática en el Órgano de Control Institucional de la Municipalidad Provincial de Huaura – Huacho; con ello se logra la invulnerabilidad de la información.
- Se recomienda que las Políticas de Seguridad Informática viables y aplicables para el Órgano de Control de la Municipalidad sean identificadas descritas y aplicadas.

# 6. FUENTES DE INFORMACION

## 6.1. FUENTES BIBLIOGRAFICAS


**Aldegani**, G. (1997). Seguridad informática. Mp Ediciones.

**Ampuero,** C (2011). Tesis titulada Diseño De Un Sistema De Gestión De Seguridad De Información Para Una Compañía De Seguros. Perú.

**Cadme**, C; Duque, D (2012). Tesis titulada Auditoría de Seguridad Informática ISO 27001 para la empresa de alimentos ITALIMENTOS CIA.LTDA. Ecuador.

**Cervigón**, A; Alegre, M (2011). Seguridad Informática. Madrid, España.

**Córdova**, N (2008). Tesis titulada Plan de Seguridad Informática para una Entidad Financiera. Perú.

**Echenique**, J (2008). Auditoria en Informática segunda. México.

**Editorial Editex** S.A (2010).Seguridad Informática. Madrid, españa.

**INDECOPI** (2009).EDI. Tecnología de la Información. Técnicas de seguridad Sistemas de Gestión de Seguridad de la Información. NTP-ISO/IEC 17799-2008.Lima, Perú.

**Lázaro,** M (2008). Seguridad de la Información. Oficina Nacional de Gobierno Electrónico e Informática PCM. Perú.

**Martínez**, V (2010). Tesis titulada Concientización En Seguridad De La Información, La Estrategia Para Fortalecer El Eslabón Más Débil De La Cadena. Colombia.

**Monzón**, C. (2009). Auditoria de seguridad de redes inalámbricas de área local Wireless Local Área Network (WLAN). Universidad Mayor de San Andrés. Bolivia.

**Muñoz**, C (2010). Auditoría en Sistemas Computacionales. México.

**Piattini**, M (2001). Auditoria informática. Un enfoque Práctico. Ra-Ma.

**Reyes**, M (2011). Tesis titulada Propuestas para impulsar la seguridad informática en materia de educación. México.

**Villena**, M (2006). Tesis titulada "Sistema De Gestión De Seguridad De Información Para Una Institución Financiera". Perú.

## 6.2. FUENTES HEMEROGRAFICAS

Diario El Peruano

Actualidad Empresarial

## 6.3. FUENTES DOCUMENTALES

Tesis de Estudiantes, Caballero Bustamante Manual de Contabilidad 123

## 6.4. FUENTES ELECTRONICAS

PAGINA WEB DE LA CONTRALORIA GENERAL DE LA REPUBLICA.
http://www.buenastareas.com/materias/politicas-y-procedimientos-control

**ANEXO B**

# VALIDACIÓN DEL INSTRUMENTO

**UNIVERSIDAD NACIONAL**

**JOSÉ FAUSTINO SÁNCHEZ CARRIÓN**

---

**VALIDACIÓN CON JUICIO DE EXPERTO:** ENCUESTA GENERAL

**TEMA:** "ELABORACION DEMODELO DE SEGURIDAD PARA EL MANEJO DE INFORMÁCION EN EL ORGANO DE CONTROL INSTITUCIONAL, MUNICIPALIDAD PROVINCIAL DE HUAURA – HUACHO".

**OPINIÓN O JUICIO DE EXPERTO:**

1. La opinión que Ud. nos brinde es Personal, Sincera y Anónima.
2. Marque con un aspa "X" dentro del cuadrado de Opinión, sólo a una vez por pregunta ó ítems de la Encuesta, la que Ud. considere válidada.

**OPINIÓN: DA: De Acuerdo ( 1 ) ED: En Desacuerdo ( 0 ).**

| PREGUNTAS y ALTERNATIVAS | OPINIÓN | |
|---|---|---|
| | DA | ED |
| Pregunta N° 1 y sus alternativas | | |
| Pregunta N° 2 y sus alternativas | | |
| Pregunta N° 3 y sus alternativas | | |
| Pregunta N° 4 y sus alternativas | | |
| Pregunta N° 5 y sus alternativas | | |
| Pregunta N° 6 y sus alternativas | | |
| Pregunta N° 7 y sus alternativas | | |
| Pregunta N° 8 y sus alternativas | | |
| Pregunta N° 9 y sus alternativas | | |
| Pregunta N° 10 y sus alternativas | | |
| Pregunta N° 11 y sus alternativas | | |
| Pregunta N° 12 y sus alternativas | | |
| Pregunta N° 13 y sus alternativas | | |
| Pregunta N° 14 y sus alternativas | | |

Muchas Gracias por su Respuesta

_____

Datos y Firma del Juez Experto 1

# VALIDACIÓN DEL INSTRUMENTO

**UNIVERSIDAD NACIONAL**

**JOSÉ FAUSTINO SÁNCHEZ CARRIÓN**

**VALIDACIÓN CON JUICIO DE EXPERTO:** ENCUESTA GENERAL

**TEMA:** "ELABORACION DE MODELO DE SEGURIDAD PARA EL MANEJO DE INFORMÁCION EN EL ORGANO DE CONTROL INSTITUCIONAL, MUNICIPALIDAD PROVINCIAL DE HUAURA – HUACHO".

**OPINIÓN O JUICIO DE EXPERTO:**

3. La opinión que Ud. nos brinde es Personal, Sincera y Anónima.
4. Marque con un aspa "X" dentro del cuadrado de Opinión, sólo a una vez por pregunta ó ítems de la Encuesta, la que Ud. considere válidada.

**OPINIÓN: DA: De Acuerdo ( 1 ) ED: En Desacuerdo ( 0 ).**

| PREGUNTAS y ALTERNATIVAS | OPINIÓN | |
|---|---|---|
| | DA | ED |
| Pregunta N° 1 y sus alternativas | | |
| Pregunta N° 2 y sus alternativas | | |
| Pregunta N° 3 y sus alternativas | | |
| Pregunta N° 4 y sus alternativas | | |
| Pregunta N° 5 y sus alternativas | | |
| Pregunta N° 6 y sus alternativas | | |
| Pregunta N° 7 y sus alternativas | | |
| Pregunta N° 8 y sus alternativas | | |
| Pregunta N° 9 y sus alternativas | | |
| Pregunta N° 10 y sus alternativas | | |
| Pregunta N° 11 y sus alternativas | | |
| Pregunta N° 12 y sus alternativas | | |
| Pregunta N° 13 y sus alternativas | | |
| Pregunta N° 14 y sus alternativas | | |

Muchas Gracias por su Respuesta

_____

Datos y Firma del Juez Experto 2

# VALIDACIÓN DEL INSTRUMENTO

**UNIVERSIDAD NACIONAL**

**JOSÉ FAUSTINO SÁNCHEZ CARRIÓN**

**VALIDACIÓN CON JUICIO DE EXPERTO:** ENCUESTA GENERAL

**TEMA**"ELABORACION DE MODELO DE SEGURIDAD PARA EL MANEJO DE INFORMÁCION EN EL ORGANO DE CONTROL INSTITUCIONAL, MUNICIPALIDAD PROVINCIAL DE HUAURA – HUACHO".

**OPINIÓN O JUICIO DE EXPERTO:**

5. La opinión que Ud. nos brinde es Personal, Sincera y Anónima.
6. Marque con un aspa "X" dentro del cuadrado de Opinión, sólo a una vez por pregunta ó ítems de la Encuesta, la que Ud. considere válidada.

**OPINIÓN: DA: De Acuerdo ( 1 ) ED: En Desacuerdo ( 0 ).**

| PREGUNTAS y ALTERNATIVAS | OPINIÓN | |
|---|---|---|
| | DA | ED |
| Pregunta N° 1 y sus alternativas | | |
| Pregunta N° 2 y sus alternativas | | |
| Pregunta N° 3 y sus alternativas | | |
| Pregunta N° 4 y sus alternativas | | |
| Pregunta N° 5 y sus alternativas | | |
| Pregunta N° 6 y sus alternativas | | |
| Pregunta N° 7 y sus alternativas | | |
| Pregunta N° 8 y sus alternativas | | |
| Pregunta N° 9 y sus alternativas | | |
| Pregunta N° 10 y sus alternativas | | |
| Pregunta N° 11 y sus alternativas | | |
| Pregunta N° 12 y sus alternativas | | |
| Pregunta N° 13 y sus alternativas | | |
| Pregunta N° 14 y sus alternativas | | |

Muchas Gracias por su Respuesta

_____

Datos y Firma del Juez Experto 3

**ANEXO C**

# ENCUESTA

**UNIVERSIDAD NACIONAL JOSÉ FAUSTINO SÁNCHEZ CARRIÓN**

**CUESTIONARIO DE ENCUESTA PARA MEDIR LA SEGURIDAD PARA EL MANEJO DE INFORMÁCION EN EL ORGANO DE CONTROL INSTITUCIONAL DE LA MUNICIPALIDAD PROVINCIAL DE HUAURA – HUACHO".**

**A.- Presentación:**

Estimado (a) trabajador del Órgano de Control Institucional de la Municipalidad Provincial de Huaura - Huacho, el presente cuestionario es parte de una investigación que tiene por finalidad obtener información, acerca de la Seguridad Informática. Respuestas personales que solamente, son de gran importancia para nuestra investigación y que serán procesadas con toda confidencialidad, respetando el anonimato en la presentación de los resultados.

**B.- Indicaciones:**

- ✓ Este cuestionario es anónimo. Por favor responda con sinceridad.
- ✓ Lea detenidamente cada ítem. Cada uno tiene tres respuestas, de las cuales sólo seleccione una.
- ✓ Conteste a las preguntas marcando con una "X" en un solo recuadro que, según su opinión. La escala de calificación es la siguiente:

  3 = SIEMPRE

  2 = A VECES

  1 = NUNCA

| Ítem | ***Variable Independiente*: Auditoria Informática** | **S** | **A** | **N** |
|---|---|---|---|---|
| | ***Gestión de Activos Informáticos*** | | | |
| 1 | *¿Se realiza el inventariado de recursos informáticos en las fechas establecidas?* | | | |
| 2 | *¿Los recursos informáticos son propiedad de la municipalidad?* | | | |
| 3 | *¿Ha intentado arreglar su computadora por su propia cuenta?* | | | |
| **Ítem** | ***Seguridad de Recursos Humanos.*** | **S** | **A** | **N** |
| 4 | *¿Conoce usted la función que debe desempeñar?* | | | |
| 5 | *¿Se dictan capacitaciones a los trabajadores para la seguridad Informática?* | | | |
| 6 | *¿Accede a los sistemas de información de la municipalidad?* | | | |
| **Ítem** | ***Control de Accesos.*** | **S** | **A** | **N** |
| 7 | *¿Monitorean constantemente los privilegios de acceso a los usuarios?* | | | |
| 8 | *¿Tiene acceso a internet a través de su celular?* | | | |
| **Ítem** | ***Variable Dependiente*: Alineamiento de políticas de seguridad informática** | **S** | **A** | **N** |
| | ***Confidencial*** | | | |
| 9 | *¿Las copias de seguridad están al alcance de los demás trabajadores?* | | | |
| 10 | *¿Puede entrar a la sala de servidores personal no autorizado?* | | | |
| 11 | *¿Cualquier trabajador puede llevarse información en USB, cd, etc?* | | | |
| **Ítem** | ***Disponible.*** | **S** | **A** | **N** |
| 12 | *¿Cuándo la gerencia pide información al departamento de informática, se le brinda a tiempo?* | | | |
| 13 | *¿Cuándo se requiere utilizar las copias de seguridad, están disponibles?* | | | |
| **Ítem** | ***Integro.*** | **S** | **A** | **N** |
| 14 | *¿Todos los encargados del área de informática pueden modificar, eliminar o cambiar la información en la base de datos?* | | | |

**Gracias por tu colaboración**

## ANEXO D.

MATRIZ DE ALPHA DE CRONBACH

[Conjunto_de_datos0] C:\Users\USER\Desktop\INFORMACION PARA TESIS\CALCULOS

### Resumen del procesamiento de los casos

| | | N | % |
|---|---|---|---|
| Casos | Válidos | 7 | 100,0 |
| | Excluidos[a] | 0 | ,0 |
| | Total | 7 | 100,0 |

a. Eliminación por lista basada en todas las variables del procedimiento.

**Estadísticos de fiabilidad**

| Alfa de Cronbach | N de elementos |
|---|---|
| ,739 | 14 |

**Estadísticos total-elemento**

| | Media de la escala si se elimina el elemento | Varianza de la escala si se elimina el elemento | Correlación elemento-total corregida | Alfa de Cronbach si se elimina el elemento |
|---|---|---|---|---|
| INVENT_RECURSINFORM | 25,00 | 12,000 | ,690 | ,692 |
| RECURS_PROPIED | 24,00 | 13,667 | ,185 | ,740 |
| ARREG_PROPIACTA | 25,14 | 10,810 | ,607 | ,687 |
| FUNC_DESEMPEÑ | 24,29 | 11,238 | ,850 | ,670 |
| CAPACIT_SEGURID | 24,86 | 10,476 | ,810 | ,660 |
| ACCESO_SISTINF | 24,71 | 13,571 | ,157 | ,745 |
| MONITOR_ACCESOS | 24,86 | 11,810 | ,482 | ,708 |
| ACCESO_IONTERCEL | 24,71 | 14,571 | ,000 | ,743 |
| COPIASEG_TRABAJ | 24,86 | 12,143 | ,406 | ,718 |
| SALASERV_PERSNAUT | 25,29 | 11,238 | ,850 | ,670 |
| INFORM_USB | 25,29 | 16,571 | -,525 | ,803 |
| INFORM_TIEMPO | 24,43 | 15,619 | -,333 | ,783 |
| COPIASEG_DISPON | 24,71 | 13,905 | ,077 | ,753 |
| MODIFI_INFORM | 25,14 | 11,810 | ,674 | ,690 |

# ANEXO A

## MATRIZ DE CONSISTENCIA

**ELABORACION DE MODELO DE SEGURIDAD PARA EL MANEJO DE INFORMACION EN EL ORGANO DE CONTROL INSTITUCIONAL, MUNICIPALIDAD PROVINCIAL DE HUAURA – HUACHO**

| PROBLEMA | OBJETIVOS | HIPÓTESIS | VARIABLES - DIMENSIONES | INDICADORES |
|---|---|---|---|---|
| **PROBLEMA GENERAL:**<br>¿Cómo el diseño de un modelo de la Auditoría Informática basado en la ISO 27001, permitirá al Órgano de Control Institucional de la Municipalidad Provincial de Huaura – Huacho tener seguridad en el manejo de información de dicho Órgano de Control Institucional? | **OBJETIVO GENERAL:**<br>Diseñar un Sistema Informático basado en la ISO 27001, que permita al Órgano de Control Institucional de la Municipalidad Provincial de Huaura – Huacho tener seguridad en el manejo de la información de dicho Órgano de Control Institucional.<br>. | **HIPÓTESIS GENERAL:**<br>El diseño de un Sistema Informático basado en la ISO 27001, si permite la seguridad para el manejo de información en el Órgano de Control Institucional en la Municipalidad Provincial de Huaura – Huacho. | **Variable Independiente:**<br>SISTEMA INFORMATICO<br>**Dimensiones:**<br>- Gestión de activos informáticos<br>- Seguridad de recursos humanos<br>- Control de accesos | Indicadores de Variable Independiente:<br>Inventario de activos.<br>Propiedad de los inventarios.<br>Uso de activos.<br>Roles de los trabajadores.<br>Concientización.<br>Derechos de acceso.<br>Gestión de privilegios.<br>Control de conexión a redes. |
| **PROBLEMAS ESPECÍFICOS:**<br>¿En qué medida el diseño de un Sistema Informático basado en la ISO 27001, con una buena Gestión de activos Informáticos, permitirá el alineamiento de Políticas de Seguridad para el manejo de la información de dicho Órgano de Control Institucional?<br><br>¿De qué manera el diseño de un modelo de un Sistema Informático basado en la ISO 27001, con una buena seguridad relacionada con los Recursos Humanos, permitirá el buen manejo de información en el Órgano de Control Institucional?<br><br>¿Cómo el diseño de un modelo de un Sistema Informático basado en la ISO 27001, con un buen Control de Accesos, permitirá tener Seguridad para el buen manejo de información en base a políticas de seguridad informática? | **OBJETIVOS ESPECÍFICOS:**<br>Diseñar un Sistema Informático basado en la ISO 27001 con una buena Gestión de activos Informáticos, que permita alinearse a las políticas de Seguridad Informática en la Municipalidad Provincial Huaura-Huacho.<br><br>Diseñar un Sistema Informático basado en la ISO 27001 con una buena seguridad relacionada con los Recursos Humanos, que permita alinearse a las políticas de Seguridad Informática en el Órgano de Control Institucional de la Municipalidad Provincial Huaura-Huacho.<br><br>Diseñar un Sistema Informático basado en la ISO 27001 con un buen Control de Accesos, que permita alinearse a las políticas de Seguridad Informática en el Órgano de Control Institucional de la Municipalidad Provincial Huaura-Huacho. | **HIPÓTESIS ESPECÍFICAS:**<br>El diseño de un Sistema Informático basado en la ISO 27001, con una buena Gestión de Activos Informáticos, si permite alinearse a las políticas de Seguridad Informática en la Oficina de Control Institucional de la Municipalidad Provincial Huaura-Huacho.<br><br>El diseño de un Sistema Informático basado en la ISO 27001, con una buena Seguridad relacionada con los Recursos Humanos, si permite alinearse a las políticas de Seguridad Informática en la Oficina de Control Institucional de la Municipalidad Provincial Huaura-Huacho.<br><br>El diseño de un Sistema Informático basado en la ISO 27001, con un buen Control de Accesos, si permite alinearse a las políticas de Seguridad Informática en la Oficina de Control Institucional de la Municipalidad Provincial Huaura-Huacho. | **Variable Dependiente:**<br>SEGURIDAD PARA EL MANEJO DE INFORMACION.<br>**Dimensiones:**<br>- Confidencial<br>- Disponible<br>- Integro | **Indicadores de Variable Dependiente:**<br>Copias de seguridad.<br>Acceso a información.<br>Acceso a la sala de servidores.<br>Información a tiempo.<br>Copias de seguridad.<br>Alterar información. |

| | | | | |
|---|---|---|---|---|