Universidad Científica del Perú - UCP
Registrado en el Asiento Nº A00010 de la Partida Nº 11000318, Personas Jurídicas de Iquitos, Superintendencia de los Registros Públicos - SUNARP

FACULTAD DE CIENCIAS E INGENIERÍA

PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

TESIS

"PROCESO DE AUDITORIA ISO 27001 PARA LA MEJORA DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE SAN JUAN BAUTISTA 2018"

PARA OPTAR EL TÍTULO PROFESIONAL EN CIENCIAS E INGENIERÍA CON MENCIÓN EN INGENIERÍA DE SISTEMAS DE INFORMACIÓN

Autores : CHAVEZ COBOS, Linder Moisés
Carrera Profesional de Ingeniería Informática y de Sistemas.

GARCIA GUERREO, Rudy Pol
Carrera Profesional de Ingeniería de Sistemas de Información.

Asesor : Ing. Carlos González Aspajo Mtr.

San Juan Bautista – Loreto – Maynas – Perú - 2018

DEDICATORIA CHAVEZ COBOS, Linder Moises

A Dios por ser el que siempre guía el camino que recorremos en nuestra vida personal y profesional.

A mis padres por brindarme ese apoyo incondicional para poder logras mis objetivos

DEDICATORIA GARCIA GUERRERO, Rudy Pool

A Dios por ser el que siempre guía el camino que recorremos en nuestra vida personal y profesional.

A mis padres por brindarme ese apoyo incondicional para poder logras mis objetivos

AGRADECIMIENTO

Expresamos nuestra gratitud a la Universidad Científica del Perú por la oportunidad de haberme permitido ampliar y profundizar nuestras convicciones profesionales.

Los Autores

CONSTANCIA DE ORIGINALIDAD DEL TRABAJO INVESTIGACIÓN DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP

El presidente del Comité de Ética de la Universidad Científica del Perú - UCP

Hace constar que:

La Tesis titulada:

"PROCESO DE AUDITORIA ISO 27001 PARA LA MEJORA DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE SAN JUAN BAUTISTA 2018"

De los alumnos: **CHAVEZ COBOS LINDER MOISÉS Y GARCIA GUERREO RUDY**

POL, de la Facultad de Ciencias e Ingeniería, pasó satisfactoriamente la revisión por el Software Antiplagio, con un porcentaje de **3% de plagio**.

Se expide la presente, a solicitud de la parte interesada para los fines que estime conveniente.

San Juan, 29 de setiembre del 2020.

CJRA/lasda 163-2020

Dr. César J. Ramal Asayag
Presidente del Comité de Ética – UCP

Urkund Analysis Result

Analysed Document:	UCP_Ing.Sist._2020_T_RudyGarcia_LinderChavez_V1.pdf (D80111568)
Submitted:	9/28/2020 5:23:00 PM
Submitted By:	revision.antiplagio@ucp.edu.pe
Significance:	3 %

Sources included in the report:

SISTEMAS_2018_PT_PANDURO_JIM.pdf (D40983364)

http://bdigital.unal.edu.co/56173/
https://revistas.unlp.edu.ar/econo/article/download/3638/3438/
https://docs.google.com/forms/d/1BxNScM1RbZ5a5R6bp9XwQiI-f6PUS6ezIxVvIvJ_ET4/edit? usp=sharing

Instances where selected sources appear:

7

UNIVERSIDAD CIENTÍFICA DEL PERÚ

"Año de la Universalización de la Salud"

FACULTAD DE CIENCIAS E INGENIERÍA

ACTA DE SUSTENTACIÓN DE TESIS

FACULTAD DE CIENCIAS E INGENIERÍA

Con Resolución Decanal N°796-2018-UCP-FCEI del 14 de octubre del 2018, la FACULTAD DE CIENCIAS E INGENIERÍA DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP designa como Jurado Evaluador de la sustentación de tesis a los señores:

- Ing. Juan Carlos Paredes Vásquez — presidente
- Ing. Paul Tello Gatica, Mg — Miembro
- Lic. Carlos Enrique Marthans Ruiz, Mg — Miembro

Como Asesor: **Ing. Carlos Gonzales Aspajo, Mg**

En la ciudad de Iquitos, siendo las 08:00 am del día 06 de abril del 2021, a través de la plataforma ZOOM supervisado en línea por la Secretaria Académica del Programa Académico de Ingeniería de Sistemas y de información de la Facultad de Ciencias e Ingeniería de la Universidad Científica del Perú., se constituyó el Jurado para escuchar la sustentación y defensa de la Tesis: **PROCESO DE AUDITORIA ISO 27001 PARA LA MEJORA DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE SAN JUAN BAUTISTA 2018"**

Presentado por el sustentante: **RUDY POL GARCIA GUERRERO**

Como requisito para optar el título profesional de**: INGENIERO DE SISTEMA DE INFORMACIÓN**

Luego de escuchar la sustentación y formuladas las preguntas las que fueron: ABSUELTAS

El Jurado después de la deliberación en privado llegó a la siguiènte conclusión:

La sustentación es: APROBADO

En fe de lo cual los miembros del Jurado firman el acta.

Presidente

Miembro

Miembro

UNIVERSIDAD CIENTÍFICA DEL PERÚ

"Año de la Universalización de la Salud"

FACULTAD DE CIENCIAS E INGENIERÍA

ACTA DE SUSTENTACIÓN DE TESIS

FACULTAD DE CIENCIAS E INGENIERÍA

Con Resolución Decanal N°797-2018-UCP-FCEI del 14 de octubre del 2018, la FACULTAD DE CIENCIAS E INGENIERÍA DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP designa como Jurado Evaluador de la sustentación de tesis a los señores:

- Ing. Juan Carlos Paredes Vásquez — presidente
- Ing. Paul Tello Gatica, Mg — Miembro
- Lic. Carlos Enrique Marthans Ruiz, Mg — Miembro

Como Asesor: **Ing. Carlos Gonzales Aspajo, Mg**

En la ciudad de Iquitos, siendo las 08:30 horas del día 06 de abril del 2021, a través de la plataforma ZOOM supervisado en línea por la Secretaria Académica del Programa Académico de Ingeniería de Sistemas y de información de la Facultad de Ciencias e Ingeniería de la Universidad Científica del Perú., se constituyó el Jurado para escuchar la sustentación y defensa de la Tesis: **PROCESO DE AUDITORIA ISO 27001 PARA LA MEJORA DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE SAN JUAN BAUTISTA 2018"**

Presentado por el sustentante: **LINDER MOISES CHAVEZ COBOS**

Como requisito para optar el título profesional de: **INGENIERO INFORMÁTICO Y DE SISTEMA**

Luego de escuchar la sustentación y formuladas las preguntas las que fueron: ABSUELTAS

El Jurado después de la deliberación en privado llegó a la siguiente conclusión:

La sustentación es: APROBADO

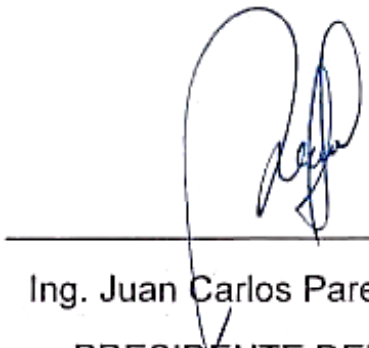
En fe de lo cual los miembros del Jurado firman el acta

Presidente

Miembro

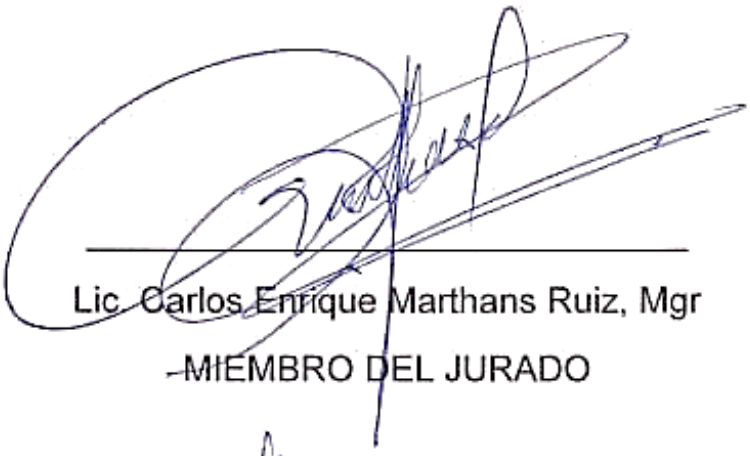
Miembro

Tesis sustentada en acto público el día 6 de abril a las 8:00 horas de 2021



Ing. Juan Carlos Paredes Vásquez

PRESIDENTE DEL JURADO



Lic. Carlos Enrique Marthans Ruiz, Mgr

MIEMBRO DEL JURADO

Ing. Paul Tello Gatica, Mgr

MIEMBRO DEL JURADO

ASESOR (es)

Ing. Carlos González Aspajo, Mtr.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

PROCESO DE AUDITORIA ISO 27001 PARA LA MEJORA DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE SAN JUAN BAUTISTA 2018.

AUTOR (es): GARCIA GUERRERO, Rudy Pol

CHAVEZ COBOS, Linder Moisés

RESUMEN

El objetivo de la investigación que se formuló fue: Determinar en qué medida el Proceso de Auditoria ISO 27001 mejorará los controles de seguridad de la información en la Municipalidad Distrital de San Juan Bautista durante el 2018.

La investigación fue de tipo no experimental, porque no hay manipulación de variables.

La población estuvo conformada por 39 trabajadores de la OIT de la Municipalidad Distrital de San Juan Bautista durante el 2018 y la muestra la conformo el 100%. La selección de la muestra para cada estrato se ha realizado en forma no aleatoria intencionada.

La técnica que se empleó en la recolección de los datos fue la encuesta, el análisis documental y los instrumentos fueron el cuestionario y el acta de evaluación.

Los resultados fueron: La significancia de p = ,001, lo que muestra que p es menor que 0,05, lo que permite señalar que la relación es significativa, por lo tanto, se rechaza la hipótesis nula y se acepta la hipótesis alterna. Es decir, Existe una relación significativa entre el proceso de auditoría y la mejora de controles de seguridad de la información de la Municipalidad Distrital de San Juan Bautista 2018.

Palabras Claves: Auditoria, ISO 27001, Procesos, Controles, Seguridad, Información.

ISO 27001 AUDIT PROCESS FOR THE IMPROVEMENT OF INFORMATION SECURITY CONTROLS IN THE DISTRICT MUNICIPALITY OF SAN JUAN BAUTISTA 2018.

AUTHORS: GARCIA GUERRERO, Rudy Pol

CHAVEZ COBOS, Linder Moisés

ABSTRACT

The objective of the investigation that was formulated was: To determine to what extent the ISO 27001 Audit Process will improve the information security controls in the District Municipality of San Juan Bautista during 2018.

The research was non-experimental, because there is no manipulation of variables.

The population was made up of 35 workers from the District Municipality of San Juan Bautista during 2018 and the sample was 100%. The selection of the sample for each stratum has been done in a non-random way.

The technique used in data collection was the survey, the documentary analysis and the instruments were the questionnaire and the evaluation report.

The results were: The significance of p = ,001, which shows that p is less than 0.05, which indicates that the relationship is significant, therefore, the null hypothesis is rejected and the alternative hypothesis is accepted. In other words, there is a significant relationship between the process between the audit process and the improvement of information security controls of the District Municipality of San Juan Bautista 2018.

Key Words: Audit, ISO 27001, Processes, Controls, Security, Information

CAPÍTULO I: INTRODUCCIÓN

La Municipalidad Distrital de San Juan Bautista es una de las más representativas de las 11 municipalidades distritales que conforman la Provincia de Maynas en la Región Loreto.

Dentro de su estructura orgánica; uno de los organismos de apoyo de la Municipalidad Distrital de San Juan Bautista es la Oficina de Informática y Telecomunicaciones OIT, que depende de la Gerencia Municipal. Se trata de un órgano de apoyo técnico, encargado de la gestión de las tecnologías de información y procesos de comunicación digital interna; establecer políticas y estrategias para los controles de datos fuentes de operación y salidas; seguridad de programas y mantenimiento de equipos de cómputo, con el fin de efectuar una gestión eficiente y asegurar la continuidad de los procesos de negocio. Su responsabilidad se extiende a las actividades relacionadas con el desarrollo, implementación, operación, mantenimiento y seguimiento de los sistemas informáticos y de brindar soporte técnico a los usuarios.[1]

Así mismo; una de las funciones más importantes e inherentes a la Oficina de Informática y Telecomunicaciones (OIT), es precisamente asegurar la continuidad del negocio mediante los sistemas de gestión de seguridad de la información de datos, la seguridad y salvaguarda de la información, ya sea esta, en su presentación lógica contenida en los repositorios locales o externos (hosting), páginas web, correo electrónico y software con las que trabaja la municipalidad o en los repositorios físicos así como los servidores, computadoras, medios magnéticos y solidos de almacenamiento, redes de comunicaciones de datos, y los manipulados por los propios usuarios que se sirven finalmente de ella. Para lo cual la Oficina de Informática y Telecomunicaciones (OIT) debe establecer directrices que fortalezcan la cultura de seguridad institucional de los trabajadores municipales y controles de seguridad que aseguren la salvaguarda de la información y la continuidad de los procesos informáticos que integran la cadena de valor de los procesos de información de la municipalidad.

[1] (Gerencia de Planeamiento y Presupuesto, 2016).

Actualmente la Oficina de Informática y Telecomunicaciones cuenta con configuraciones básicas para la seguridad de la información; de las cuales no cuentan con una directiva para su cumplimiento obligatorio para todos los órganos y/o unidades orgánicas de la Municipalidad. Así mismo cuenta con algunos controles de seguridad de la información que están administrados sin cumplir directrices. A continuación, hacemos mención de los controles que cuenta actualmente la Oficina de informática:

- Seguridad de los equipos
- Protección contra el software malicioso (malware)
- Copias de Seguridad
- Gestión de la seguridad de las redes

Sin embargo, la infraestructura tecnológica implementada para la seguridad no refleja una estructura estandarizada ni normalizada que contribuya con la seguridad de la información. Estas implementaciones aparentemente sin dirección debilitan más los controles de seguridad de la información.

La Oficina de Informática carece de una cultura de normalización que afecta o debilita la seguridad debido a la falta o inadecuada implementación de directrices para los usuarios y controles para los procesos de seguridad de la información que conforman el Core de negocio municipal, más aún teniendo en cuenta la creciente proliferación de nuevas generaciones de amenazas y ataques dirigidos con el objetivo de vulnerar la continuidad de los procesos de negocio.

Los controles implementados para la seguridad de la información no poseen mecanismos de seguimiento o retroalimentación que permitan medir su adecuado cumplimiento, lo que debilita aún más la seguridad de la información en la Municipalidad Provincial de San juan Bautista.

Justificación

Según distintos informes a nivel mundial, entre un 90% y un 95% de los ataques o incidentes en materia de seguridad de la información, se deben finalmente a fallas humanas.[2]

Los estudios realizados en seguridad de la información asegura que la vulnerabilidad a la seguridad en las instituciones es ocasionada mayormente por el error humano (usuarios finales); esto sumado a la falta de dirección para la implementación de infraestructura tecnológica de seguridad y a la falta de directrices para el control de la seguridad de la información, incentiva excesivamente la elaboración del presente proyecto de investigación de tesis; que busca fortalecer la aplicación y verificación del cumplimiento de los controles de seguridad de la información aplicados por la Oficina de Informática y Telecomunicaciones OIT en salvaguardar la información de la Municipalidad distrital de San Juan Bautista; mediante el fortalecimiento del proceso de auditoria informática basadas en la Norma ISO 27001.

En un contexto general debemos entender que la seguridad de la información a más de ser un problema de Tecnología Informática, también es un asunto de negocios. Si una institución quiere sobrevivir, y mucho más prosperar, es necesario comprender la importancia de la seguridad de la información y poner en práctica medidas, procesos y controles apropiados. Es vital estar preocupado por la seguridad de la información ya que gran parte de la cadena de valor de los procesos que generan información para las áreas funcionales y operativas de una institución se concentra precisamente en su información. Por tanto, valorar y proteger la información son tareas cruciales para las organizaciones modernas, actividad que debe ser circunscrita en una correcta asimilación de una norma como la ISO 27001 para la generación de controles de auditoria que aseguren su cumplimiento y la salvaguarda de la información, así como la continuidad de los procesos de negocios municipales en la municipalidad Distrital de San Juan Bautista.

[2] (Zaidman, 2017) (Net Media Europe, 2014)

El estudio fue trabajado bajo los siguientes objetivos:

Objetivo General

Determinar en qué medida el Proceso de Auditoria ISO 27001 mejorará los controles de seguridad de la información en la Municipalidad Distrital de San Juan Bautista durante el 2018.

Objetivos Específicos

- Evaluar si el proceso de Auditoria ISO 27001, favorece la generación de directrices de seguridad y salvaguarda de la información en la Municipalidad Distrital de San Juan Bautista durante el 2018.
- Analizar si el proceso de Auditoria ISO 27001, fortalece la infraestructura tecnológica de redes de datos de la Municipalidad Distrital de San Juan Bautista durante el 2018.
- Establecer si los controles de seguridad de la ISO 27001, mejora la cultura de seguridad de la información en la Municipalidad Distrital de San Juan Bautista durante el 2018.

Hipótesis

H_0: El proceso de Auditoria: Funcionalidad basado en la norma ISO 27001 no mejora la generación de directrices de seguridad y salvaguarda de la información de la Oficina de Informática y telecomunicaciones de la municipalidad distrital de San Juan Bautista durante el 2018.

H_1: El Proceso de Auditoria: Funcionalidad basado en la norma ISO 27001, mejora la generación de directrices de seguridad y salvaguarda de la información de la Oficina de Informática y telecomunicaciones de la municipalidad distrital de San Juan Bautista durante el 2018.

CAPÍTULO II: MATERIALES Y MÉTODOS

2.1. Tipo y diseño de Investigación

2.1.1 Tipo de Investigación

La investigación será de tipo no experimental porque no hay manipulación de variables; se expondrá como el proceso de auditoría de seguridad informática para mejorar los controles de seguridad informática en la Municipalidad Distrital San Juan Bautista, Provincia de Maynas del Departamento de Loreto, durante el año 2018.

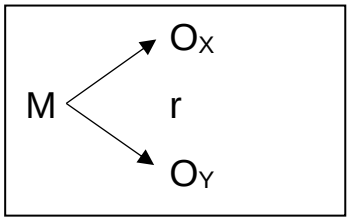
2.1.2 Diseño de Investigación

El diseño perteneció a la investigación no experimental y al tipo correlacional transversal.

Es no experimental porque el estudio se realizó sin manipular deliberadamente a la variable independiente: Proceso De Auditoria ISO 27001, si no que se observó los hechos tal como se encuentra en su contexto natural.

Es correlacional transversal porque se recolecto los datos en un solo momento en un tiempo único.

El diseño es:



M = Muestra.

OX = Observación a la variable independiente.

OY = Observación a la variable dependiente.

r = Posible relación o incidencia entre la variable dependiente e independiente.

2.2. Población y Muestra

2.2.1. Población

La población la conformaron 39 trabajadores de la OIT de la Municipalidad Distrital de San Juan Bautista, que laboraron durante el año 2018.

2.2.2. Muestra

La muestra la conformaron 39 trabajadores de la OIT de la Municipalidad Distrital de San Juan Bautista, que laboraron durante el año 2018.

2.3. Técnicas, Instrumentos y Procedimientos de Recolección de Datos

2.3.1. Técnicas de Recolección de Datos

La técnica que se empleó en la recolección de datos fue la encuesta, porque se buscaba conocer la opinión pública. Que consiste en el acopio de testimonios orales y escritos de personas.

2.3.2. Instrumentos de Recolección de Datos

El instrumento de recolección de datos fue el cuestionario. En la investigación de campo, para la recopilación de información se utilizó el cuestionario. Puede definirse como la relación que se establece entre el investigador y los sujetos de estudio. Puede ser individual o grupal, libre o dirigida.

2.3.3. Procedimientos de Recolección de Datos

Los procedimientos que se siguieron en la recolección de datos fueron:

- Coordinación con la Municipalidad Distrital de San Juan Bautista
- Elaboración de los Instrumentos de recolección de Datos
- Validación y confiabilidad de los instrumentos de recolección de datos
- Aplicación de los instrumentos de recolección de datos para recoger la información
- Procesamiento de los datos
- Organización de los datos mediante gráficos

- Análisis e interpretación de los datos
- Elaboración de informe de la tesis
- Presentación del informe de la Tesis
- Aprobación del informe de la Tesis
- Sustentación de la Tesis

2.4. Procesamiento de los Datos

2.4.1. Procesamiento de la Información

La información será procesada en forma computarizada utilizando el software SPSS V.26, sobre la base de datos con el cual se organizará la información en cuadros para luego representarlos en gráficos.

2.4.2. Análisis de la Información

El análisis utilizó pruebas paramétricas de dos variables cuantitativas ordinales y recurre a las técnicas de coeficiente de correlación de Pearson (grado de relación entre variables). Es decir, Existe una relación significativa entre el proceso de auditoría y la mejora de controles de seguridad de la información de la Municipalidad Distrital de San Juan Bautista.

CAPÍTULO III: RESULTADOS Y DISCUSIÓN

3.1 Resultados

3.3.1. Análisis descriptivo de Auditoría ISO 27001

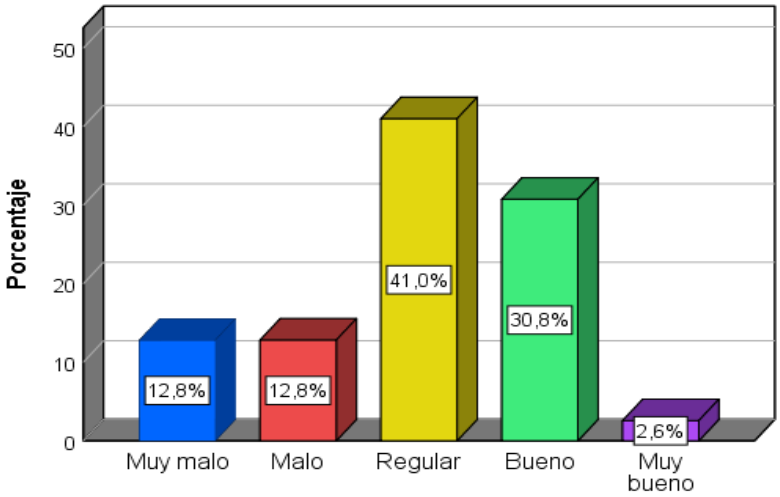
Tabla 1

Nivel de Conocimiento de Auditoria ISO 27001 para la generación de directrices de seguridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy malo	5	12,8	12,8	12,8
	Malo	5	12,8	12,8	25,6
	Regular	16	41,0	41,0	66,6
	Bueno	12	30,8	30,8	97,4
	Muy bueno	1	2,6	2,6	100,0
	Total	**39**	**100,0**	**100,0**	

Fuente: Base de datos de la encuesta realizada a los trabajadores

Figura 1: Nivel de Conocimiento de Auditoria ISO 27001 para generación de directrices de seguridad



Fuente: Tabla 1

Del 100% de los trabajadores encuestados de la Municipalidad Distrital de San Juan Bautista, el 41% tienen un nivel de conocimiento regular en los procesos de auditoría basados en las normas ISO-27001 para la generación de directrices, el 30.8% tienen conocimiento bueno, el 12.8% tienen un nivel conocimiento malo, el 12.8% tienen un nivel conocimiento muy malo y el 2.6% un nivel de conocimiento muy bueno.

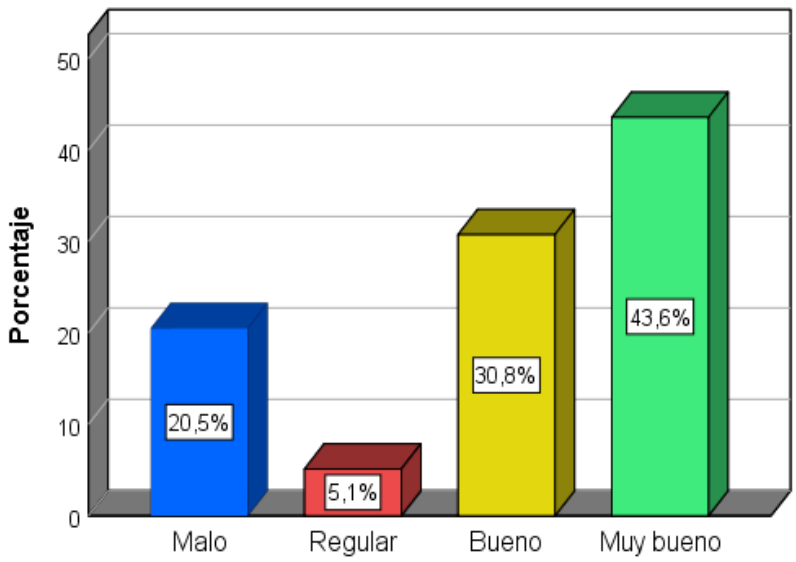
Tabla 2

El Nivel de eficacia percibida que tendría la aplicación periódica de procesos de auditoria ISO-27001 por los directivos

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	8	20,5	20,5	20,5
	Regular	2	5,1	5,1	25,6
	Bueno	12	30,8	30,8	56,4
	Muy bueno	17	43,6	43,6	100,0
	Total	**39**	**100,0**	**100,0**	

Fuente: Base de datos de la encuesta realizada a los trabajadores

Figura 2: El Nivel de eficacia percibida que tendría la aplicación periódica de procesos de auditoria ISO-27001 por los directivos



Fuente: Tabla 2

En la tabla y figura 2, podemos observar del 100% de los trabajadores de la Municipalidad Distrital de San Juan Bautista, el 43.6% de los trabajadores tienen un nivel de eficacia muy bueno percibida de la aplicación periódica de procesos de auditoria basada en la norma ISO_27001 a los controles de seguridad para la generación de las directrices, el 30.8% lo perciben en el nivel de eficacia bueno, 20.5% lo percibe un nivel malo y el 5.1% lo percibe regular.

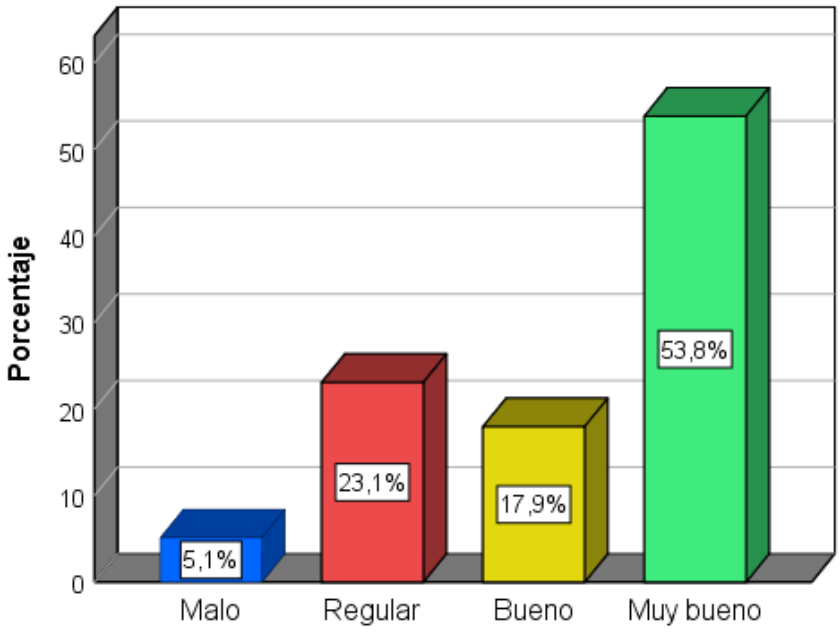
Tabla 3

El Nivel de eficiencia percibida que tendría la aplicación periódica de procesos de auditoria ISO-27001 a los controles de seguridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	2	5,1	5,1	5,1
	Regular	9	23,1	23,1	28,2
	Bueno	7	17,9	17,9	46,2
	Muy bueno	21	53,8	53,8	100,0
	Total	**39**	**100,0**	**100,0**	

Fuente: Base de datos de la encuesta realizada a los trabajadores

Figura 3: El nivel de eficiencia percibida que tendría la aplicación periódica de procesos de auditoria ISO-27001 a los controles de seguridad



Fuente: Tabla 3

Se aprecia en la tabla y figura 3, la respuesta de interrogante El Nivel de la eficiencia percibida de la aplicación periódica de procesos de auditoria basada en la norma ISO-“27001 a los controles de seguridad para la generación de directrices en menor tiempo y recursos, el 53.8% percibe muy bueno la eficiencia de la aplicación periódica, el 23.1% percibe con un nivel regular, el 17.9% lo percibe en el nivel bueno y el 5.1% lo percibe en el nivel malo.

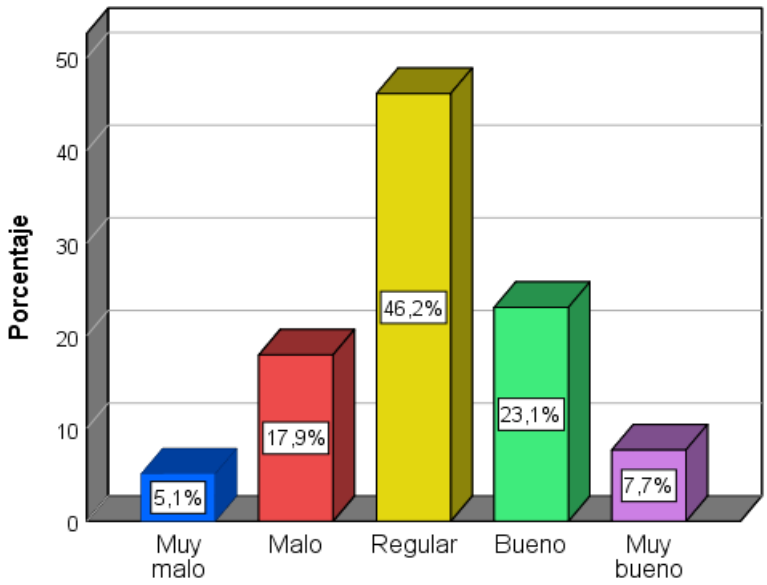
Tabla 4

Nivel de conocimiento que tiene acerca de los procesos de auditoria, basado en la Norma ISO-27001

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy malo	2	5,1	5,1	5,1
	Malo	7	17,9	17,9	23,1
	Regular	18	46,2	46,2	69,2
	Bueno	9	23,1	23,1	92,3
	Muy bueno	3	7,7	7,7	100,0
	Total	**39**	**100,0**	**100,0**	

Fuente: Base de datos de la encuesta realizada a los trabajadores

Figura 4: Nivel de conocimiento que tiene acerca de los procesos de auditoria, basado en la Norma ISO-27001



Fuente: Tabla 4

Como se aprecia en la tabla y figura 4, el 46.2% de los trabajadores encuestados de la Municipalidad Distrital de San Juan Bautista tienen un nivel de conocimiento regular acerca de los procesos de auditoria basada en la norma ISO-27001 para el fortalecimiento de la infraestructura tecnológica, el 23.1% tienen un nivel de conocimiento bueno, el 17.9% tiene un nivel de conocimiento malo, el 7.7% tienen un nivel de conocimiento muy bueno y el 5.1% tienen un nivel de conocimiento muy malo.

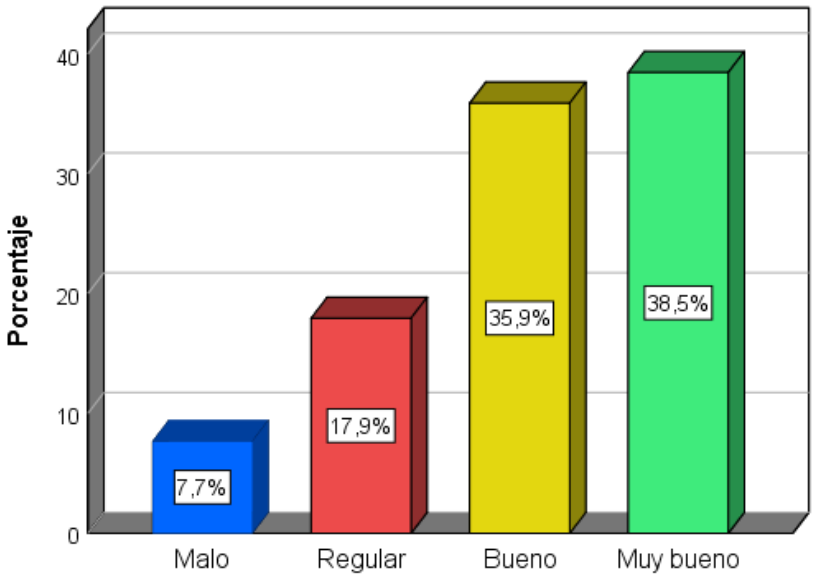
Tabla 5

Nivel de seguridad percibida tendría la aplicación periódica de procesos de auditoria iso27001

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	3	7,7	7,7	7,7
	Regular	7	17,9	17,9	25,6
	Bueno	14	35,9	35,9	61,5
	Muy bueno	15	38,5	38,5	100,0
	Total	**39**	**100,0**	**100,0**	

Fuente: Base de datos de la encuesta realizada a los trabajadores

Figura 5: Nivel de seguridad percibida tendría la aplicación periódica de procesos de auditoria iso27001



Fuente: Tabla 5

La tabla y figura 5, muestra acerca del nivel de seguridad percibida en la aplicación periódica de auditoria ISO-27001 a los controles de seguridad para el fortalecimiento de la infraestructura tecnológica de hardware, del 100% de los trabajadores encuestados de la Municipalidad Distrital de San Juan Bautista, el 38.5% lo percibe como muy bueno, el 35.9% lo percibe como bueno, el 17.9% lo percibe como regular y el 7.7% lo percibe como malo.

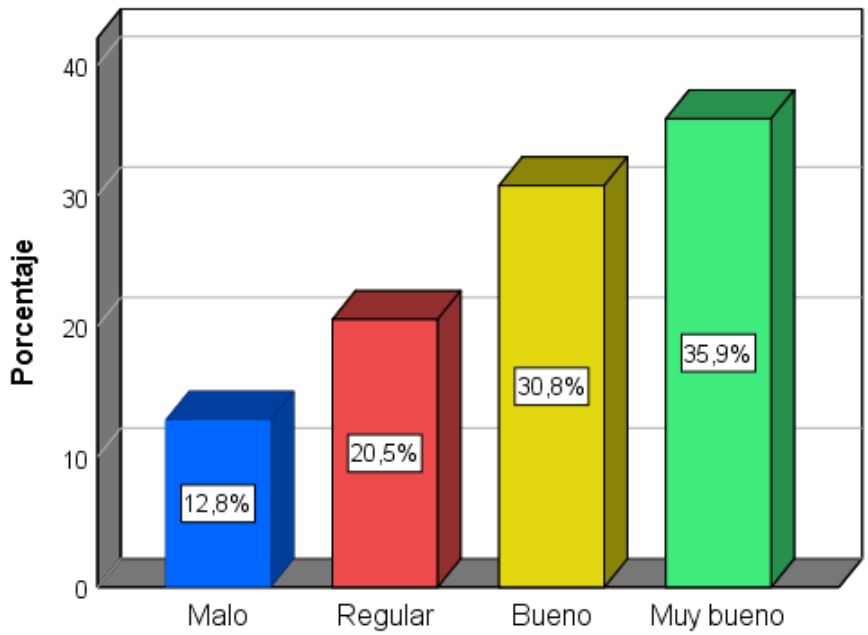
Tabla 6

Nivel de seguridad percibida tendría la aplicación periódica de procesos de auditoria ISO-27001

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	5	12,8	12,8	12,8
	Regular	8	20,5	20,5	33,3
	Bueno	12	30,8	30,8	64,1
	Muy bueno	14	35,9	35,9	100,0
	Total	**39**	**100,0**	**100,0**	

Fuente: Base de datos de la encuesta realizada a los trabajadores

Figura 6: ivel de seguridad percibida tendría la aplicación periódica de procesos de auditoria ISO-27001



Fuente: Tabla 6

En la tabla y figura 6, se observa, que el 35.9% de los trabajadores encuestados de la Municipalidad Distrital de San Juan Bautista percibe como muy bueno en el nivel de seguridad en la aplicación periódica de proceso de auditoria ISO 27001 a los controles de seguridad para el fortalecimiento de la infraestructura tecnológica de software, el 30.8% percibe como bueno, el 20.5% percibe como regular y el 12.8% percibe como malo.

3.3.2. Análisis descriptivo de control de seguridad

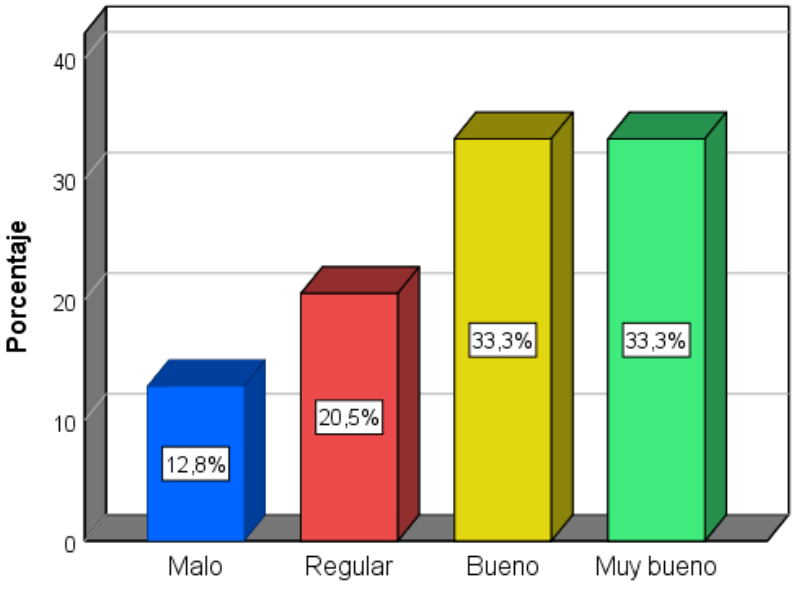
Tabla 7

Conocimiento acerca de los procesos de auditoria, basado en la Norma ISO-27001 para la mejora de la cultura de seguridad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Malo	5	12,8	12,8	12,8
	Regular	8	20,5	20,5	33,3
	Bueno	13	33,3	33,3	66,7
	Muy bueno	13	33,3	33,3	100,0
	Total	**39**	**100,0**	**100,0**	

Fuente: Base de datos de la encuesta realizada a los trabajadores

Figura 7: Nivel de conocimiento tiene acerca de los procesos de auditoria, basado en la Norma ISO-27001 para la mejora de la cultura de seguridad



Fuente: Tabla 7

Observamos los resultados de la tabla y figura 7, del 100% de los trabajadores encuestados de la Municipalidad Distrital de San Juan Bautista, referente al nivel de conocimiento sobre los procesos de auditoría basado en la norma ISO-27001, para la mejora de la cultura de seguridad, el 33.3% tiene un nivel de conocimiento muy bueno, el 33.3% tiene conocimiento bueno, el 20.5% tiene un nivel de conocimiento regular y el 12.8% tiene un nivel de conocimiento malo.

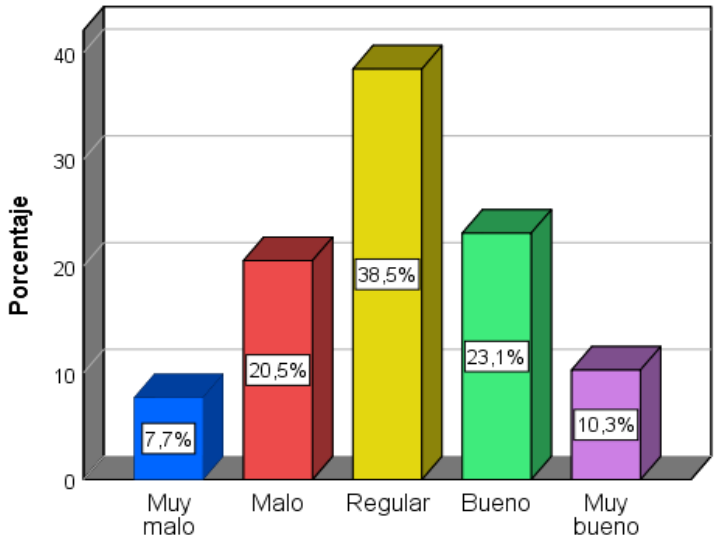
Tabla 8

Nivel de cultura de seguridad percibida tendría la aplicación periódica de procesos de auditoria ISO-27001 a los controles de seguridad para la sensación de protección de la Información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy malo	3	7,7	7,7	7,7
	Malo	8	20,5	20,5	28,2
	Regular	15	38,5	38,5	66,7
	Bueno	9	23,1	23,1	89,7
	Muy bueno	4	10,3	10,3	100,0
	Total	**39**	**100,0**	**100,0**	

Fuente: Base de datos de la encuesta realizada a los trabajadores

Figura 8: Nivel de cultura de seguridad percibida tendría la aplicación periódica de procesos de auditoria ISO-27001 a los controles de seguridad para la sensación de protección de la Información



Fuente: Tabla 8

En la tabla y figura 8, describimos acerca del nivel de cultura de seguridad percibida en la aplicación periódica de procesos de auditoría en la norma ISO-27001 a los controles para la sensación de protección de la información, el 38.5% de los trabajadores de la Municipalidad Distrital de San Juan Bautista percibe un nivel regular, el 23.1% percibe un nivel bueno, el 20.5% percibe un nivel malo, el 10.3% percibe un nivel muy bueno y 7.7% percibe un nivel muy malo.

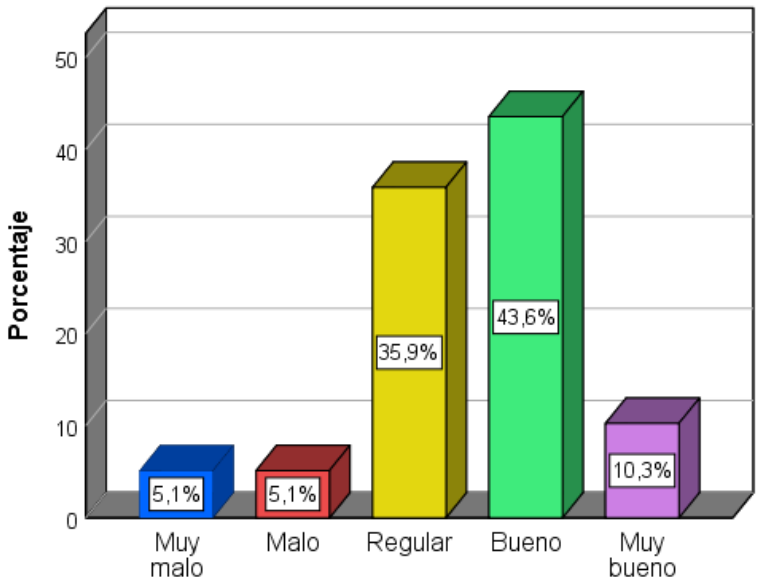
Tabla 9

Nivel de cultura de seguridad percibida tendría la aplicación periódica de procesos de auditoria ISO-27001 a los controles de seguridad para la aplicación de buenas prácticas de seguridad de la Información

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy malo	2	5,1	5,1	5,1
	Malo	2	5,1	5,1	10,3
	Regular	14	35,9	35,9	46,2
	Bueno	17	43,6	43,6	89,7
	Muy bueno	4	10,3	10,3	100,0
	Total	**39**	**100,0**	**100,0**	

Fuente: Base de datos de la encuesta realizada a los trabajadores

Figura 9: Nivel de cultura de seguridad percibida tendría la aplicación periódica de procesos de auditoria ISO-27001 a los controles de seguridad para la aplicación de buenas prácticas de seguridad de la Información



Fuente: Tabla 9

Los resultados que muestra la tabla y figura 9 sobre el nivel de cultura de seguridad percibida en la aplicación periódica de procesos de auditoría ISO-27001 a los controles de buenas prácticas de seguridad de la información, el 43.6% de los trabajadores de la Municipalidad Distrital de San Juan Bautista, percibe bueno, el 35.9% percibe regular, el 10.3% percibe muy bueno, el 5.1% percibo malo y el 5.1% percibe muy malo.

3.3.3. Análisis global de efectividad

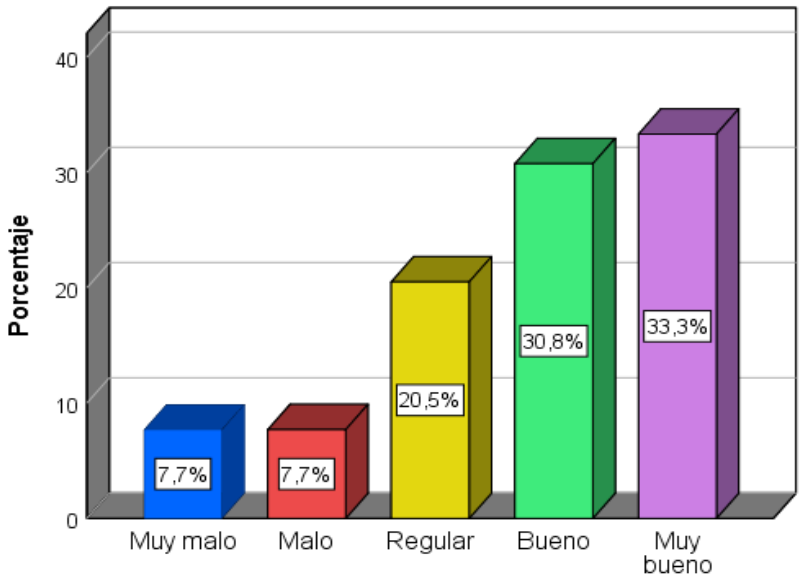
Tabla 10

Análisis global de efectividad (Categorizada)w

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy malo	3	7,7	7,7	7,7
	Malo	3	7,7	7,7	15,4
	Regular	8	20,5	20,5	35,9
	Bueno	12	30,8	30,8	66,7
	Muy bueno	13	33,3	33,3	100,0
	Total	**39**	**100,0**	**100,0**	

Fuente: Tabla 1, 2 y 3

Figura 10: Análisis global de efectividad (Categorizada)



Fuente: Tabla 10

Los resultados del análisis global de efectividad podemos ver en la tabla y figura 10, sobre los procesos de auditoria de seguridad informática normativa – efectividad, el 33.3% de los trabajadores de la Municipalidad Distrital de San Juan Bautista percibe muy bueno la efectividad en su conjunto como medidas preventivas de la Municipalidad en el proceso de auditoría, el 30.8% percibe como bueno, el 20.5% percibe como regular, el 7.7% percibe como malo y el 7.7% lo percibe como muy malo.

3.3.4. Análisis global de funcionabilidad

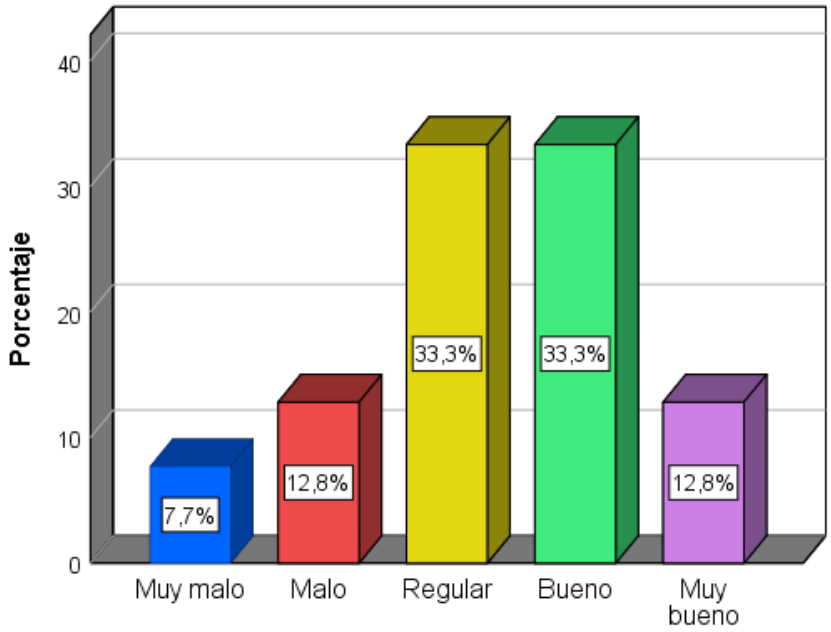
Tabla 11

Análisis global de funcionalidad (Categorizada)

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy malo	3	7,7	7,7	7,7
	Malo	5	12,8	12,8	20,5
	Regular	13	33,3	33,3	53,8
	Bueno	13	33,3	33,3	87,2
	Muy bueno	5	12,8	12,8	100,0
	Total	**39**	**100,0**	**100,0**	

Fuente: Tabla 4, 5 y 6

Figura 11: Análisis global de Funcionalidad (Categorizada)



Fuente: Tabla 11

La tabla y figura 11, cuyos resultados hacen mención de la funcionalidad del proceso de auditoría de seguridad informática de infraestructura tecnológica, el 33.3% de los trabajadores de la Municipalidad Distrital de San Juan Bautista percibe como bueno, el 33.3% percibe como regular, el 12.8% percibe como muy bueno, el 12.8% percibe como malo y el 7.7% percibe como muy malo la funcionalidad de la Municipalidad.

3.3.5. Análisis global de confiabilidad

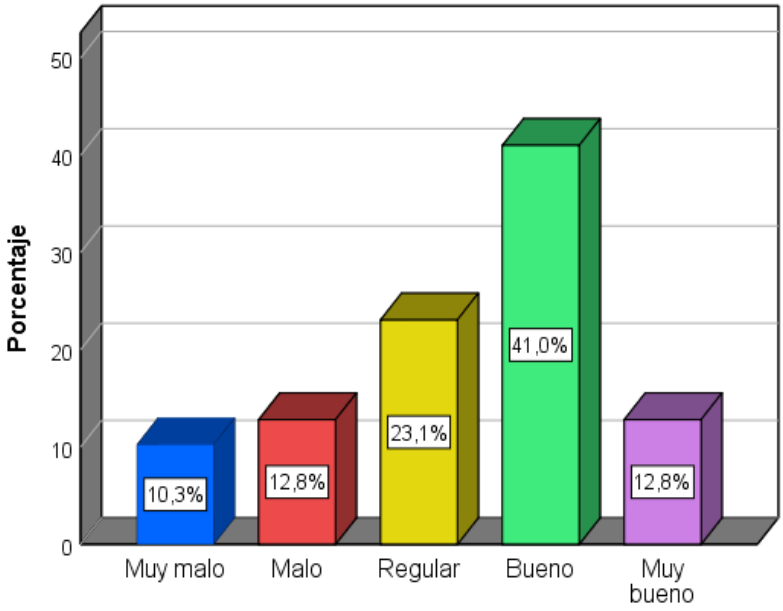
Tabla 12

Análisis global de confiabilidad (Categorizada)

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy malo	4	10,3	10,3	10,3
	Malo	5	12,8	12,8	23,1
	Regular	9	23,1	23,1	46,2
	Bueno	16	41,0	41,0	87,2
	Muy bueno	5	12,8	12,8	100,0
	Total	**39**	**100,0**	**100,0**	

Fuente: Tabla 7, 8 y 9

Figura 12: Análisis global de Confiabilidad (Categorizada)



Fuente: Tabla 12

En la tala y figura 12 observamos los resultados sobre confiabilidad de la auditoría ISO-27001, mejora los controles de seguridad de la información de la Municipalidad Distrital de San Juan Bautista, el 41% percibe como bueno, 23.1% percibe como regular, el 12.8% percibe como muy bueno, el 12.8% percibe como malo y 10.3% percibe como muy malo.

4.1 Análisis estadístico inferencial

3.4.1. Prueba estadística para la determinación de normalidad

Los resultados alcanzados se determinaron, primordialmente de acuerdo al tipo de distribución que presentan los datos de las muestras de las variables, para ello se utilizó la prueba de normalidad de bondad de ajuste. La prueba admite medir el grado de correspondencia existente entre la distribución de un conjunto de datos de distribución teórica específica. El propósito es indicar si los datos consignados de una población tienen una distribución normal o no normal.

Tabla 13

Prueba de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Proceso de Auditoría	,128	39	,105	,965	39	,271
Confiabilidad	,178	39	,003	,931	39	,019

a. Corrección de significación de Lilliefors

La tabla 13 nos muestra dos estadísticos de normalidad, de las cuales tomamos el estadístico de Shapiro-Wilk, por cuanto, la muestra es de 39, la misma que muestra una significancia mayor que 0.05, lo que indica que la muestra tiene distribución de probabilidad normal, por lo tanto, el análisis utilizó pruebas paramétricas de dos variables cuantitativas ordinales y recurre a las técnicas de coeficiente de correlación de Pearson (grado de relación entre variables).

3.4.2. Contraste de hipótesis

Contraste de hipótesis general

H_0 = El Proceso de Auditoria ISO 27001, no mejora los Controles de Seguridad de la Información de la Oficina de Informática y Telecomunicaciones de la Municipalidad Distrital de San Juan Bautista en el 2018.

H_1 = El Proceso de Auditoria ISO 27001, mejora los Controles de Seguridad de la Información de la Oficina de Informática y Telecomunicaciones de la Municipalidad Distrital de San Juan Bautista en el 2018.

Nivel de significancia $\alpha = 0.05 = 5\%$ de margen de error

Regla de decisión $p \geq \alpha$ se acepta la hipótesis nula (H_0)

$p < \alpha$ se acepta la hipótesis alterna (H_1)

Tabla 14

Coeficiente de correlación de Pearson de las variables: Proceso de Auditoría ISO – 27001 ∗ Mejora los controles de seguridad

Correlaciones

		Proceso de Auditoría	Mejora de controles de seguridad
Proceso de Auditoría:	Correlación de Pearson	1	,519**
	Sig. (bilateral)		,001
	N	39	39
Mejora de controles de seguridad	Correlación de Pearson	,519**	1
	Sig. (bilateral)	,001	
	N	39	39

**. La correlación es significativa en el nivel 0,01 (bilateral).

Descripción del grado de relación entre las variables:

Los resultados del contraste estadístico dan cuenta de la existencia de una relación r = 0,519 entre las dos variables: Proceso de Auditoría y la Mejora de controles de seguridad, mostrándonos que existe relación positiva y significativa con un nivel de correlación positiva considerable.

Decisión estadística:

La significancia de p = 0,001, demuestra que p es menor que 0,05, lo que permite señalar que la relación es significativa, por lo tanto, se rechaza la hipótesis nula y se acepta la hipótesis alterna. Es decir, Existe una relación significativa entre el proceso de auditoría y la mejora de controles de seguridad de la información de la Municipalidad Distrital de San Juan Bautista.

Contraste de hipótesis específico 1

H_0 = El proceso de Auditoria: Efectividad basado en la norma ISO 27001 no mejora la generación de directrices de seguridad y salvaguarda de la información de la Oficina de Informática y telecomunicaciones de la municipalidad distrital de San Juan Bautista durante el 2018.

H_1 = El Proceso de Auditoria: Efectividad basado en la norma ISO 27001, mejora la generación de directrices de seguridad y salvaguarda de la información de la Oficina de Informática y telecomunicaciones de la municipalidad distrital de San Juan Bautista durante el 2018.

Nivel de significancia $\alpha = 0.05 = 5\%$ de margen de error

Regla de decisión $p \geq \alpha$ se acepta la hipótesis nula (H_0)

$p < \alpha$ se acepta la hipótesis alterna (H_1)

Tabla 15

Proceso de Auditoría de efectividad de seguridad informática normativa – efectividad ∗ Mejora de controles de seguridad

Correlaciones

		Proceso de Auditoría: Efectividad	Mejora de controles de seguridad
Proceso de Auditoría: Efectividad	Correlación de Pearson	1	,117
	Sig. (bilateral)	,	,477
	N	39	39
Mejora de controles de seguridad	Correlación de Pearson	,117	1
	Sig. (bilateral)	,477	,
	N	39	39

**. La correlación es significativa en el nivel 0,01 (bilateral).

Descripción del grado de relación entre las variables:

Los resultados del contraste estadístico dan cuenta de la existencia de una relación r = ,117 entre las variables: Proceso de Auditoría: Efectividad y la Mejora de controles de seguridad, mostrándonos que existe relación positiva y significativa con un nivel de correlación positiva considerable.

Decisión estadística:

La significancia de p = ,000, lo que muestra que p es menor que 0,05, lo que permite señalar que la relación es significativa, por lo tanto, se rechaza la hipótesis nula y se acepta la hipótesis alterna. Es decir, Existe una relación significativa entre el proceso de auditoría: Efectividad y la mejora de controles de seguridad de la información de la Municipalidad Distrital de San Juan Bautista.

Contraste de hipótesis específico 2

H_0 = El proceso de Auditoria: Funcionalidad basado en la norma ISO 27001 no mejora la generación de directrices de seguridad y salvaguarda de la información de la Oficina de Informática y telecomunicaciones de la municipalidad distrital de San Juan Bautista durante el 2018.

H_1 = El Proceso de Auditoria: Funcionalidad basado en la norma ISO 27001, mejora la generación de directrices de seguridad y salvaguarda de la información de la Oficina de Informática y telecomunicaciones de la municipalidad distrital de San Juan Bautista durante el 2018.

Nivel de significancia	$\alpha = 0.05 = 5\%$ de margen de error	
Regla de decisión	$p \geq \alpha$	se acepta la hipótesis nula (H_0)
	$p < \alpha$	se acepta la hipótesis alterna (H_1)

Tabla 16

Proceso de Auditoría de funcionalidad de seguridad informática normativa – Funcionalidad ∗ Mejora de controles de seguridad

Correlaciones

		Proceso de Auditoría: Funcionalidad	Mejora de controles de seguridad
Proceso de Auditoría: Funcionalidad	Correlación de Pearson	1	,662**
	Sig. (bilateral)	,	,000
	N	39	39
Mejora de controles de seguridad	Correlación de Pearson	,662**	1
	Sig. (bilateral)	,000	,
	N	39	39

**. La correlación es significativa en el nivel 0,01 (bilateral).

Descripción del grado de relación entre las variables:

Los resultados del contraste estadístico dan cuenta de la existencia de una relación r = ,662 entre las variables: Proceso de Auditoría: Funcionalidad y la Mejora de controles de seguridad, mostrándonos que existe relación positiva y significativa con un nivel de correlación positiva considerable.

Decisión estadística:

La significancia de p = ,000, lo que muestra que p es menor que 0,05, lo que permite señalar que la relación es significativa, por lo tanto, se rechaza la hipótesis nula y se acepta la hipótesis alterna. Es decir, Existe una relación significativa entre el proceso de auditoría: Funcionalidad y la mejora controles de seguridad de la información de la Municipalidad Distrital de San Juan Bautista.

3.2 Discusión

Luego del análisis, se encontró que existe relación significativa entre el Proceso de Auditoría ISO 27001 y la mejora de los controles de seguridad de la información de la Municipalidad Distrital de San Juan Bautista, lo que establece las condiciones y diferencias con otros autores del mismo tema de estudio.

Al analizar los resultados de prueba de hipótesis se confirma que influye el Proceso de auditoría y la mejora de los controles de seguridad de la información de la Municipalidad Distrital de San Juan Bautista, aplicando la encuesta a los trabajadores, con la prueba de Pearson, se evidencia que los resultados de la encuesta de la muestra de estudio fueron estadísticamente iguales.

El estadístico paramétrico de coeficiente de correlación de Pearson demuestra el contraste de hipótesis, se encontró que existe una relación significativa entre el Proceso de auditoría y la mejora de controles de seguridad en la Municipalidad Distrital de San Juan Bautista, 2018, que existe una relación positiva considerable. En la tabla el contraste de hipótesis general se observa la Sig. Asintótica (bilateral) cuyo valor es 0,519. El valor p (sig. Asintótica) bilateral es menos a 0.05, por lo que se rechaza la hipótesis nula y concluye que existe relación significativa, para decir, que existe relación entre el proceso de auditoría y la mejora de controles de seguridad de información de la Municipalidad Distrital de San Juan Bautista, 2018 con un nivel de significancia del 5% de margen de error.

Posterior al análisis se tuvo resultado del proceso de auditoría para mejora de los controles de seguridad de la información de la Municipalidad del Distrito de San Juan Bautista 2018, Bermeo; Paguay; Zamora (2017), en su trabajo de investigación Auditoría de la Seguridad Informática basado en la ISO 27001 Sistema de Gestión de Seguridad de la Información para el GAD Municipal del Milagro. Universidad Estatal del Milagro. Ecuador. Se concluye: Que los controles y procedimientos que contiene la norma ISO 27001:2013, que está dirigida a la seguridad, esto quiere decir que la información que manipula el GAD municipal de Milagro será segura.

Berrío López, Juan Pablo (2016), en su trabajo de investigación Metodología para la evaluación del desempeño de controles en sistemas de gestión de seguridad

de la información sobre la norma ISO/IEC 27001. Universidad Nacional de Medellín. Colombia Concluye: Que la implementación de un SGSI requiere estar a la vanguardia de las innovaciones tecnológicas, en este aspecto, el área de tecnología sí tiene un papel muy destacado, ya que debe proponer herramientas metodológicas tanto para la prevención como para la detección de riesgos relacionados con el aumento de vulnerabilidades informáticas, teniendo en cuenta que la mayoría de áreas de una compañía está conectada a la red

Los resultados obtenidos en la tesis de Francisco Nicolás Solarte, Edgar Rodrigo, Enríquez Rosero, Mirian del Carmen Benavides; (2015), en su trabajo de investigación Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Universidad Nacional Abierta y a Distancia, Pasto Nariño. Colombia; Concluye: Que con el resultado obtenido se puede concluir que no existe un compromiso real de las directivas, que los empleados no son conscientes de los objetivos que se pretende con el sistema de control de seguridad de la información y que el personal del área informática no está capacitado para asumir esta responsabilidad. Por lo tanto, es fundamental que las organizaciones cuenten con un marco normativo de seguridad, que permita aplicar la auditoría basada en la norma ISO/IEC 27002. Del proceso de auditoría a la seguridad de la información se concluye que este proceso debe ser continuo y que debe ser realizado por los entes de control interno de cada organización, y periódico por empresas auditoras externas que permitan hacer la evaluación y seguimiento del sistema de control de seguridad informático para el diseño, implementación e implantación de un SGSI adecuado a sus necesidades.

Del mismo modo García y Del Águila (2017). en su trabajo de investigación Análisis e Implementación de la Seguridad de la información del centro de datos de Universidad Nacional de la Amazonia Peruana Bajo la Norma ISO 27002. Universidad Nacional de la Amazonia Peruana. Iquitos. Perú. Concluye: que La implementación de controles de seguridad basados en la norma ISO/IEC 27002, les permite mejorar tres características importantes como son: la confidencialidad, integridad y disponibilidad de la información.

Así mismo Gastulo y Canaza (2017). en su trabajo de investigación Diseño e Implementación de un sistema de gestión de seguridad de la información en el proceso de control de acceso a la red en una institución del Estado. Universidad Tecnológica del Perú. Lima Perú. Se concluye: Que gestionar la seguridad de la información, en un entorno sistemático, por lo que se ha tomado como referencia la norma ISO 27001:2003 y la metodología de gestión de riesgos ISO 31000:2009, aplicada a la evaluación del acceso de los recursos y servicios de la institución, su implementación, permitirá asegurar adecuadamente el procedimiento de acceso a la red institucional.

Así mismo Zeña Ortiz, Victor Eduardo (2016). en su trabajo de investigación Estándar internacional ISO 27001 para la gestión de seguridad de la información en la oficina central de informática de la UNPRG. Universidad Nacional Pedro Ruiz Gallo. Trujillo Se concluye: Que el Sistema de Gestión de Seguridad de la Información en el Proceso de Soporte de TI de la Oficina Central de informática - UNPRG, el nivel de riesgo se logra disminuir en promedio de 6 a 4.4, lo que significa un 26.67%. El cual se logra después de haber aplicado la metodología de análisis y evaluación de riesgos, finalizando con la implementación de los controles de la ISO 27001, anexo A., con lo cual se puede afirmar que el nivel de riesgo ha disminuido.

CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

Primero. En función al objetivo general, existe una relación significativa entre el Proceso de auditoría para la mejora de los controles de seguridad de información en la Municipalidad Distrital de San Bautista 2018, ello confirma los resultados obtenidos del estadístico de coeficiente de correlación de Pearson r = ,519 y la Significancia asintótica (bilateral) p = ,001 es menor que 0.05. Es decir, que existe relación positiva considerable entre el proceso de auditoría y los controles de seguridad de la Municipalidad Distrital de San Juan Bautista, 2018.

Segundo. En cuanto a la dimensión efectividad, existe relación significativa del proceso de auditoría para la mejora de los controles de seguridad de la información (confiabilidad) en la Municipalidad Distrital de San Juan Bautista, de acuerdo a los resultados estadístico de coeficiente de correlación de Pearson r ,117 y la significancia asintótica (bilateral) p = ,477 es mayor que 0,05. Es decir, que existe relación positiva media entre el proceso de auditoría para la mejora de los controles de seguridad de la información de la Municipalidad Distrital de San Juan Bautista, 2018.

Tercero. Referente a la dimensión funcionalidad, existe una relación significativa del proceso de auditoría para la mejora de los controles de seguridad de la información (confiabilidad) en la Municipalidad Distrital de San Juan Bautista, el resultado estadístico de coeficiente de correlación de Pearson r = ,662 y la significancia asintótica (bilateral) p = ,000 es menor que 0.05. Es decir, que existe una relación positiva considerable entre el proceso de auditoría para los controles de seguridad de la información de la Municipalidad Distrital de San Juan Bautista, 2018.

Cuarto. Acorde a los resultados obtenidos para la dimensión de confiabilidad se determina que el proceso de auditoría ISO – 27001, mejora los controles de seguridad de la información en la Oficina de Informática y telecomunicación, se logró mejorar los controles de seguridad de información como resultado de las continuas auditorías que efectúen en la Municipalidad Distrital de San Juan Bautista, 2018.

4.2 Recomendaciones

- Promover las evaluaciones periódicas de Auditoría ISO – 27001 en la Municipalidad Distrital de San Juan Bautista a través de la revisión y análisis de documentos, para la generación de directrices de seguridad y así salvaguardar la información en menor tiempo y recursos de la Municipalidad.
- Implementar el proceso de auditoría de seguridad informática, para el fortalecimiento de la infraestructura tecnológica, en forma periódica para mejorar los controles de seguridad de la información de hardware y software de la Municipalidad Distrital de San Juan Bautista.
- Desarrollar jornadas de capacitación del personal de la Municipalidad Distrital de Maynas sobre métodos de auditoría a aplicar, la norma ISO 27001, para interactuar con el personal de la auditoría y así tener mayor funcionalidad y mejora del control se seguridad de la información.
- Asegurar la confiabilidad del proceso de auditoría de seguridad informática, cultura de seguridad, realice buenas prácticas de seguridad de la información, a fin de asegurar la protección de la información de la Municipalidad Distrital de San Juan Bautista.

CAPÍTULO V: REFERENCIA BIBLIOGRAFCA

- **Bermeo Almeida, Oscar Xavier, Paguay Lema, Cinthya Katherine y Zamora Arana, Gabriel Eduardo. 2017.** Universidad Estatal el Milagro. *www.repositorio.unemi.edu.ec.* [En línea] 2017. [Citado el: 10 de 07 de 2018.] http://repositorio.unemi.edu.ec/handle/123456789/3845.

- **Berrío Lopez, Juan Carlos. 2016.** Universidad Nacional de Colombia. *www.bdigital.unal.edu.co.* [En línea] 2016. [Citado el: 10 de 07 de 2018.] http://bdigital.unal.edu.co/56173/.

- **Canaza chambi, Willians Yobany. 2017.** Universidad Tecnologica del Perú. *www.utp.edu.pe.* [En línea] 2017. [Citado el: 10 de 07 de 2018.] www.utp.edu.pe.

- **Gerencia de Planeamiento y Presupuesto. 2016.** Municipalidad Distrital de San Juan Bautista. *www.munisanjuan.gob.pe.* [En línea] 2016. [Citado el: 06 de 06 de 2018.]

  http://www.munisanjuan.gob.pe/transparencia/ROF-2016-MDSJB.pdf.

- **Mapfre. 2004.** Fundacion Mapfre. *https://www.fundacionmapfre.org.* [En línea] 2004. [Citado el: 06 de 06 de 2018.]

  https://www.fundacionmapfre.org/documentacion/publico/es/catalogo_imagenes/grupo.cmd?path=1025574.

- **NETMEDIAEUROPE. 2014.** Silicon. *www.silicon.es.* [En línea] NETMEDIAEUROPE, 2014. [Citado el: 06 de 06 de 2018.]

  https://www.silicon.es/el-95-por-ciento-de-las-incidencias-de-seguridad-informatica-se-deben-errores-humanos-61228.

- **Solarte Solarte, Francisco Nicolas, Enriquez rosero, Edgar Rodrigo y Del Carmen Benavidez, Mirian. 2015.** Revista Tecnologica Espol. *www.rte.espol.edu.ec.* [En línea] 2015. [Citado el: 10 de 07 de 2018.] http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456.

- **Zaidman, Emilio. 2017.** Revistas UNLP Argentina. *www.revistas.unlp.edu.ar.* [En línea] 2017. [Citado el: 06 de 06 de 2018.] https://revistas.unlp.edu.ar/econo/article/download/3638/3438/.
- **Zeña Ortiz, Victor Eduardo. 2016.** Renati. *www.renati.sunedu.gob.pe.* [En línea] 2016. [Citado el: 10 de 07 de 2018.]

  http://renati.sunedu.gob.pe/handle/sunedu/143327.

CAPÍTULO VI: ANEXOS

6.1. Anexo 1: Operacionalización de Variables

6.2. Anexo 2: Matriz de Consistencia

6.3. Anexo 3: Propuesta para la mejora de los controles de seguridad de la información en la municipalidad según la ISO 27001.

6.4. Anexo 4: Instrumento de Recolección de Datos

6.5. Anexo 5: Cuestionario digital usando la herramienta de google drive

6.6. Anexo 6: Anexo “A” de la ISO 27001

6.7. Anexo 7: Inventario de activos del proceso gestión de la infraestructura tecnológica de la Municipalidad Distrital de San Juan Bautista

ANEXO N° 1: Operacionalización de Variables

Tabla 17

Operacionalización de Variables.

VARIABLES	DIMENSIÓN	INDICADORES	ÍNDICES
V.I. (X): Proceso de Auditoria Basado en la Norma ISO 27001	• Normatividad • Infraestructura Tecnológica	• Efectividad • Confiabilidad	MUY MALO = 0 – 4 MALO = 4 – 8 REGULAR = 8 -12 BUENO = 12-16 MUY BUENO = 16 - 20
V.D.(Y): Controles de Seguridad de la Información.	• Cultura de Seguridad	• Funcionalidad	

Fuente: Elaboración propia

ANEXO N° 2: Matriz de Consistencia

Tabla 18

Matriz de consistencia.

Problema	Objetivo	Hipótesis	Metodología	Variables	Dimensiones	indicadores	Instrumentos
Problema General: Determinar en qué medida el proceso de Auditoria ISO 27001 mejorará los controles de seguridad de la información en la Municipalidad Distrital de San Juan Bautista en el 2018 **Problemas Especifico** • Evaluar si el proceso de Auditoria ISO 27001 favorece la generación de directrices de seguridad y salvaguarda de la información de la municipalidad distrital de San Juan Bautista durante el 2018 • Establecer si los controles de seguridad ISO 27001, mejora la	**Objetivo General:** Determinar en qué medida el proceso de Auditoria de la ISO 27001 mejorará los controles de seguridad de la información en la Municipalidad Distrital de San Juan Bautista en el 2018 **Objetivos Específicos:** • Evaluar si el proceso de Auditoria ISO 27001 favorece la generación de directrices de seguridad y salvaguarda de la información de la municipalidad distrital de San Juan Bautista durante el 2018 • Establecer si los controles de seguridad ISO 27001, mejora la cultura de seguridad de la información en la Municipalidad Distrital	**Hipótesis General:** Proceso de Auditoria ISO 27001, Mejora los Controles de Seguridad de la Información de la Oficina de Informática y Telecomunicaciones de la Municipalidad Distrital de San Juan Bautista en el 2018 **Hipótesis Específicos:** • El proceso de Auditoria ISO 27001 favorece la generación de directrices de seguridad y salvaguarda de la información de la municipalidad distrital de San Juan Bautista durante el 2018 • Los controles de seguridad ISO 27001, de la Oficina de Informática y Telecomunicaciones mejora la cultura de seguridad de la información en la Municipalidad Distrital	**Tipo de Investigación:** La investigación será de tipo no experimental porque no hay manipulación de variables; se expondrá como el proceso de auditoría de seguridad informática para mejorar los controles de seguridad informática en la Municipalidad Distrital San Juan Bautista **Diseño de Investigación:** • El diseño perteneció a la investigación no experimental y al tipo correlacional transversal. • Es no experimental porque el estudio se realizó sin manipular deliberadamente a la variable independiente: Proceso De Auditoria ISO 27001, si no que se observó los hechos tal	V.I. (X): Proceso De Auditoria ISO 27001 V.D.(Y): Controles De Seguridad De La Información.	• Normatividad • Infraestructura Tecnológica • Cultura de Seguridad	• Efectividad • Confiabilidad • Funcionalidad	• Cuestionario

cultura de seguridad de la información en la Municipalidad Distrital de San Juan Bautista durante el 2018 • Analizar si el proceso de Auditoria ISO 27001 fortalece la infraestructura tecnológica de redes de datos de la Municipalidad Distrital de San Juan Bautista durante el 2018	de San Juan Bautista durante el 2018 • Analizar si el proceso de Auditoria ISO 27001 fortalece la infraestructura tecnológica de redes de datos de la Municipalidad Distrital de San Juan Bautista durante el 2018	de San Juan Bautista durante el 2018 • El proceso de Auditoria ISO 27001 fortalece la infraestructura tecnológica de redes de datos de la Municipalidad Distrital de San Juan Bautista durante el 2018	como se encuentra en su contexto natural. • Es correlacional transversal porque se recolecto los datos en un solo momento en un tiempo único.

Fuente: Elaboración propia

ANEXO N° 3: PROPUESTA PARA LA MEJORA DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD SEGÚN LA ISO 27001.

1. PROCESOS DE LA ISO 27001 A APLICAR.

Los Procesos de la Auditoria ISO a aplicar está en Base a los controles de seguridad de la Información descritos en el anexo A de la Norma ISO 27001:

- **A5. POLITICAS DE LA SEGURIDAD DE LA INFORAMACION (Normativa)**
- **A.11 SEGURIDAD FISICA Y DEL ENTORNO (Infraestructura)**
- **A12 SEGURIDAD DE LAS OPERACIONES (Cultura)**

2. LOS CONTROLES A MEJORAR SEGÚN EL ANEXO A DE LA ISO 27001 SON:

- A5.1 Directrices de gestión de la seguridad de la Información
- A11.1 Áreas seguras
- A11.2 Seguridad de los equipos
- A12.1 Procedimientos y responsabilidades operacionales
- A12.2 Protección contra el software malicioso (malware)
- A12.3 Copias de Seguridad
- A12.4 Registros y supervisión
- A12.5 Control del Software en explotación
- A12.6 Gestión de Vulnerabilidad Técnica
- A12.7 Consideraciones sobre la auditoria de sistemas de información

3. PROPUESTA PARA MEJORAR LOS CONTROLES DE SEGURIDAD DE LA MUNICIPALIDAD SEGÚN LA ISO 27001

1. ALCANCE.

Las normas y procedimientos deben estar establecidos en una Directiva para su cumplimiento obligatorio para todos los órganos y/o unidades orgánicas de la Municipalidad distrital de san Juan Bautista.

2. RESPONSABILIDAD.

Los Gerentes, Subgerentes y demás funcionarios públicos de la Municipalidad Distrital de san Juan Bautista, son los responsables de la implementación y cumplimiento de la Directiva.

La Responsabilidad recae en todos los trabajadores independientemente del régimen laboral que tengan con la corporación Municipal, tratándose de un mecanismo de seguridad de la información.

La Gerencia de Tecnologías de Información es la responsable de la implementación, aplicación, seguimiento y supervisión para el estricto cumplimiento de la Directiva.

3. DISPOSICIONES GENERALES.

3.1. Los Gerentes, Subgerentes, y demás funcionarios públicos de la Municipalidad distrital de San Juan Bautista, son los responsables directos del buen uso de la información en sus respectivas unidades orgánicas.

3.2. La Municipalidad Distrital de san Juan Bautista, garantizará la aplicación de las medidas de seguridad de la información establecidas y optimizará su gestión mediante la conformación del Comité de seguridad de la Información, el Oficial o Coordinador.

3.3. La Alta Dirección reconoce como activos de información estratégicos de la corporación municipal, la información contenida en cualquier medio y sistemas que la soportan. Por lo tanto, las directivas de seguridad de la información son de aplicación obligatoria para todo el personal.

3.4. Cuando exista la necesidad de otorgar algún acceso lógico y físicos a los servicios de tecnologías de la información u oficinas de la institución a personas o empresas que no tengan ningún vínculo directivo y/o contrato, deberán ejecutarse medidas que garanticen la seguridad de la información, las cuales serán establecidas previamente por la Gerencia de tecnologías de la Información y los responsables de las unidades orgánicas de la entidad.

3.5. En todos los contratos suscritos ya sea de presentación de servicios personales, servicios para la administración y control de los sistemas de información, redes y/o ambientes de procesamiento de información, consultorías, servicios entre otros, se deberá establecer la inclusión de términos relacionados a la seguridad de la información.

3.6. La Gerencia de Tecnologías de la Información es el órgano rector de las actividades informáticas y responsable de la administración de los sistemas implementados en la Entidad.

3.7. La Subgerencia de Recursos Humanos debe implementar dentro de su procedimiento de reclutamiento de personal, la firma por parte del nuevo personal de un acta de compromiso de conocimiento y aplicación de la directiva, así como de otros documentos que aseguren el correcto uso de la información de la Corporación Municipal.

4. DISPOSICIONES ESPECÍFICAS.

4.1. DE MEDIDAS DE SEGURIDAD.

4.1.1. Con relación a las medidas de seguridad presentadas en la Municipalidad.

a. La Gerencia de Tecnologías de la Información, en el marco de un plan de seguridad de la información, deberá implementar las medidas antes mencionadas, debiendo contar con la infraestructura adecuada.
b. La Gerencia de Tecnologías de la Información, debe informar periódicamente a los usuarios de las restricciones de seguridad implantadas en la institución, para proteger la información gestionada para los servicios.
c. La Gerencia de Tecnologías de la Información por lo menos una vez al año deberá realizar un inventario de los activos de la información en la cual indique el tipo de activo, clasificación, propietario el cual se le dará la responsabilidad respectiva en el uso adecuado del activo.
d. Crear las políticas e implementar los controles de la seguridad física, mediante la generación de perímetros de seguridad de protección de los activos informáticos.
e. La información que se procesa será respaldada por periodos, de acuerdo a la frecuencia de modificación de la información.
f. Una vez concluido el proceso de respaldo de la información, se realizará una prueba de funcionamiento utilizando el medio de respaldo, para comprobar que las copias se han realizado con éxito.
g. La información almacenada se mantendrá por un periodo que estime conveniente la institución, en concordancia con las normas establecidas por la autoridad competente.
h. La actividad de respaldo de la información, será supervisada por el responsable de la seguridad de la información de la institución.

i. Las copias de respaldo (backup) se almacenarán en la caja fuerte de la municipalidad, en sobre lacrado. De ser posible se deberá contratar almacenamiento fuera de las instalaciones del centro de cómputo como medida de control de seguridad.

4.1.2. Acciones de Detección.

a. Revisar periódicamente las últimas actividades realizadas en la base de datos en busca de acciones sospechosas, efectuadas por usuarios externos o internos, mediante controles preventivos adecuados, como detectores de intrusos, registros de auditoria, entre otras.
b. Configurar el sistema y guardar periódicamente sus resultados en un medio confiable. Realizar comparaciones periódicas de la configuración operativa actual con la configuración inicial.
c. comprobar periódicamente la integridad de los archivos importantes del sistema.
d. verificar periódicamente los permisos de los archivos que se encuentren en los directorios de usuarios.
e. Asegurar que los eventos y debilidades en la seguridad de la información asociados con los sistemas de información, sean comunicados de manera que se tomen las acciones correctas a tiempo.

4.1.3. Acciones de Recuperación.

a. Disponer de procedimientos de contingencias, que permitan minimizar los daños y proteger la información del servicio a nivel bases de datos, aplicaciones, configuración de los sistemas operativos y de comunicaciones, para ello es necesario contar con un sistema de respaldo de información (backup).
b. Los procedimientos de contingencias, deberán ser debidamente documentados y difundidos entre el personal responsable y operativo de la Gerencia de Tecnologías de la Información.

c. La Gerencia de Tecnologías de Información, deberá planificar el desarrollo de un plan de contingencia que incluya identificación de riesgo, identificación de soluciones, estrategias, documentación de procesos, realización de pruebas, implementación y mejoras.
d. Establecer periódicamente cursos de capacitación y simulacros, que permitan evaluar la respuesta del personal involucrado en la recuperación de contingencia, de sistemas completos (sistema operativo, aplicaciones, servicios y datos).

4.2. DE LAS ACCIONES DE PREVENCIÓN.

4.2.1. Con relación a las áreas de trabajo y las aplicaciones utilizadas.

a. La Gerencia de Tecnologías de la Información, debe brindar a los usuarios acceso restringido, de acuerdo a sus funciones y responsabilidades asignadas al personal autorizado.
b. La información de servicios y procedimientos administrativos a proveer a la ciudadanía, deben administrarse por medios electrónicos con aplicaciones seguras.
c. Debe incorporarse un sistema de seguridad antivirus, a los servidores que gestionan las bases de datos, y en las estaciones donde se procesa la información.
d. Se recomienda incluir una herramienta de detecciones de intrusos y control de accesos, para proteger la información de carácter confidencial de la institución.
e. Disponer de copias completas de seguridad (backup) de la información, base de datos y aplicativos, con herramientas de respaldo en línea que evite interrumpir los servicios de los servidores.
f. Disponer de dispositivos para copias de respaldo (backup), Discos Duros de tecnología SCSI o SATA conforme a los servidores, para un respaldo adecuado.
g. Resolver el problema de administración de cuentas y grupos para tener el absoluto control de quienes son las personas autorizadas y con

derechos en los recursos de almacenamiento. Debe existir un registro de usuarios con sus derechos y privilegios. Debe existir registro de usuarios con sus derechos y privilegios.

h. Tener adecuada alimentación eléctrica, que involucra el estado de los pozos a tierra, estabilizador, UPS (Suministro de Poder Ininterrumpido), grupo electrógeno y redes de alimentación eléctrica independientes.

4.3. DE LOS SISTEMAS DE REDES.

4.3.1. Con relación a los sistemas de red local y de conectividad a Internet.

a. La red local y el sistema de conectividad a Internet deben contar con sistemas de seguridad.
b. Debe tenerse en consideración la aplicación de todas las técnicas de seguridad que se evalúa como convenientes: Cortafuegos, detección de intrusos, inspección de contenido, auditoria, filtrado, proxi, criptografía o autenticación; que permitan controlar la seguridad de los usuarios de la red local y del sistema de conectividad e internet.
c. Implementar políticas de restricciones en la asignación de las direcciones IP, en los usuarios.
d. Se debe tener actualizado la estructura de la red de datos y comunicaciones, identificando locales, equipos utilizados, ips y demás información relevante para su supervisión.
e. Dadas las acciones de control en los equipos, sobre el bloqueo de programas como Facebook, twitter, YouTube y otros que la entidad considere necesario limitar, se considerara como falta de parte del usuario, el vulnerar dichas configuraciones a fin de recuperar dichos accesos.

4.3.2. Con relación a la gestión del servidor web y servidor de Correo Electrónico.

a. Cerrar los servicios de comunicación del servidor, que no sean estrictamente necesarios y en especial los scripts CGI y los módulos de los aplicativos que soportan la identificación para acceso remoto (login remoto).
b. Minimizar el número de aplicaciones y archivos abiertos en los servidores.
c. implementar políticas de control de acceso (deshabilitar las cuentas del sistema a usuarios que dejaron de laborar en la institución, personal con licencia, control de horario en cuentas, deshabilitar las cuentas de usuarios que no se conecten al sistema durante un periodo de tiempo determinado por el administrador, etc.).
d. implementar procedimientos de validación del servicio de datos y otros procesos, para garantizar los servicios de 7 días por 24 horas.

4.4. DE LA SEGURIDAD FÍSICA.

4.4.1. Se recomienda que los equipos donde se graba la información reciban mantenimiento preventivo y correctivo, con una frecuencia de acuerdo a las especificaciones técnicas del equipo o a un cronograma estable.

4.4.2. Se deben desarrollar documentos normativos y guías de seguridad en el buen uso y tratamiento de los equipos, para poder brindar seguridad física de los activos más importantes de la Municipalidad.

4.4.3. Los ambientes donde se guardan los medios de almacenamiento de la información contarán con adecuadas condiciones de temperatura, humedad, entre otras.

4.4.4. Los ambientes donde se encuentran los medios de almacenamiento serán de acceso restringido, solo estará autorizado el ingreso al personal responsable de la Seguridad de la Información

4.5. DE LA DOCUMENTACIÓN

4.5.1. La gerencia de Tecnología de Información, planificará y organizará el proceso del respaldo de la información de la institución, teniendo en cuenta el nivel de importancia de la información. El procedimiento formara parte del Plan de Seguridad de la Información institucional.

4.5.2. La Gerencia de Tecnología de la Información, especificará y documentará, en el Plan de Contingencias institucionales, los procedimientos utilizados en el respaldo de la información, plan que debe considerar lo siguiente:

a. El respaldo de la configuración de los servidores y estaciones cliente, que permitan su puesta en marcha ante una eventual contingencia.
b. Los procedimientos para realizar el respaldo y la restauración de la información a nivel de servidores y estaciones cliente.

4.6. DEL RESPALDO.

4.6.1. La Gerencia de Tecnologías de Información, dispondrá de un sistema de respaldo de información para minimizar los daños y proteger la información procesada, al nivel de base de datos, aplicaciones, configuración de los sistemas operativos y de comunicaciones.

4.6.2. Dependiendo de la importancia del servicio que preste la Municipalidad y con la finalidad de asegurar la continuidad de sus

operaciones, ésta dispondrá de un sistema de respaldo de información en línea (dos sistemas de respaldo de información simultáneos), de acuerdo a su disponibilidad presupuestal.

4.6.3. Se realizará copias de seguridad de la información en medios de almacenamiento cada vez que los archivos o bases de datos se actualicen, estas copias se podrán efectuar en tres formas:

a. Respaldo Total: copia completa de todos los archivos en un solo medio de almacenamiento.

b. Respaldo Incremental: copia de todos los cambios o adiciones que se realizan a determinados archivos cada día.

c. Respaldo Diferencial: copia de cambios o adiciones que se realizan a determinados archivos respecto al respaldo total, después de cierto periodo de tiempo.

4.6.4. Los usuarios que tienen asignada una computadora, son responsables de realizar el respaldo de la información local, de acuerdo al periodo establecido en el plan de respaldo de la información institucional, para lo cual la Gerencia de Tecnologías de la Información, facilitara los recursos necesarios y guardara la copia de los mismos. Para los casos de mayor riesgo, de acuerdo a la disponibilidad del servidor, podrán guardar su información en carpetas compartidas, en las cuales se realizarán las copias de respaldo adicional.

4.6.5. El disco duro será depurado permanentemente, eliminando o realizando una copia de los archivos que no volverán a ser utilizados en forma inmediata.

4.6.6. El responsable del respaldo proporcionará a los usuarios las copias de seguridad de la información, base de datos y aplicativos, en caso de pérdida o daño de la información residente en el medio local.

4.6.7. Se informará periódicamente a los usuarios, el cronograma de respaldo de información, asimismo, hará de conocimiento general las políticas de seguridad y respaldo de información.

5. ASPECTOS COMPLEMENTARIOS.

5.1. La Gerencia de Tecnología de la Información brindara el asesoramiento y apoyo técnico correspondiente.

5.2. El traslado de información interno o externo debe ser autorizado por el funcionario responsable que genera la información o su inmediato superior de ser necesario.

5.3. Los archivos digitales cualquiera sea su origen (hoja de cálculo, procesador de texto u otros), no deben contener claves que restrinjan su visualización salvo orden o autorización expresa del funcionario responsable.

5.4. Los datos, registros y todo tipo de recolección o generación de información generada como parte de las labores que desempeña un trabajador que presta servicios a la entidad municipal, son parte del archivo digital de la misma; motivo por el cual debe proveer el acceso a dicha información en caso de vacaciones, permisos programados, suspensión, cese u otro tipo de ausencia.

5.5. Las unidades orgánicas quedan encargadas de comunicar y formular las disposiciones complementarias a su personal para la implementación de la directiva.

6. DISPOSICIONES COMPLEMENTARIAS FINALES.

PRIMERA. Para los aspectos no previstos en la Directiva, se aplicará supletoriamente las normas legales vigentes sobre la materia. Adicionalmente se deberá tener en cuenta la adecuación a cualquier norma legal que se establezca con posterioridad a la fecha de aprobación de la Directiva.

SEGUNDA. La Subgerencia de Recursos Humanos en coordinación con la Gerencia de Tecnologías de la Información efectuaran periódicamente eventos de capacitación al personal de la Municipalidad Distrital de San Juan Bautista, referido a la normatividad vigente para el cumplimiento de la Directiva y de las normas legales sobre la materia.

TERCERA. LA Gerencia de Tecnologías de la Información podrá emitir disposiciones específicas en el marco de las normas establecidas en la Directiva.

CUARTA. El incumplimiento de las disposiciones contenidas en la Directiva, por parte de cualquier servidor de la Municipalidad Distrital de San Juan Bautista, deviene en responsabilidad del servidor infractor y del funcionario a cargo del Órgano y/o Unidad Orgánica a la que pertenece, por lo que se les aplica las sanciones correspondientes de acuerdo a lo establecido por las normas legales vigentes y normas internas de la Corporación Municipal de acuerdo al Régimen laboral al que pertenezca.

QUINTA. La Directiva entrara en vigencia a partir del día siguiente de su aprobación a través del correspondiente acto administrativo. Asimismo, será publicada en el portal institucional de la Corporación Municipal.

7. ÁREAS INVOLUCRADAS EN EL PROCESO DE AUDITORIA SEGÚN LA ISO 27001.

- OFICINA DE INFORMÁTICA Y TELECOMUNICACIONES.
- GERENCIA DE ADMINISTRACIÓN Y FINANZAS.
  - SUB GERENCIA DE RECURSOS HUMANOS.
  - SUB GERENCIA DE CONTABILIDAD.
  - SUB GERENCIA DE TESORERÍA.
  - SUB GERENCIA DE LOGÍSTICA.
- GERENCIA DE RENTAS.
  - SUB GERENCIA DE ADMINISTRACIÓN Y FISCALIZACIÓN TRIBUTARIA.
  - SUB GERENCIA DE RECAUDACÓN Y ARCHIVO TRIBUTARIO.
  - SUB GERENCIA DE EJECUCIÓN COACTIVA
- GERENCIA DE PLANEAMIENTO Y PRESUPUESTO.

ANEXO 04

CUESTIONARIO

(Para Trabajadores de la Municipalidad Distrital de San Juan Bautista)

CÓDIGO: ----------

El presente cuestionario tiene como propósito obtener datos sobre **EL PROCESO DE AUDITORIA ISO 27001 PARA LA MEJORA DE LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE SAN JUAN BAUTISTA - 2018**

Gracias

I. Instrucciones

- Lee detenidamente el cuestionario y respóndalas
- La información que nos proporciona será confidencial.
- No deje preguntas sin responder.

II. Contenido.

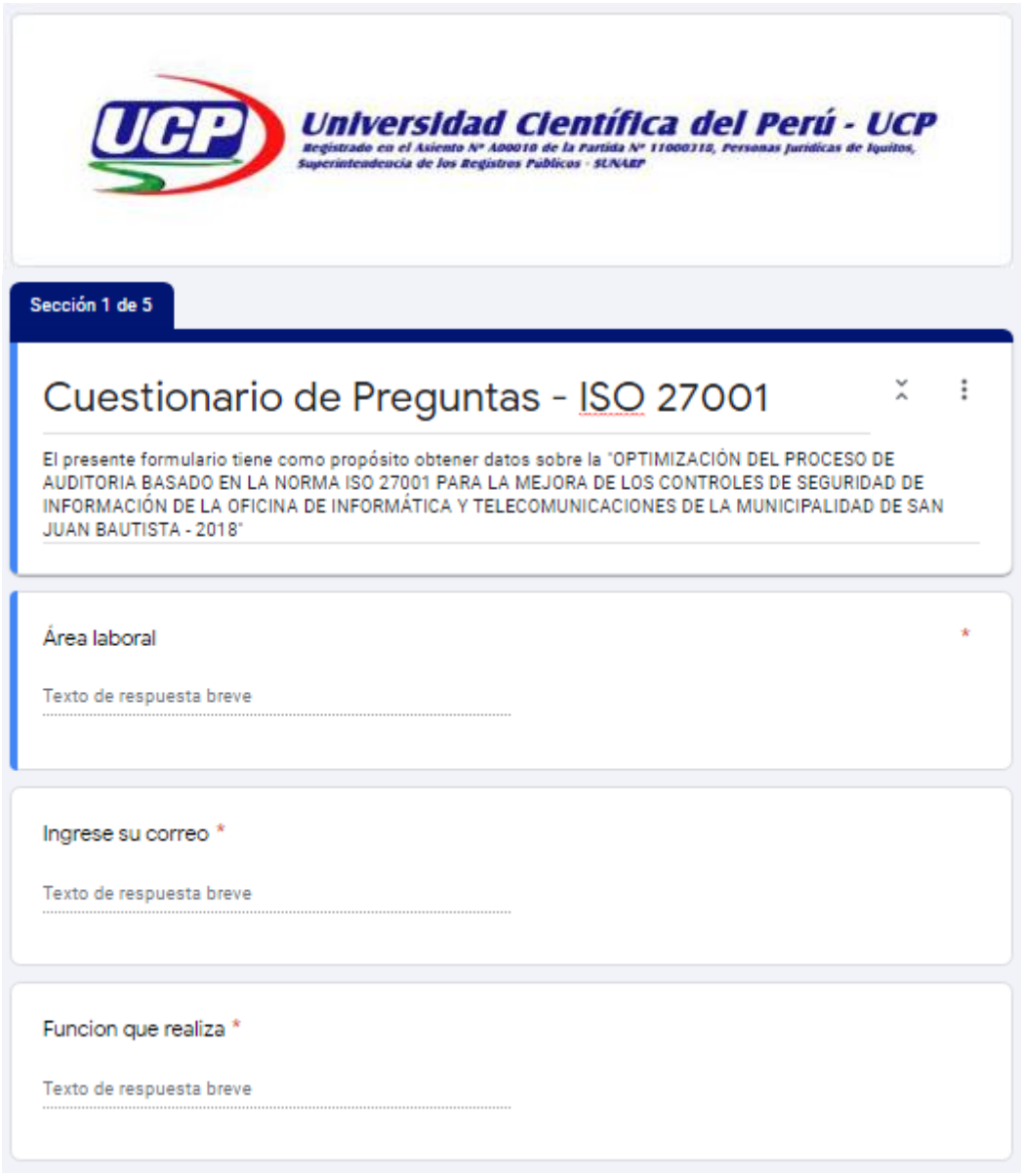
PROCESO DE AUDITORIA DE SEGURIDAD INFORMATICA – NORMATIVIDAD		MUY MALO	MALO	REGULAR	BUENO	MUY BUENO
	EFECTIVIDAD	0 - 3	4 - 7	8 - 11	12 - 15	16 - 20
P1	¿En una escala del 0 al 20, qué nivel de conocimiento tiene acerca de los procesos de auditoria ISO - 27001 para la generación de directrices de seguridad?					
P2	¿En una escala del 0 al 20, que nivel de eficacia percibida tendría la aplicación periódica de procesos de auditoria ISO 27001 a los controles de seguridad para lograr la generación de directrices?					
P3.	¿En una escala del 0 al 20, que nivel de eficiencia percibida tendría la aplicación periódica de procesos de auditoria ISO 27001 a los controles de seguridad para la generación de directrices con menos tiempo y recursos?					
	Promedio ($\overline{x}$)					

PROCESO DE AUDITORIA DE SEGURIDAD INFORMATICA – CULTURA DE SEGURIDAD		MUY MALO	MALO	REGULAR	BUENO	MUY BUENO
	CONFIABILIDAD	0 - 3	4 - 7	8 - 11	12 - 15	16 - 20
P4	¿En una escala del 0 al 20, qué nivel de conocimiento tiene acerca de los procesos de auditoria, basado en la Norma ISO - 27001 para la mejora de la cultura de seguridad?					
P5	¿En una escala de 0 a 20; qué nivel de cultura de seguridad percibida tendría la aplicación periódica de procesos de auditoria ISO 27001 a los controles de seguridad para la sensación de protección de la Información?					
P6	¿En una escala de 0 a 20; qué nivel de cultura de seguridad percibida tendría la aplicación periódica de procesos de auditoria ISO 27001 a los controles de seguridad para la aplicación de buenas prácticas de seguridad de la Información?					
	Promedio ($\overline{x}$)					

PROCESO DE AUDITORIA DE SEGURIDAD INFORMATICA – INFRAESTRUCTURA TECNOLOGICA		MUY MALO	MALO	REGULAR	BUENO	MUY BUENO
Funcionalidad		0 - 3	4 - 7	8 - 11	12 - 15	16 - 20
P7	¿En una escala del 0 al 20, qué nivel de conocimiento tiene acerca de los procesos de auditoria ISO 27001 para el fortalecimiento de la infraestructura tecnológica?					
P8	¿En una escala de 0 a 20; qué nivel de seguridad percibida tendría la aplicación periódica de procesos de auditoria ISO 27001 a los controles de seguridad para el fortalecimiento de la infraestructura tecnológica de hardware?					
P9	¿En una escala de 0 a 20; qué nivel de seguridad percibida tendría la aplicación periódica de procesos de auditoria ISO 27001 a los controles de seguridad para el fortalecimiento de la infraestructura tecnológica de software?					
	Promedio ($\overline{x}$)					

ANEXO 05

CUESTIONARIO DIGITAL USANDO LA HERRAMIENTA DE GOOGLE DRIVE



Universidad Científica del Perú - UCP

Registrado en el Asiento Nº A00010 de la Partida Nº 11000310, Personas Jurídicas de Iquitos, Superintendencia de los Registros Públicos - SUNARP

Sección 1 de 5

Cuestionario de Preguntas - ISO 27001

El presente formulario tiene como propósito obtener datos sobre la "OPTIMIZACIÓN DEL PROCESO DE AUDITORIA BASADO EN LA NORMA ISO 27001 PARA LA MEJORA DE LOS CONTROLES DE SEGURIDAD DE INFORMACIÓN DE LA OFICINA DE INFORMÁTICA Y TELECOMUNICACIONES DE LA MUNICIPALIDAD DE SAN JUAN BAUTISTA - 2018"

Área laboral *

Texto de respuesta breve

Ingrese su correo *

Texto de respuesta breve

Funcion que realiza *

Texto de respuesta breve

Sección 2 de 5

VÍDEO SOBRE LA ISO - 27001

Sistemas de Gestión de Seguridad de la Información

ISO - 27001

Sección 3 de 5

Cuestionario de Preguntas - ISO 27001

PROCESO DE AUDITORIA DE SEGURIDAD INFORMÁTICA - NORMATIVIDAD

¿En una escala del 0 al 20, Cual es nivel de conocimiento que tiene acerca de la aplicación de procesos de auditoria Basado en la Norma ISO - 27001? *

Texto de respuesta breve

¿En una escala del 0 al 20, Que nivel de eficacia tendría la aplicación periódica de procesos de auditoria de seguridad de la información basada en la ISO - 27001, en el cumplimiento de las directrices de seguridad en la oficina de informática y telecomunicaciones de la Municipalidad Distrital de San Juan Bautista? *

Texto de respuesta breve

¿En una escala del 0 al 20, Que nivel de eficiencia tendría la aplicación periódica de procesos de auditoria de seguridad de la información basada en la ISO - 27001, en el cumplimiento de las directrices de seguridad en la oficina de informática y telecomunicaciones de la Municipalidad Distrital de San Juan Bautista? *

Texto de respuesta breve

Sección 4 de 5

Cuestionario de Preguntas - ISO 27001

PROCESO DE AUDITORIA DE SEGURIDAD INFORMÁTICA - CULTURA DE SEGURIDAD

¿En una escala del 0 al 20, Cual es nivel de cultura de seguridad de los usuarios finales de la infraestructura tecnológica que se percibe en la Municipalidad Distrital de San Juan Bautista? *

Texto de respuesta breve

¿En una escala de 0 a 20; indicar; cual es el nivel de conocimiento que tiene acerca de la aplicación de procesos de auditoria basados en la norma ISO 27001 y su relación con la mejora de la cultura de seguridad en las instituciones públicas o privadas? *

Texto de respuesta breve

¿En una escala de 0 a 20; indicar; qué nivel de Confiabilidad en la tecnología informática genera la aplicación periódica de procesos de auditoria de seguridad de la información basada en la ISO 27001, en la oficina de informática y telecomunicaciones de la Municipalidad Distrital de San Juan Bautista? *

Texto de respuesta breve

Sección 5 de 5

Cuestionario de Preguntas - ISO 27001

PROCESO DE AUDITORIA DE SEGURIDAD INFORMÁTICA - INFRAESTRUCTURA TECNOLÓGICA

¿En una escala de 0 a 20; indicar; cual es el nivel de conocimiento que tiene acerca de la aplicación de procesos de auditoria basados en la norma ISO 27001 y su relación con la seguridad de la infraestructura tecnológica de la información? *

Texto de respuesta breve

¿En una escala de 0 a 20; indicar; qué nivel de funcionalidad tendria la infraestructura de tecnologías de información con la aplicación periódica de procesos de auditoria de seguridad de la información basada en la ISO 27001, en la oficina de informática y telecomunicaciones de la Municipalidad Distrital de San Juan Bautista? *

Texto de respuesta breve

¿En una escala de 0 a 20; indicar; cual es el nivel de satisfacción dela funcionalidad de la infraestructura de tecnologías de información con la aplicación periódica de procesos de auditoria de seguridad de la información basada en la ISO 27001, en la oficina de informática y telecomunicaciones de la municipalidad Distrital de San Juan Bautista? *

Texto de respuesta breve

ANEXO 6
ANEXO "A" DE LA ISO 27001
ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
5.1 Directrices de la Dirección en seguridad de la información.
5.1.1 Conjunto de políticas para la seguridad de la información.
5.1.2 Revisión de las políticas para la seguridad de la información.
6 ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Asignación de responsabilidades para la segur. de la información.
6.1.2 Segregación de tareas.
6.1.3 Contacto con las autoridades.
6.1.4 Contacto con grupos de interés especial.
6.1.5 Seguridad de la información en la gestión de proyectos.
6.2 Dispositivos para movilidad y teletrabajo.
6.2.1 Política de uso de dispositivos para movilidad.
6.2.2 Teletrabajo.
7 SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
7.1 Antes de la contratación.
7.1.1 Investigación de antecedentes.
7.1.2 Términos y condiciones de contratación.
7.2 Durante la contratación.
7.2.1 Responsabilidades de gestión.
7.2.2 Concienciación, educación y capacitación en segur. de la información
7.2.3 Proceso disciplinario.
7.3 Cese o cambio de puesto de trabajo.
7.3.1 Cese o cambio de puesto de trabajo
8 GESTION DE ACTIVOS
8.1 Responsabilidad sobre los activos.
8.1.1 Inventario de activos.
8.1.2 Propiedad de los activos.
8.1.3 Uso aceptable de los activos.
8.1.4 Devolución de activos.
8.2 Clasificación de la información.
8.2.1 Directrices de clasificación.
8.2.2 Etiquetado y manipulado de la información.
8.2.3 Manipulación de activos.
8.3 Manejo de los soportes de almacenamiento.
8.3.1 Gestión de soportes extraíbles.
8.3.2 Eliminación de soportes.
8.3.3 Soportes físicos en tránsito.
9 CONTROL DE ACCESOS
9.1 Requisitos de negocio para el control de accesos.
9.1.1 Política de control de accesos.
9.1.2 Control de acceso a las redes y servicios asociados.
9.2 Gestión de acceso de usuario.
9.2.1 Gestión de altas/bajas en el registro de usuarios.
9.2.2 Gestión de los derechos de acceso asignados a usuarios.
10.1.2 Gestión de claves.
11. SEGURIDAD FÍSICA Y AMBIENTAL.
11.1 Áreas seguras.
11.1.1 Perímetro de seguridad física.
11.1.2 Controles físicos de entrada.
11.1.3 Seguridad de oficinas, despachos y recursos.
11.1.4 Protección contra las amenazas externas y ambientales.
11.1.5 El trabajo en áreas seguras.
11.1.6 Áreas de acceso público, carga y descarga.
11.2 Seguridad de los equipos.
11.2.1 Emplazamiento y protección de equipos.
11.2.2 Instalaciones de suministro.
11.2.3 Seguridad del cableado.
11.2.4 Mantenimiento de los equipos.
11.2.5 Salida de activos fuera de las dependencias de la empresa.
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
11.2.8 Equipo informático de usuario desatendido.
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
12. SEGURIDAD EN LA OPERATIVA.
12.1 Responsabilidades y procedimientos de operación.
12.1.1 Documentación de procedimientos de operación.
12.1.2 Gestión de cambios.
12.1.3 Gestión de capacidades.
12.1.4 Separación de entornos de desarrollo, prueba y producción.
12.2 Protección contra código malicioso.
12.2.1 Controles contra el código malicioso.
12.3 Copias de seguridad.
12.3.1 Copias de seguridad de la información.
12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad.
12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema.
12.4.4 Sincronización de relojes.
12.5 Control del software en explotación.
12.5.1 Instalación del software en sistemas en producción.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Gestión de las vulnerabilidades técnicas.
12.6.2 Restricciones en la instalación de software.
12.7 Consideraciones de las auditorías de los sistemas de información.
12.7.1 Controles de auditoría de los sistemas de información.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.
13.1 Gestión de la seguridad en las redes.
13.1.1 Controles de red.
14.2.1 Política de desarrollo seguro de software.
14.2.2 Procedimientos de control de cambios en los sistemas.
14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el
sistema operativo.
14.2.4 Restricciones a los cambios en los paquetes de software.
14.2.5 Uso de principios de ingeniería en protección de sistemas.
14.2.6 Seguridad en entornos de desarrollo.
14.2.7 Externalización del desarrollo de software.
14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
14.2.9 Pruebas de aceptación.
14.3 Datos de prueba.
14.3.1 Protección de los datos utilizados en pruebas.
15. RELACIONES CON SUMINISTRADORES.
15.1 Seguridad de la información en las relaciones con suministradores.
15.1.1 Política de seguridad de la información para suministradores.
15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
15.2 Gestión de la prestación del servicio por suministradores.
15.2.1 Supervisión y revisión de los servicios prestados por terceros.
15.2.2 Gestión de cambios en los servicios prestados por terceros.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
16.1 Gestión de incidentes de seguridad de la información y mejoras.
16.1.1 Responsabilidades y procedimientos.
16.1.2 Notificación de los eventos de seguridad de la información.
16.1.3 Notificación de puntos débiles de la seguridad.
16.1.4 Valoración de eventos de seguridad de la información y toma de
decisiones.
16.1.5 Respuesta a los incidentes de seguridad.
16.1.6 Aprendizaje de los incidentes de seguridad de la información.
16.1.7 Recopilación de evidencias.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
17.1 Continuidad de la seguridad de la información.
17.1.1 Planificación de la continuidad de la seguridad de la información.
17.1.2 Implantación de la continuidad de la seguridad de la información.
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad

ANEXO 7

Inventario de activos del proceso de gestión de la infraestructura tecnológica de la OIT de la Municipalidad Distrital de San Juan Bautista

N°	Nombre del activo	Descripción del activo	Tipo de Activo	Ubicación
1	Datos vitales	Datos que almacenan los diferentes sistemas de información esenciales para el funcionamiento de la MPSJB	Dato/Información	Data Center
2	Archivos Personales	Documentos personales de los trabajadores de la MPSJB	Dato/Información	Computadoras Personales
3	Copias de Respaldo	Copias de respaldo de la datos/información que manejan los distintos sistemas de la MPSJB	Dato/Información	Data Center/PC Administrador
4	Datos de Configuración de los Sistemas de Información	Corresponde a los documentos, manuales y procedimientos relacionados con la administración de los diferentes sistemas de información	Dato/Información	Archivo físico (estantería)
5	Datos de Gestión interna	Corresponde a los documentos de la MPSJB	Dato/Información	Archivo físico (estantería)/VPS
6	Credenciales (contraseñas)	Usuario y Contraseña que utilizan los usuarios para ingresar a los recursos tecnológicos.	Dato/Información	Excel (Administradores)
7	Datos de control de acceso	Corresponde a los datos de los usuarios internos que utilizan los sistemas de información y/o aplicaciones	Dato/Información	Base de Datos/Usuario Interno

8	Log de los sistemas de información	Log que contiene los registros de los eventos de seguridad y de los eventos de administración sobre las aplicaciones.	Dato/Información	Servidores
9	Código fuente de los sistemas de información	Corresponde a los códigos fuente de los distintos sistemas desarrollados en MPSJB	Dato/Información	Servidores de Versiones (en la nube)
10	Código ejecutable	Corresponde a los códigos ejecutables de los diferentes sistemas de información	Dato/Información	Servidor de desarrollo/Disco de backup)
11	Servicios online	Corresponde a los servicios de consulta como, por ejemplo: Portal de transparencia, Foro Municipal, consulta de visita a funcionarios.	Servicio	Página Web de la MPSJB
12	Correo electrónico	Correo electrónico institucional	Servicio	Servidor de correo electrónico GMAIL corporativo
13	Gestión de privilegios	Corresponde al mecanismo para la administración y asignación de privilegios de acceso a los recursos tecnológicos y aplicaciones.	Servicio	Sistemas de información
14	Base de Datos	Bases de datos de los diferentes sistemas que almacenan la información de la entidad	Servicio	Servidores de base de Datos
15	Página Web	Página Web de la entidad	Software/Aplicaciones informática	VPS
16	Sistema de trámite documentario	Sistema para la gestión de trámite externo e interno,	Software/Aplicaciones informática	Servidor de aplicaciones Windows

		utilizado por la unidad de trámite documentario y archivos		
17	Calendario de actividades	Registro de las actividades que se realizan en la MPSJB	Software/Aplicaciones informática	Servidor VPS
18	SIAF	Sistema que manejan las dependencias de la oficina de administración	Software/Aplicaciones informática	Servidor SIAF
19	Sistema de Catastro y ficha catastral	Sistemas que usa la Sub Gerencia de Planeamiento Urbano y Catastro	Software/Aplicaciones informática	Servidor de aplicación catastro/servidor de BD Catastro
20	Sistema Gestor de Base de Datos	Sistema de gestión y administración de las bases de datos de la entidad	Software/Aplicaciones informática	PC de los administradores
21	Aplicaciones Comerciales	Office, sistemas operativos, antivirus, entre otros	Software/Aplicaciones informática	Computadoras Personales
22	Gestor de máquinas virtuales	Aplicativo que gestiona las máquinas virtuales	Software/Aplicaciones informática	PC Administradores
23	Scripts de backup	Scripts para sacar backup	Software/Aplicaciones informática	PC Administradores
24	Aplicativos de Desarrollo	Aplicativos que se usan para el desarrollo de software interno	Software/Aplicaciones informática	PC de administradores
25	Servidores de aplicaciones de Producción	Servidores de producción que soportan las aplicaciones y sistemas de información	Equipos informáticos	Data Center de la Municipalidad
26	Servidores de Base de datos	Servidores de producción que soportan los motores e instancias de bases de datos	Equipos informáticos	Data Center de la Municipalidad
27	Servidores de prueba	Servidor en que se realizan las pruebas de los sistemas de información.	Equipos informáticos	Data Center de la Municipalidad

28	Servidor de desarrollo	Servidor de desarrollo	Equipos informáticos	
29	Computador del Funcionario	Computadores que utilizan los funcionarios de la entidad	Equipos informáticos	Oficina de Tecnologías de Información
30	Computadores administradores de SI	Computadores que utilizan los administradores de las plataformas, los desarrolladores	Equipos informáticos	Oficina de Tecnologías de Información
31	Computadores de escritorio usuarios	Computadores asignados a los colaboradores de la Oficina de Tecnologías de Información	Equipos informáticos	Oficina de Tecnologías de Información
32	Impresoras	Impresoras de la OIT	Equipos informáticos	Oficina de Tecnologías de Información
33	Escáner	Escáner de la Oficina de Tecnologías de Información	Equipos informáticos	Oficina de Tecnologías de Información
34	Firewall	Equipos informáticos destinados a proteger la seguridad perimetral de la entidad	Equipos informáticos	Data center
35	Soporte de la red	Equipamiento necesario para transmitir datos: routers, módems, switch, punto de acceso inalámbrico	Equipos informáticos	Data center
36	Centralita telefónica	Red de comunicación analógica	Redes de Comunicaciones	Data center
37	ADSL	Infraestructura utilizada para la conectividad	Redes de Comunicaciones	Data center
38	Red inalámbrica	Red de comunicación inalámbrica	Redes de Comunicaciones	Oficinas de la MPSJB

39	Red local	Red de comunicaciones cableada	Redes de Comunicaciones	Red local
40	Internet	Red de redes	Redes de Comunicaciones	Internet
41	Disco duro externo	Disco duro externo	Soportes de Información	Data center
42	Dispositivos de almacenamiento externo	CDs, DVDs, etc.	Soportes de Información	Archivo físico o estante
43	Soportes no electrónicos	Dispositivos físicos de almacenamiento no electrónico como material impreso	Soportes de Información	Archivo físico o estante
44	Sistema de alimentación ininterrumpida	UPS	Equipamiento auxiliar	oficinas
45	Sistema de aire acondicionado	Sistema de aire acondicionado	Equipamiento auxiliar	Data Center
46	Gabinetes	Armarios de soporte a los sistemas de información	Equipamiento auxiliar	Data center
47	Data Center	Centro Principal de procesamiento donde reside la infraestructura para soportar la operación del negocio	Instalaciones	Local central de la MPSJB
48	Área de personal	Instalación donde están ubicados los colaboradores de la Oficina de Tecnologías de Información	Instalaciones	Local central de la MPSJB
49	Usuarios Externos	Usuarios externos a la MPSJB y que usan los servicios a través de la Página Web	Personal	Usuarios Externos
50	Usuarios Internos	Personal propio de la MPSJB	Personal	Oficinas de la MPSJB

51	Administradores de las plataformas	Corresponde a los administradores de los diferentes Sistemas, comunicaciones, BBDD, Seguridad	Personal	Oficina de Tecnologías de Información
52	Desarrolladores/Programadores	Personal encargado de producir los sistemas de información	Personal	Oficina de Tecnologías de Información
53	Personal de soporte técnico	Personal encargado del soporte técnico de la Municipalidad	Personal	Oficina de Tecnologías de Información
54	Proveedores	Proveedores de tecnología y comunicaciones	Personal	Externo