UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

PROGRAMA DE ESTUDIOS DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

Modelo de Seguridad informática para la seguridad de la información:Municipalidad Provincial de Yungay, 2021

Tesis para obtener el título profesional de Ingeniera en Informática y de Sistemas

Autora

Cochachin Jara Silvia Soledad

Asesor

Código ORCID 0000-0002-0741-5458

Martínez Carrión Javier

Huaraz – PERÚ

2022

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

PALABRAS CLAVE

Tema	**Política de Seguridad**
Especialidad	Seguridad Informática

KEYWORDS

Theme	**Security Policy**
Specialty	Computer Security

LÍNEA DE INVESTIGACIÓN

Línea	Sistema de Gestión
Área	Ciencias Sociales
Sub área	Economía y Negocios
Disciplina	Negocios y Management

Constancia de Originalidad

USP | VICERRECTORADO DE INVESTIGACIÓN

UNIVERSIDAD SAN PEDRO

CONSTANCIA DE ORIGINALIDAD

El que suscribe, Vicerrector de Investigación de la Universidad San Pedro:

HACE CONSTAR

Que, de la revisión del trabajo titulado **"Modelo de seguridad informática para la seguridad de la información: Municipalidad Provincial de Yungay, 2021"** del (a) estudiante: **Silvia Soledad Cochachin Jara,** identificado(a) con **Código Nº 1509100111**, se ha verificado un porcentaje de similitud del 19%, el cual se encuentra dentro del parámetro establecido por la Universidad San Pedro mediante resolución de Consejo Universitario Nº 5037-2019-USP/CU para la obtención de grados y títulos académicos de pre y posgrado, así como proyectos de investigación anual Docente.

Se expide la presente constancia para los fines pertinentes.

Chimbote, 21 de Febrero de 2023

UNIVERSIDAD SAN PEDRO
RECTORADO
Dr. LUIS VENEGAS GORDILLO
RECTOR (e)

NOTA:
Este documento carece de valor si no tiene adjunta el reporte del Software TURNITIN.

TÍTULO

Modelo de Seguridad informática para la seguridad de la información:Municipalidad Provincial de Yungay, 2021

RESUMEN

La presente investigaciones se trazó como objetivo general proponer un Modelo de Seguridad Informática basado en NIST SP 800 - 30 para proteger la información en la Municipalidad Provincial de Yungay, 202. La hipótesis consistió en que la propuesta del Modelo de Seguridad Informática influirá significativamente en la protección de la información. El tipo de investigación fue no experimental, de diseño descriptivo, se trabajó con población y muestra de 28 trabajadores ediles. Se aplicó encuesta. Se concluyó que la propuesta del Modelo de Seguridad Informática basado en NIST SP 800 - 30 va a contribuir a que cada uno de los usuarios tomen conciencia de la seguridad informática y se mejore la protección de la información desde las dimensiones de confidencialidad, integridad y disponibilidad. Que el estado situacional de la información sobre confidencialidad fue 9.68, esto significa malo, respecto a integridad de la información fue 10.39, es decir fue malo, y el estado situacional de la información respecto a la disponibilidad fue 10.71, lo cual fue malo. El estado situacional de la información en general fue 10.39, lo cual fue malo. Que se han encontrado 26.7% de riesgos con nivel bajo, 60.0% de riesgos con nivel medio o moderado, y 13.3% de riesgos de tipo alto, en total se encontraron 15 riesgos en el uso del sistema de información. Que el modelo de Seguridad Informática basado en NIST SP 800 – 30 ha sido desarrollado teniendo en cuenta las fases y riesgos encontrados en el sistema de información.

ABSTRACT

The present research was drawn as a general objective to propose a Computer Security Model based on NIST SP 800 - 30 to protect information in the Provincial Municipality of Yungay, 202. The hypothesis was that the proposed Computer Security Model will significantly influence the protection of information. The type of research was non-experimental, descriptive in design, we worked with the population and sample of 28 municipal workers. Survey was applied. It was concluded that the proposal of the Computer Security Model based on NIST SP 800 - 30 will contribute to each of the users becoming aware of computer security and improving the protection of information from the dimensions of confidentiality, integrity and availability. That the situational stateof the information on confidentiality was 9.68, this means bad, regarding the integrity of the information was 10.39, that is, it was bad, and the situational state of the information regarding availability was 10.71, which was bad. The overallsituational state of the information was 10.39, which was bad. That 26.7% of risks with low level, 60.0% of risks with medium or moderate level, and 13.3%of risks of high type have been found, in total 15 risks were found in the use of the information system. That the Computer Security model based on NIST SP 800 – 30 has been developed taking into account the phases and risks found in the information system.

I. INTRODUCCIÓN

El Presente Informe, se basa en antecedentes Locales. Nacionales e Internacionales. A nivel internacional, Medina (2017) en la tesis de grado denominada "Seguridad Informática: virus ransomware, el Secuestro virtual de datos es Posible" realizada en la Universidad Empresarial Siglo 21. Argentina, tuvo como objetivo general llevar a cabo la determinación de cómo los ataques informáticos tipo ransomware se infiltra, en las empresas, para ello, analizó técnicas más usadas por los piratas informáticos. Metodología: Se identificó que la investigación fue de tipo descriptiva y documental, de enfoque cualitativo, utilizó cuestionarios y fichas de observación, utilizó software de detección de ataques tipo Rasomware, análisis de los registros de la institución estudiada en el conocimiento del estado situacional respecto a la seguridad, los datos fueron registrados en Microsoft Excel, y en función a estos datos y los conocimientos teóricos de seguridad informática se describió el estado de seguridad informática en Microsoft Word. Concluyó que los objetos estudiados fueron atacados por diversas técnicas de malware, que la ejecución del ransomware modificaba los archivos, que uno de los aportes fue la profundización del funcionamiento de las distintas versiones de ransomware del tipo cifrador y donde se determinó un patrón de funcionamiento muy similar. Que se descubrieron propagación del virus por la red. En general el estado situacional de las instituciones financieras fue bueno, pero que fueron atacados esporádicamente.

A nivel nacional, Jara (2018) en la tesis de maestría titulada "Sistema de gestión deseguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018". Tesis de maestría. Universidad César Vallejo. Perú, se planteó como objetivo general la determinación de la influencia entre la implementación del Sistema de Gestión con el proceso de gestión del riesgo en el espacio estudiado. Metodología: aplicó enfoque cuantitativo, el tipo de investigación fue aplicada experimental de diseño pre experimental, aplicó método deductivo, trabajo con una población y nuestra

de 31 activos y 114 controles. Resultados: el nivel de riesgo encontrado antes fue de 9.96, mientras que en el después fue de 5.90. Los controles fueron aplicados en el pretest con 92.1% y en el postest con 99.1%. Concluyó que la implementación del Sistema de Gestión de Seguridad de la Información influyó en el proceso de gestión, que también influyó positivamente en la evaluación del riesgo en el proceso de gestión del riesgo, y que también influyó en el tratamiento del riesgo en el proceso de gestión del riesgo en el espacio estudiado.

Cabrera (2018) en la tesis de grado titulada "Diseño de un modelo de políticas basado en la norma ISO 27001, para mejorar la gestión de la seguridad de la información en la Municipalidad Distrital de Florida – Bongará Amazona" realizada en la Universidad Peruana Unión, Tarapoto, Perú; se planteó como objetivo general la implantación de un modelo de políticas basado en la norma ISO27001 con fines de gestión de la seguridad de la información en el espacio en estudio. Metodología: el tipo de investigación fue aplicada no experimental, de diseño descriptivo, de enfoque cuantitativo; trabajó con una población y muestra de 13 trabajadores. Concluyó que los trabajadores administrativos del espacio estudiado no consideraron a la seguridad como una prioridad alineada con sus propias estrategias; que la investigación, contribuyó a que la Municipalidad, en especial el personal de las áreas de Gerencia y Tesorería, tomen conciencia de la importancia en sus dimensiones de confiabilidad, integridad y disponibilidad para la institución, y que se fomentó la cultura de seguridad.

A nivel local, Armas y Pérez (2018) en la tesis de grado denominada "Desarrollo de un sistema de gestión de seguridad de la información para minimizar riesgos en los activos de información en la sub gerencia de informática y telecomunicaciones de la Municipalidad Distrital de Independencia 2016" realizada en la UNASAM, Huaraz, Perú; se planteó como objetivo general el desarrollo de un sistema de gestión de seguridad de la información, para minimizar riesgos en los activos de información de la Sub Gerencia de Informática y Telecomunicaciones en el espacio estudiado. Metodología: trabajó con una población y nuestra de 10 trabajadores, la

investigación fue aplicada de diseño descriptivo. Concluyó que de acuerdo con la aplicación del MAGERIT se encontró que el CID de la Información para su valoración como criterio. Que la identificación de los procesos involucrados y los activos y la evaluación de los riesgos y amenazas de cada uno de ellos y a los que están expuestos, se encontró que en su mayoría estuvieron entre un estado de intolerable y extremo riesgo.

Ortigoza et al. (2019) en la investigación de grado denominada "Políticas de seguridad informática para la administración de recursos tecnológicos y gestión de la información en la empresa consultorías y asesorías en seguridad y salud en el trabajo S.A.S, 2019", realizada en la Universidad Cooperativa de Colombia, se planteó como objetivo general realizar el diseño de políticas de seguridad informática para el manejo y control de los recursos informáticos en el espacio en estudio. Como metodología de desarrollo aplicó metodología basado en NTC- ISO/IEC 27001:2013 y 27002:2015, Microsoft Excel para cálculos estadísticos, Microsoft Word para elaboración del informe. La investigación fue de tipo no experimental, de diseño descriptivo, trabajó con una población de 34 trabajadores, aplicó encuesta. Concluyó que la institución no estableció o no contó con los protocolos obligatorios que garanticen los principios de la seguridad informática de confidencialidad, integridad y disponibilidad. Que se evidenció que la información y los equipos de la institución no estuvieron protegidos.

Monteza (2019) en la tesis de grado denominada "Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la Municipalidad Distrital de El Agustino", realizada en la Universidad Peruana de Ciencias Aplicadas. Lima. Perú, se planteó como objetivo general desarrollar el diseño del Sistema de Gestión de Seguridad de la Información fundamentado en la norma ISO/IEC 27001:2013 con la finalidad de dar protección a los activos de recaudación y fiscalización tributaria del espacio en estudio. Metodología: Aplicó la metodología Magerit, Mehari, Cramm, Octave y NIST SP 800-30. Concluyó que se encontró que no contaron con las medidas de seguridad adecuadas o de tenerlos no se encuentran correctamente definidos. Que respecto a la

identificación, clasificación y valorización de los activos de información del proceso de recaudación y fiscalización tributaria en el área de rentas existieron varios activos de información con nivel de criticidad alta en un 72% que deben ser protegidos. Que respecto a la identificación de los riesgos de los activos de información del proceso de recaudación y fiscalización tributaria en el área de rentas existieron varios activos de información que tienen un nivel de riesgo alto con un 44% y medio con 56%, en ese sentido, se recomendó implementar controles y medidas de seguridad. Que la propuesta en el área de rentas se puede reducir cuantitativamente los riesgos de los activos de información en un nivel aceptable.

Medrano (2019) en la tesis de grado denominada "Plan de la seguridad de la información basado en la norma ISO 27001 para la sub gerencia de informática y tecnologías de la información de la Municipalidad de Punta Hermosa" realizada en la Universidad Nacional Tecnológica de Lima Sur, Perú; se planteó como objetivo general realizar la propuesta de un Plan de Seguridad de Información cimentado en la norma ISO 27001 para mejorar la disponibilidad, confidencialidad e integridad de la información en el espacio en estudio. Metodología; la investigación fue de tipo no experimental de diseño descriptico, de enfoque cuantitativo. Concluyó que se clasificaron las amenazas, vulnerabilidades y la estimación de los riesgos de acuerdo a los criterios de confidencialidad, disponibilidad e integridad, que se definieron las políticas y controles para reducir los riesgos de la confiabilidad e integridad de la información y la protección de los activos y los intereses del objeto de estudio, que se analizaron los riesgos, se identificaron las vulnerabilidades y amenazas que enfrentaron los activos de información del espacio estudiado.

Blas y Pretell (2020) en la tesis de grado denominada "Modelo de seguridad de la información para mejorar la gestión informática en la Municipalidad Distrital de Florencia de Mora" realizada en la Universidad Nacional de Trujillo. Perú. Se planteó como objetivo general realizar la mejora de la gestión informática de la Municipalidad Distrital de Florencia de Mora a través de la aplicación de un modelo de seguridad de la información

basado en la Norma ISO 27002:2013. Trabajó con una población y muestra de tamaño de 25 empleados de la municipalidad estudiada, el tipo de investigación fue no experimental, de diseño no descriptivo, como metodología aplicó la norma ISO 27002:2013. Resultados: se encontró problemas de administración y manejo de claves, de seguridad en las comunicaciones, y escaso control en la administración de la red en general. Concluyó que se logró controlar los accesos a los recursos informáticos con la finalidad de incrementar la disponibilidad de la información, definieron políticas de cifrado con fines de aumento de la integridad de la información, establecieron la seguridad física, en las operaciones y se definieron medidas para adquirir, desarrollar y dar mantenimiento al sistema de información edil, el correcto funcionamiento de los niveles de seguridad y su interacción con los usuarios.

Para el estudio, respecto a la variable se fundamenta científicamente, tomando bases teóricas:

Modelo de seguridad Informática

Se entiende a la seguridad informática como las medidas y controles que las autoridades de una organización establecen para el aseguramiento de los sistemas informáticos, impidiendo que intrusos internos o externos realicen ataques o procedimientos no autorizados sobre dicho sistema; de acuerdo con Corletti (2016), la adecuada la protección de las aplicaciones para evitar problemas de seguridad informática estas aplicaciones se deben de descargar en fuentes confiables y actualizarlas frecuentemente. Para mantener protegidos los datos, es necesario realizar constantemente copias de seguridad, el cifrado de la información, realizar un almacenamiento redundante de datos y deshabilitar componentes que supongan la entrada o salida de información no autorizada. Para evitar el robo de equipos se debe de cifrar los contenidos críticos, controlar o evitar los intentos de conexión de equipos externos no autorizados, y realizar mantenimientos preventivos.

Seguridad de la información

También es entendida cómo es el nivel de protección con el que se cuenta en un determinado tiempo en la red, para tener la capacidad de proteger los datos, archivos, software, hardware en general, frente a intrusos internos o externos que pretendan realizar acciones de monitoreo, modificación, intercepción y eliminación de la información, asimismo como contar con políticas, métodos, procedimientos de recuperación cuando se sufra alguna amenaza informática (CISCO, 2016).

Para mi investigación se tiene como Justificación de la investigación a lo siguiente: Se justifica socialmente debido a que la medida que el sistema de información de la Municipalidad Provincial de Yungay disponga de seguridad, los usuarios serán mejor atendidos ya que el sistema estará funcionando permanentemente. La seguridad del sistema de información va a beneficiar a los usuarios de la municipalidad quienes se van a atender en los diversos servicios que presta la institución edil; asimismo, se beneficia a los empleados ediles porque ellos conocerán diversos tipos de ataques a los que están expuestos estos tipos de instituciones, y estarán mejor preparados y concientizados respecto a la seguridad de todos los activos de importancia para la municipalidad, en ese sentido, la institución edil y su imagen estará más fortalecida, se evitarán secuestro de información, pérdidas de datos y se minimizarán los costos originados por los ataques informáticos**.**

Además, se justifica científicamente porque se fundamenta en teóricamente en los principios fundamentales de la ciencia computacional y la ciencia informática, específicamente en los principios de la seguridad informática, en los principios del Marco de Seguridad Basado en NIST SP 800 -30, en los principios de seguridad de informática. Se justifica técnicamente porque, el marco de seguridad basado en NIST SP – 800 – 30 va a guiar los procesos de asegurar la información de las licitaciones de obras, liquidaciones, de obras, pagos a proveedores, proyectos de inversión civil, entre otros documentos de alta confidencialidad para las autoridades ediles. Este marco de seguridad indicará las formas de cómo deben actuar los usuarios de tecnologías informáticas en la municipalidad respecto al uso de la

tecnología de la información y comunicación en la generación, registro, almacenamiento y distribución de las informaciones confidenciales.

La presente investigación es importante porque permitirá el apoyo en el nivel de protección de la información documentaria e información confidencial creados, distribuidos y almacenados en la institución en estudio. El trabajo de investigación adquiere relevancia, en tanto que los resultados permitirán, mejorar la protección de la información, guiando a los usuarios de las tecnologías informáticas en el cómo, cuándo y porque proteger la información.

Se justifica tecnológicamente porque se hará uso de normas orientadas hacia la seguridad de la información con la finalidad de contribuir en la mejora de la seguridad informática edil, asimismo, busca el cumplimiento de los verdaderos objetivos de la seguridad de la documentación física y lógica Las implicancias, prácticas de la presente investigación, permitirá, a los empleados ediles trabajar en equipo, elevar sus conocimientos sobre los temas de seguridad informática y también en la defensa sobre los ataques informáticos con la finalidad de garantizar la seguridad de la información edil.

Consideré como Problema de investigación, a lo siguiente: Primero mi Planteamiento del problema, donde se considera que a nivel internacional, las organizaciones ediles por ley tienen como función la gobernabilidad de sus espacios jurisdiccionales, se encargan de administrar un sector de la población, utilizan sistemas de información con diversos tipos de datos a los cuales debe proteger, estos datos, muchos de ellos son de vital importancia, en ese sentido, se hace necesario que las instituciones gubernamentales protejan los datos de agentes internos y externos, quienes, por diversos factores o motivos tratan de acceder a la información, ya sea para robar información, generar caos, o demostrar que ellos pueden acceder a cualquier tipo de sistema solo por orgullo o vanidad. Muchas municipalidades en el mundo han reportado que han sido hackeados por intrusos desde cualquier parte del mundo, para evitar estos tipos de ataques informáticos, estas instituciones han aplicado diversos métodos de seguridad informáticas, entre ellos las políticas de seguridad. Las municipalidades, a nivel internacional,

están expuestas a robo de información por medio de técnicas modernas de ataques informáticos, los cuales pueden ser ataques internos y externos, son vulnerables por estos tipos de ataques debido a que los empleados de las municipalidades solo utilizan la tecnología para resolver problemas del tipo operativos y administrativos, y si saben algo de seguridad informática, poco pueden hacer frente a los ataques por profesionales, quienes han dedicado años en la adquisición de diversas técnicas de ataques cada vez más modernas y efectivas; y que pertenecen generalmente a bandas u organizaciones criminales.

A nivel nacional, existen 196 municipalidades provinciales, 1655 municipalidades distritales, y 2534 municipalidades de Centros Poblados, lo que hace un total de 4385 municipalidades a nivel nacional (Instituto Nacional de Estadística e Informática, 2017). El 90% de los ataques cibernéticos en Perú son realizados por los mismos empleados de las empresas, de acuerdo con una encuesta realizada en el país y en otras 59 naciones a 1,825 organizaciones. Que el 80% de los encuestados manifestaron dice que no contaron con información actualizada sobre los riesgos o vulnerabilidades que podrían afectar a sus sistemas de información (RPP, 2015). En los ciberataques que llevan a cabo frecuentemente son ataques hombre en el medio, ataque de fuerza bruta, phishing y cryptojacking, etc., fueron las modalidades de delitos informáticos más frecuentes en el Perú durante el año 2019. Asimismo, Perú es un espacio muy especial para los hackers debido a que la mayoría de usuarios de la informática no saben usar software antivirus o procesos de seguridad informática, uno de los últimos rincones en donde aún no se han adoptado las nuevas tendencias de ciberseguridad, el riesgo es bastante alto, y que, al no invertir en seguridad, nos vuelve vulnerables y atractivos para el hacker que ya conoce cómo atacar rápidamente sistemas de seguridad de tecnología tradicional.

Las municipalidades provinciales son instituciones públicas que generan gran cantidad de información, un porcentaje considera de ellos (11.2%) son considerados de alta seguridad e importancia, y que solo las autoridades pertinentes deben tener la respectiva accesibilidad, esta información pueden

ser: Archivos de licitaciones públicas, archivos de proyectos de inversión pública, archivos de finanzas de proyectos urbanos y rurales, planilla de sueldo y salarios, proyectos o convenios realizados, contratos, archivos confidenciales de las gerencias generales de cada área, archivos confidenciales del Alcalde, etc. El problema es que todas las municipalidades, en mayor o menor dimensión, están expuestas a ataques informáticos para, precisamente, robar información importante, tales como, información de bases de licitaciones de proyectos obras, proyectos de infraestructura antes de ser licitadas, documentaciones consideradas confidenciales para las gerencias de las municipalidades, ordenanzas municipales, decretos de alcaldía, resoluciones de alcaldía, gerenciales y jefaturales, acuerdos municipales, convenios, adendas, documentos de oficina, cartas, correos electrónicos institucionales, etc.

A nivel local, la Municipalidad Provincial de Yungay está organizada jerárquicamente a través de la Alcaldía, Gerencia Municipal, Unidad de Administración tributaria y Rentas, Unidad de Administración y Finanzas, Unidad de Planeamiento y Presupuesto, Unidad de Infraestructura y Catastro, Unidad de Servicios Sociales, y la Unidad de Desarrollo Económico Local y Medio Ambiente. En todas estas unidades se elabora, reciben, y envían diversos tipos de información, siendo los más importantes, la información generada en cada una de las gerencias, así como en la Alcaldía.

El problema que se evidenció en esta municipalidad en estudio, es que no existe una política general de seguridad o marco de seguridad en el uso de las herramientas tecnológicas de la información y la comunicación, que permita a cada uno de los usuarios del sistema de información a que protejan adecuadamente los datos e información, específicamente, los de alto valor, importancia y confidencialidad. Esta realidad problemática está generando los siguientes problemas: Deficiencias en la protección de los archivos de licitaciones públicas con técnicas modernas, marcos de seguridad, o con recomendaciones de las normas internacionales de calidad en el uso de la tecnología informática. Falencias en la protección de archivos de proyectos de inversión pública, Vulnerabilidades en la protección de los archivos de

finanzas de proyectos urbanos y rurales, Negligencia en el cuidado y protección de los archivos de la planilla de sueldo y salarios, Deficiencias en la protección de los archivos de proyectos y convenios realizados, contratos. Falencias en la protección de los archivos confidenciales de las gerencias generales de cada área, archivos confidenciales del alcalde, archivos de acuerdo del alcalde con los Regidores, etc.

El problema muestra que, si en el corto y mediano plazo no se resuelve el problema, la Municipalidad Provincial de Yungay podría correr el riesgo de que los intrusos informáticos accedan a los archivos y puedan robarlos, modificarlos, venderlos, con los documentos de licitaciones públicas, las empresas podrían conocer los montos de las inversiones de los proyectos de construcción teniendo ventajas ilegales, creando caos, confusión, grandes pérdidas económicas y de imagen a la municipalidad, ante esta situación, se busca proponer un marco de seguridad basado en NIST SP 800 - 30 con la finalidad de mejorar la Protección de datos en la Municipalidad Provincial de Yungay, y se plantea el siguiente problema. Ante esta realidad problemática, la presente investigación propone un modelo de seguridad informática en los ataques informáticos en la Municipalidad Provincial de Yungay con la finalidad de prevenir los tres tipos de ataques informáticos. Se planteó como Formulación del Problema a lo siguiente: ¿Cómo elaborar un Modelo de Seguridad Informática basado en NIST SP 800 - 30 para proteger la información en la Municipalidad Provincial de Yungay, 2021?

Se consideraron conocimientos importantes para el desarrollo de la propuesta. En ese sentido, se conceptualiza y operacionaliza la variable de estudio.

NIST SP 800:30

Es un conjunto de normas que constituye un estándar y que ha sido elaborado por el Instituto Nacional de Estándares y Tecnología con la finalidad de que se pueda evaluar los riesgos de seguridad relacionados con la información que se genera con el uso de las nuevas tecnologías informáticas, esta norma presenta una guía y orientación para que usuarios de los sistemas

informáticos puedan generar seguridad al capital tecnológico con el cual trabaja, provee fundamentos administrativos enfocados hacia los riesgos su evaluación y la reducción de los riesgos que se puedan identificar en dicho sistema (Monteza, 2019; CERT, 2013).

La metodología NIST SP 800:30 se estructura en 9 etapas en donde se puede establecer el ámbito y las fronteras de operación de los aspectos de evaluación de riesgos para la institución, se identifican las amenazas mediante la definición de fuentes, se identifican las vulnerabilidades que puedan ser utilizadas por los atacantes, se analizan los controles se identifica la probabilidad de poder ser atacado, se analizan los impactos la determinación del riesgo como estos ayudan a evaluar el riesgo integral de todo el sistema además, se pueden realizar sugerencias sobre el control enfocados a la reducción de riesgo hasta que se pueda aceptar por toda la institución, finalmente se elabora la documentación en donde se describen los resultados sobre amenazas y vulnerabilidades, la aplicación de esta metodología sirve entonces para analizar los riesgos institucionales en función al uso de las tecnologías de la información, en ese sentido se debe tener en cuenta que cualquier organización debe ser consciente de la importancia de la seguridad informática debido a que dentro de ella se pueden configurar diversos tipos de ataques que podrían poner en riesgo la seguridad integral del sistema (ISO 27001; 2010; Lázaro,2008; Veritas, 2005).

Para que una empresa pueda desarrollar un cierto nivel de seguridad informática también debe desarrollar un cierto grado de conocimiento y habilidades para evitar cualquier tipo de ataque informático, y de esta manera proteger toda la documentación guardada dentro del sistema, esta capacidad le va a dar a la empresa un nivel de imagen, caso contrario le podría provocar considerables pérdidas económicas, en ese sentido es fundamental que las empresas cuenten con sistemas seguros que le permita hacer frente a cualquier tipo de amenazas y minimizar sus vulnerabilidades (Cisco, 2016; De Pablo, 2007).

Es necesario resaltar que NIST SP 800-30 presentan los siguientes objetivos: Trata de asegurar que cualquier tipo de sistema de información en donde se almacenan y se llevan a cabo procesamientos y transmisión de datos, se asegura y apoya decididamente en la gestión y análisis de los riesgos, en ese sentido trata de optimizar la gestión de riesgos en función a los resultados que se obtienen de un análisis riguroso de riesgos, otro objetivo es la protección de las capacidades

organizacionales en el logro de su misión, es decir que esta norma apoya también decididamente en la formación del personal respecto a la importancia de la seguridad informática (ISO/IEC 27001, 2018; Grijalva, 2018; Kawamoto, 2005).

Propósito de la norma NIST 800 – 30

Esta norma tiene como finalidad la de contribuir y de alcanzar una fundamentación en la ejecución de la gestión del riesgo, así como alcanzar información respecto a los controles de la seguridad informática relacionados con el giro del negocio; otro propósito de esta norma, es la de apoyo en la metodología de gestión de riesgos que cada organización debe adoptar, ayuda en la evaluación del riesgo en función a sus respectivas vulnerabilidad, esta norma señala que en la evaluación del riesgo se deben identificar las amenazas a las que está sujeto a la empresa; esto significa las operaciones, las actividades, la documentación en riesgo y los actores que puedan participar; las amenazas indica que pueden ser internas o externas, también ayuda en la identificación y cuantificación del daño ante un ataque potencial, así como puede ayudar en la identificación de la probabilidad con que el daño pueda ocurrir, como resultado último, consiste en la configuración del riesgo a lo que está sujeto la empresa.

Con la norma NIST SP 800-30, las evaluaciones de riesgos están sujetas a una gran cantidad de decisiones y de procesos fundamentados en el riesgo, y que cada analista en función de sus grados o jerarquías, puede llevar a cabo la gestión de riesgos tales como el desarrollo de una plataforma de seguridad de la información, en este caso se definen las necesidades de conexión de los

del sistema, se desarrollan los diseños de soluciones para garantizar la seguridad de información, así como también se configuran los ambientes en donde se van a realizar los procesos operativos, incluye la selección de cada 1 de los controles de seguridad las herramientas tecnológicas, quienes pueden proveer estas tecnologías y suministros. Esta metodología puede ser usada en los procesos de evaluación de sistemas de información que están interrelacionados al sistema más grande, es decir, la tecnología con que dispone cada área de la institución (Ortiz, 2015; ISO/IEC 27001,2010).

Proceso de análisis de riesgos

En los procesos de caracterización o de análisis de riesgo se desarrollan un conjunto de procesos, tales como, la caracterización de sistemas, cómo se identifican las amenazas y las vulnerabilidades, se realizan los controles, se establecen las probabilidades, se lleva a cabo el análisis de impacto la determinación de riesgo, se recomiendan los controles y se documentan los resultados (Ríos, 2014; Roa, 2014).

Caracterización de sistemas

En la caracterización de los sistemas se identifican los niveles de tecnología de hardware de software y el nivel de conocimientos del manware, así como también, se establece comunicación con los proveedores y en función a ello se establecen cierto nivel de criticidad con la finalidad de describir hasta qué nivel de riesgo está expuesto el sistema de información, así mismo, se identifica de qué manera o forma se está protegido frente a una determinada amenaza (Zauzich, 2016; Mel & Scarfone, 2007).

Identificación de las amenazas

En la sección de identificación de las amenazas de acuerdo a esta metodología se revisan los ataques históricos que haya podido tener la institución. Asimismo, también, se identifican los datos de otras instituciones como agencias de inteligencia quienes podrían alcanzar información sobre los probables ataques ocurridos a la institución (Javier, 2008).

Identificación de las vulnerabilidades

En la fase de identificación de vulnerabilidades, esta norma señala que se deben analizar los informes o documentación que hayan evaluado riesgos anteriores, tales como auditorías de seguridad informática, solicitudes de requerimientos de seguridad, pruebas de seguridad realizados, procesos de identificación de vulnerabilidades potenciales, etc. (Karina, 2013).

Análisis de controles

En la fase de análisis de controles esta norma señala que se deben de analizar los controles que se están desarrollando actualmente, así como también, a los controles que se hayan planificado y confeccionado, ello involucra control de la cantidad de recurso humano que accede al sistema de información cotidianamente, el registro de información confidencial que usa contraseñas, así como también la revisión adecuada de la operatividad del equipo informático (Sullivan, 2004).

Determinación de probabilidades

En la etapa de determinación de probabilidades consiste en el estudio motivacional frente a los ataques, es el espacio en donde se prueba la capacidad de la institución de hacer frente a las amenazas, se analizan la naturaleza o características de las habilidades de los controles, así como también, se elabora una tabla jerárquica de probabilidades de que se llegue a concretizar la amenaza en los niveles bajo, medio y alto (Álvarez, 2014).

Análisis de impacto (pérdida de integridad, disponibilidad y confidencialidad)

En la etapa de análisis de impactos estudia los costos que podría generar un eventual ataque informático al sistema esto abarca los costos de pérdida de integridad costos de disponibilidad y costos de confidencialidad, se analiza la valoración de criticidad de activos de los datos y su sensibilidad frente a un probable ataque informático.

Determinación del riesgo

Respecto a la determinación del riesgo, se determina la posibilidad de explotación de las amenazas, así como la magnitud del impacto de cada uno de ellos, se adecúan los controles existentes, así como también, los que están ya planificados, es en esta etapa en donde se determinan los niveles de riesgo a los que está expuesto el sistema informático, los cuales pueden ser bajo, medio y alto (Arotinco, 2017).

Recomendación de controles

En la fase de recomendación de controles se lleva acabo la revisión de las políticas que corresponden a la seguridad de la información y de la tecnología utilizada, lo cual implica revisión y actualización de software antivirus, el cambio de claves de manera periódica, la implementación de firewalls, así como, los aspectos punitivos o de sanciones al personal en caso de incumplimiento de las políticas o normas actuales (Areitio, 2008).

Documentación de resultados

En la documentación de resultados, se realizan todas las actividades de descripción de cada una de las etapas estudiadas, es la última fase en donde se elabora el informe que califica el nivel de riesgos y vulnerabilidades encontradas en el sistema de información (Bonilla & González,2012).

Fase de gestión de riesgos

Priorización de acciones. En la norma NIST SP 800-30, para la fase de gestión de riesgos, la primera actividad que realiza es la priorización de las acciones, la cual consiste, en que, a partir de los niveles de riesgo encontrados, se elabora el ranking de acciones, se evalúan las opciones se estudia la viabilidad así como su eficacia y eficiencia, como, la adecuación hacia el proceso de trabajo que se requiere para combatir los riesgos, se lleva a cabo un análisis de costo y de beneficios, en donde se estudia el impacto que podría tener su implementación o no implementación de cada uno de los controles propuestos, se analiza también los costos que implican la implementación de la norma, en ese sentido, la instalación de cualquier sistema de protección de

la seguridad, decisiones sobre cambios de contraseñas, de actualización de software antivirus, así como la asignación de actividades y responsabilidades al recurso humano, todas ellas constituyen las actividades de priorización de acciones (ISO/IEC 27001, 2018: Everett, 2011). Algunas medidas que se podrían adoptar en la priorización de las acciones son:

Prevención: Esta medida consiste en crear una especie de salvaguarda preventiva en el caso de que se reduzcan las probabilidades de que un ataque ocurra, en el caso de que esta prevención fallará y el ataque se concretice los daños podrían ser los mismos, para prevenir se requiere participación de los usuarios, la gestión de perfiles o privilegios, la organización de las capacidades, técnicas y métodos desarrollo de software, pruebas pre operativas y selección de las actividades (Daltabuit, et al, 2007).

Disuasión: Se considera como disuasión aquella actividad o actividades que puedan intimidar o permitir que ocurra aquí el atacante se abstenga, ello reduce las posibilidades de que cualquier tipo de ataque ocurra, no obstante, se considera que no tienen influencia en los futuros daños, para disuadir se puede poner claves complejas o con bastantes dígitos, personal de seguridad, aviso de castigo del delito, leyes qué castigan severamente a este tipo de delitos, etc. (DELOITTE, 2017).

Eliminación: La posibilidad de eliminar un incidente consiste en hacer frente a un ataque y reducirlo, se consideran como salvaguardas que se llevan a cabo antes de que el incidente o ataque se produzca, no obstante, no reducen o minimizan los daños, pero ello no implica que esta actividad no sea necesaria; para llevar a cabo esta actividad se pueden eliminar, cuentas estándar, cuenta sin contraseña o clave, servicios no necesarios, etc. (Sullivan, 2004).

Minimización del impacto / limitación del impacto

Consiste en minimizar o limitar el impacto del ataque hacia el sistema, ello se puede llevar a cabo mediante diferentes acciones que se originan como resultado del dominio de hacer frente a ataques informáticos, ello implica la desconexión de redes, detención de servicios, cumplimiento de normas y aplicar gestión de segurosde cobertura.

Corrección: Para minimizar el impacto de un ataque es necesario también realizar correcciones de vulnerabilidades o de riesgos encontrados se considera la corrección como una salvaguarda que se ejecuta después de que el accidente o ataque haya ocurrido en ese sentido esta acción implica la reducción de daños (Sullivan, 2004).

Recuperación: Otro proceso de minimización de impacto consiste en la recuperación del sistema o la recuperación de cualquier capital que haya sido atacado el proceso de recuperación es una salvaguarda que permite reducir probabilidades de incidentes y que minimizan los daños en cierto periodo de tiempo. las copias de seguridad son un ejemplo de recuperación (Ríos, 2014).

Monitorización: El proceso de monitorización consiste en visualizar el sistema de información y específicamente los puntos más vulnerables por dónde se puede hacer atacado este proceso permite detectar probables ataques en tiempo real en el caso de que este proceso se deje de ejecutar puede permitir que el personal pueda aprender del ataque ya que se está visualizando su forma de ataque (Carlini, 2016).

Detección: El proceso de detección consiste en desarrollar un conjunto de actividades que contribuyan a la detección del ataque hacia el sistema informático, en esta fase también se desarrolla un informe de lo que está ocurriendo, aunque este proceso generalmente no evita el ataque, pero si ayuda a qué el sistema de seguridad opere con medidas y técnicas que ayuden a enfrentar un probable ataque informático, con ellos estaría reduciendo significativamente los

daños hacia la institución, la instalación de un software antivirus, implementación de detectores de incendio corresponden a actividades de esta fase (Gómez, 2011).

Concientización: La concientización consiste en ejecutar un conjunto de tareas, en donde se busca, la formación y concientización del recurso humano que utiliza el sistema de información para que puedan formarse y validar la importancia de la seguridad antes, durante y después de la utilización del sistema de información; en este proceso se capacita para que el personal disponga de una cultura sostenible de la seguridad de la información, implica también que el recurso humano pueda adoptar conductas de eficiencia y eficacia frente a los ataques informáticos (Gómez,2011).

Administración: El proceso de administración es considerado como una salvaguarda enfocada con los elementos estructurales que tienen que ver con la seguridad del sistema, una pertinente y adecuada administración conlleva a que se reduzcan los riesgos las vulnerabilidades, se esté más fortalecido frente a los ataques informáticos y se reducen los costos que ello implica de manera integral. Una administración es garantía de seguridad para la institución siempre en cuando esta se desarrolle adecuadamente (McKinsey, Samandari & Simoes, 2006).

Implantación de controles seleccionados

Respecto a la implementación de controles seleccionados, en esta fase se evalúan los riesgos y los niveles de riesgo, los cuales consiste en el desarrollo de acciones previas análisis y control que se ha planificado controles previamente seleccionados, recurso humano, pertinente fecha de inicio de los controles, así como también la fecha de finalización y los requerimientos que implica (Moreira, 2019; Romero, 2018).

Seguridad Informática

A la seguridad informática se le comprende o conceptúa cómo un grupo de actividades que se tienen que llevar a cabo en el hardware y software para que estos sean seguros, se encarga de llevar a cabo los controles para que no se produzcan ataques desde adentro o desde afuera, la seguridad informática implica una adecuada administración de los riesgos y vulnerabilidades y de la seguridad en general, para ello tienen que llevar a cabo seguimientos y pruebas, así como cambios en el acceso al sistema por parte de los usuarios. La seguridad de la información es comprendida como una actividad tecnológica relativamente compleja y difícil de gestionar al 100% debido a que no existe seguridad absoluta. Llegar a un nivel de seguridad conlleva a desarrollar conocimientos, inversiones, y disponibilidad de tiempo para el análisis y operación de los ataques informáticos en el plano empresarial (Morales, 2006).

La seguridad de un sistema de información depende mucho de la seguridad que le imprima cada uno de los usuarios del sistema de información, en ese sentido se considera que la seguridad es la sumatoria de las seguridades con la que aporta cada usuario, por lo tanto, es necesario estudiar a cada uno de ellos por separado y de esta manera se estaría integrando la solución a los problemas de seguridad de manera integral. (Aguilera, 2010; Nichols, 2003).

Uno de los factores por lo que la seguridad informática puede verse afectada negativamente es el cambio organizacional, es decir el cambio de personal o la rotación del mismo. Se desconoce qué capacidad cuenta cada uno de ellos respectoa la seguridad, asimismo, ellos desconocen el sistema y las políticas inherentes a la empresa, por lo tanto, el cambio de personal puede afectar significativamente a todo lo que la empresa ha trabajado respecto a la seguridad (Corletti, 2016: Aguirre, 2006), En la actualidad los sistemas de información han sido estudiados de manera parcial respecto a su seguridad, en ciertas veces, han sido estudiados de forma integral; la recomendación es que se estudie todo el sistema con la finalidad de minimizar las vulnerabilidades y los riesgos que pudieran tener (Comer, 2015).

Características de la seguridad informática

Los usuarios en un sistema de información son los directos responsables de la seguridad informática por lo menos operativamente en ese sentido las empresas norman los procesos que ellos realizan, entre ellos está la seguridad, en ese sentido, se busca que cada usuario deba conocer los riesgos los ataques el software antivirus, así como también, debe conocer toda la infraestructura informática y el capital documentario que se produce en la institución, los usuarios están comprometidos en el trabajo en un determinado tiempo y cada uno de ellos en función a su jerarquía tienen una responsabilidad en la generación de documentación importante para la institución, por lo tanto, deben conocer los riesgos vulnerabilidades y ataques que pudieran sufrir en el uso de las nuevas tecnologías de la información (Montes, 2014, Villalon, 2004).

Tipos de seguridad

La Seguridad Lógica: Se considera como seguridad lógica a la situación restrictiva hacia el acceso de los programas y archivos de un sistema de información la cual se realizan mediante encriptación también hace referencia a la asignación de limitaciones a cada usuario también entendida como privilegios que se asignan para la realización de una determinada tarea (Comer, 2015). Consiste en aplicar mecanismos y barreras que mantienen con seguridad a la información de la institución, ciertos controles son utilizados para garantizar dicha seguridad (Montes, 2010), la seguridad lógica se limita a dar acceso a ciertos usuarios para que utilicen aplicaciones archivos programas mediante el ingreso con claves es un control de acceso hacia el sistema de la institución, para que cada usuario pueda realizar la tarea correspondiente (Borghello, 2011; Montes, 2010).

Seguridad Física: Se considera como seguridad física a la seguridad fáctica o real que tiene un sistema informático frente a las amenazas interna y externas, estas amenazas pueden ser generalmente debidos a la naturaleza, tales como, desastres naturales, inundaciones, incendios,

terremotos, etc., así como también, amenazas que pueden ocasionar los usuarios de manera involuntaria (Morales, 2006).

Riesgos informáticos

Los riesgos informáticos son considerados como posibilidades de que ocurra un accidente es decir es la incertidumbre real de la ocurrencia de una posible concretización de un suceso relacionado con la ocurrencia de un daño o accidente hacia los bienes capitales tecnológicos de una empresa, estos pueden ser daños a las computadoras, instalaciones de red, software, información, archivos de datos, etc. (Sullivan, 2004).

También se considera como riesgo informático al grado de probabilidad en que ocurra la concreción de un accidente o amenaza en donde se aproveche la parte débil o vulnerabilidad del sistema, la ocurrencia de los ataques hacia un sistema deinformación es considerado como de alto riesgo cuando la vulnerabilidad también es alta y viceversa (Aguilera, 2010. p. 14).

Amenazas lógicas: Una amenaza lógica es la capacidad o potencialidad que dispone un atacante que puede hacer daño hacia un sistema de información valiéndose de herramientas tecnológicas como hardware y software, específicamente material tecnológico que sirve para atacar sistemas de información, estos pueden ser gusanos virus, troyanos, etc. (Aguilera, 2010. p. 14).

Si era como amenaza hacia un sistema informático a la probabilidad o posibilidad de que éste sea atacado en función a sus grados de vulnerabilidad, en ese sentido, se hace necesario que se eviten estos tipos de ataques mediante la toma de conciencia y de la importancia que se le puede dar a la seguridad como mecanismo de prevención de ataques frente a las amenazas lógicas a las que está expuesta todo sistema de información (Borghello, 2011).

Vulnerabilidad: La vulnerabilidad es definida como un estado de debilidad de un sistema de información o una parte de ella, a las vulnerabilidades son puertas por donde ingresan los atacantes interno y

externo con la finalidad de poner en riesgo todo el capital informático de la institución, permite qué se pueda poner en peligro las características de confidencialidad, integridad, disponibilidad de la información (Mell & Scarfone, 2007).

Las vulnerabilidades de los sistemas de información son sucesos en dónde una cierta cantidad de usuarios pueden hacer uso debido o indebido de los recursos del sistema de información. Los riesgos que competen al software están en el diseño del programa y en los accesos que pueda presentar, Por otro lado, los usuarios pueden usar esta vulnerabilidad para poder hacer uso de los de los recursos sin autorización por lo tanto la facilidad de acceso hacia un sistema depende bastante de la seguridad de acceso (Allende & Gui, 2011).

Seguridad de los Sistemas Informáticos

Se define como seguridad de los sistemas informáticos a un conjunto de acciones debidamente planificadas y organizadas que van a conducir a garantizar un cierto grado o nivel de seguridad para dichos sistemas, también se le considera como un grupo de técnicas y procedimientos sí configuran un cierto nivel de eficiencia y eficacia en la generación de seguridad para dicho sistema (Ríos, 2014).

Seguridad de la información

Se define como seguridad de información al nivel o grado de dificultad con que los usuarios atacantes presentan en el momento de sus ataques hacia la información, la seguridad de información consiste en la protección de la documentación frente a ataques internos o externos haciendo uso de las tecnologías informáticas, también se le considera como una cantidad de procedimientos se ejecutan con la finalidad de gestionar y ejecutar procesos de seguridad que garanticen que la documentaciónno sea vulnerada (Montes, 2010).

Para CISCO (2016), la seguridad informática es el nivel de protección los activos físicos y lógicos de cualquier sistema de información, con el objetivo de asegurar y garantizar la protección de la información que significa valor

para la institución, así como también de los activos físicos, tales como, los datos, archivos, software, hardware en general, de los ataques internos o externos que intenten y concreticen dichos atacantes. Con el objetivo de garantizar seguridad, se desarrollan acciones de monitoreo, modificación, intercepción y eliminación de la información, implica también alcanzar políticas, métodos, procedimientos de recuperación en el sentido de que haya sido atacado.

Dimensiones de la seguridad de la información

Disponibilidad: La disponibilidad dentro de la seguridad informática hace referencia a que el sistema informático debe asignar y permitir acceso adecuado a los usuarios y debe negar a quienes no deban ingresar al sistema. Otras sub dimensiones son la prevención y la seguridad. Es la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento. Constantemente los clientes realizan diversas consultas en la página web de la Municipalidad Provincial de Yungay, por lo que siempre deben estar disponibles para los clientes (Borghello, 2011).

Accesibilidad: Se refiere a la capacidad con que el sistema informatice garantice el acceso a personas autorizadas a los procesos, servicios y datos del sistema informático (Corletti, 2016).

Prevención: Hace referencia a la integración de diferentes mecanismos que ayuden a evitar un ataque de denegación del servicio, es decir, el atacante evite que use tu propio sistema. Este ataque se produce por parte de terceras personas o entidades y provoca que el sistema de accesibilidad que se puso en marcha con anterioridad falle, es decir, que los usuarios legítimos no puedan acceder a los equipos o a información determinada (Corletti, 2016).

Seguridad: El acceso al servicio por parte de personas debidamente autorizadas deben estar aseguradas mediante uso de protocolos de seguridad determinados que dependerán de las necesidades de la empresa

y del profesional que los implemente, esto evita la entrada de intrusos al sistema (Corletti, 2016).

Integridad: Es la capacidad de garantizar que los datos no hayan sido modificados desde su creación sin autorización. La información en sus diversos formatos debe ser válida y consistente. Este objetivo es muy importante cuando se realizan trámites bancarios por Internet. Se deberá garantizar que ningún intruso pueda capturar y modificar los datos en tránsito (Ríos, 2014; Roa, 2013).

Confidencialidad: Se refiere a la capacidad del sistema informático de garantizar que la información almacenada o transmitida solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información. Si los archivos o información caen en agentes no autorizados, los verdaderos destinatarios no podrían acceder a la información o a su interpretación. Este es uno de los principales problemas a los que se enfrenta generalmente el sistema financiero; en los últimos años se ha incrementado el robo de cuentas de ahorros en sus diversos tipos con la consecuente pérdida de información confidencial, de clientes, líneas de negocio, etc. (Allende & Gui, 2011).

Autenticación: Es la capacidad del sistema informático que permite verificar que un documento pertenece a quién el documento así lo indica. Aplicada a la verificación de la identidad de un usuario, la autenticación se produce cuando el usuario puede aplicar algún modo de que se pueda verificar que dicha persona es quien dice ser. La autenticación en la informática se suele hacer con un usuario y contraseña (Boyles, 2010). A la parte que se identifica se le llama probador. A la parte que verifica la identidad se la llama verificador. Es habitual que el probador sea un usuario que quiere acceder a ciertos recursos y el verificador sea un sistema que protege el acceso a dichos recursos y tiene que verificar que el que accede sea un usuario que tiene permisos para acceder a esos recursos. Para poder tener autenticación es necesaria, como condición previa, la existencia de identidades unívocamente identificadas de tal forma que se permita su identificación (Borghello, 2001).

Fundamentos de los ataques informáticos

Los ataques de informáticos, en la actualidad, generalmente son realizados por correos electrónicos y las redes sociales. Estos atacantes envían millones de correos a listas obtenidas por el atacante de forma dolosa, utilizando diversas técnicas y herramientas informáticas para envío masivo de spam. Estos correos tienen un título inusual indicando algún tipo de urgencia, esta estrategia sirve para llamar la atención de la víctima y lograr que siga los pasos que indica el correo electrónico (Aguilera, 2010).

Los piratas informáticos utilizan ciertas fallas de diseño en los puertos SMTP, POP3 e IMAP, ellos envían correos engañosos usando estos puertos a destinos legítimos, para ello adicionan cierta cantidad de texto al mensaje, usan URL similar al nombre de la página legítima con código malicioso, en el caso de que el usuario no se da cuenta de este ataque se convierte en una víctima del ataque. La finalidad del envió de dicha URL reside en solicitar información de datos personales a la víctima, datosde tarjetas de crédito, entre otros tipos de datos (Ortigoza et al, 2019).

Basado en Páginas Web: Los ataques basados en páginas web se realizan mediante la inserción de código malicioso, así como también en este caso el atacante explota la vulnerabilidad que puede existir en el servidor web específicamente en su sistema operativo de red, y el atacante crea una página web similar a la original y le envía a la víctima, si la víctima utiliza la página engañosa, entonces involuntariamente está alcanzando toda la información que solicita el atacante (Nichosls, 2006). Los ataques basados en página web también pueden realizarse mediante la creación de publicidad falsa en internet, estos objetos son enviados al usuario, quien al interactuar con la página falsa otorga información a su atacante (Corletti, 2016).

Basados en Voz sobre IP: Otra forma de ataque a los sistemas de información consiste en los ataques fundamentados en la voz sobre el protocolo de internet también se le conoce como Vishing, en este caso el atacante permite que la víctima alcance información sensible Porque

generalmente este tipo de ataque está direccionado hacia las gerencias o autoridades de las instituciones (Corletti, 2016).

Basados en Mensajería Instantánea: Otra forma de ataque informático es la que se fundamenta en la mensajería instantánea, este ataque se configura cuando los usuarios intercambian mensajes de texto y de voz en tiempo real con diversos tipos de personas que interactúan en el sistema informático esto sucede cuando el usuario utiliza las redes sociales en general, estos programas de redes sociales son usados para diversos tipos de ataques permiten el intercambio de archivos vídeos imágenes direcciones electrónicas, los cuales ayudan a que los ataques vía web se realicen mediante mensajería instantánea, para ello utilizan un código malicioso y que se ejecuta generalmente sin la intervención del usuario, estos virus finalmente están diseñados para que extraiga información del sistema informático de la víctima (Montes, 2011).

Ataques de Cryptojacking: El cryptojacking Este tipo de ataques, cuya metodología se asemeja a la minería de criptomonedas, es bastante usado en la actualidad y constituye una amenaza emergente debido a que es un tipo de ataque oculto y que utiliza los dispositivos móviles como recurso para extraer diversos tipos de información, se aprovecha de los navegadores web, sobre todo de su falta de experiencia en la navegación web, así puede afectar a varios tipos de dispositivos, computadoras de escritorio laptops, smartphone, entre otro tipo de hardware, utiliza ataques maliciosos generalmente diseñado para permanecer oculto (Villalon, 2004).

Respecto a la Hipótesis General, esta Investigación tiene un alcance de carácter descriptivo, por lo que no se plantea una hipótesis, debido a que no se intenta correlacionar o explicar causalidad de variables y el objetivo a alcanzar está claro. Por tal razón se considera una hipótesis implícita.

Sobre los Objetivos, tenemos como Objetivo General: Proponer un Modelo de Seguridad Informática basado en NIST SP 800 - 30 para proteger la información en la Municipalidad Provincial de Yungay, 2021. Así mismo

se consideró como Objetivos Específicos: a) Diagnosticar el estado situacional de la seguridad informática en la Municipalidad Provincial de Yungay, 2021, b) Planificar las fases del Modelo de Seguridad Informática basado en NIST SP 800 – 30, c) Elaborar Modelo de Seguridad Informática basado en NIST SP 800 - 30 para proteger la información en la Municipalidad Provincial de Yungay, 2021.

II. METODOLOGÍA

El Tipo de investigación fue de tipo no experimental, porque no se tuvo que manipular la variable independiente para ver sus efectos en la variable problema, se hizo una presentación del funcionamiento del modelo de seguridad informática a los elementos de muestra (Hernández, Fernández y Baptista, 2010).

El Diseño fue descriptivo porque se tuvo que describir el estado situacional de la seguridad de la información de la municipalidad, así como, el posible impacto del modelo en la protección de la información de la institución edil. El diseño es el siguiente: G: O_1 X O_2

En donde G: es el grupo único que son los encuestados
O1 es la encuesta antes
O2 es la encuesta después
X es el marco de Seguridad NIST SP – 800

Se consideró como Población: de estudio a todos los trabajadores, que estuvo conformada por 28 trabajadores empleados de la Municipalidad Provincial de Yungay. Estos trabajadores trabajan cotidianamente con el sistema informático de la institución edil en estudio. P = 28.

Respecto a la Muestra estuvo conformada por la misma población de estudio, la cual está conformada por 28 trabajadores empleados de la Municipalidad Provincialde Yungay. M = 28

Para las Técnicas e instrumentos de investigación se aplicó la técnica de observación para el diagnóstico del sistema de información y la encuesta a los trabajadores que utilizan el sistema informático de la Municipalidad

Provincial de Yungay por única vez. El instrumento aplicado fue el cuestionario, y será aplicada a los elementos de la muestra de manera simultánea.

Tabla 1

Técnicas e instrumentos de recolección de datos

Técnicas	Instrumentos
Entrevistas	Guía de entrevista a personal especializado
Encuestas	Cuestionarios
Análisis documental	Textos, tesis, revistas y estudios previos

Para la Metodología de desarrollo, se trabajó la metodología del Marco de Seguridad basado en NIST SP-800, como metodología se aplica en las siguientes fases (ISO/IEC 27001, 2018):

Identificación: La fase de identificación consiste en identificar los activos de información de la institución edil, establecer los riesgos en la que se encuentran los diversos activos de la institución y las responsabilidades que se tiene por cada uno de los activos. en la identificación de los activos consiste en determinar la cantidad de hardware, la cantidad de software, y la cantidad de personal que está a cargo de toda esta tecnología. En la cantidad de los activos de información se cuantifica el software en función a tipos, ya sean de sistema operativo, de trabajo en la municipalidad, y de acceso a internet, así como también el software antivirus que utiliza el sistema. Respecto a los riesgos de los activos esta metodología aplica la identificación de los riesgos por cada área y por persona, para ello analiza los procesos que realizan cada uno de ellos y, cómo lo están utilizando en función a las normas establecidas. En las responsabilidades del activo se determina la responsabilidad de cada área y de cada usuario, todo ello, en función a la seguridad del sistema de información.

Protección: En la fase de protección, esta metodología aborda el tema sobre qué usuarios están usando los activos, también analiza los programas de seguridad las políticas de eliminación o enfrentamiento de ataques de forma segura, tiene en cuenta la capacitación en ciberseguridad, en la comprobación de riesgos personales y en la protección adecuada de los

datos. respecto a los usuarios del activo, esta metodología permite determinar cómo están protegiendo a los activos cada 1 de los usuarios del sistema, y respecto a los programas de seguridad, en esta fase se capacitan y se hace de conocimiento sobre el contenido integral de dicho programa a cada uno de los usuarios, respecto a las políticas de eliminación segura, esta metodología guía y orienta sobre la elaboración de políticas de seguridad en el uso de sistemas de información que cada usuario debe acceder y conocer, así como, aplicar en su trabajo cotidiano. Esta metodología también contempla en esta fase, de que los usuarios deben ser capacitados en ciberseguridad, esto es un aspecto fundamental, debido a quemuchos usuarios ediles desconocen los tipos de ataques y los riesgos a los que están expuestos cuando utilizan internet o las redes sociales. Respecto a la comprobación de riesgos personales, esta metodología analiza y estudia cada uno de los riesgos a los que está expuesto cada usuario del sistema de información, con la finalidad de establecer un nivel para cada uno de los riesgos, y así tomar decisiones adecuados,por último, en esta fase, también se analiza la Protección de Datos por parte de los usuarios del sistema de información, la cual consiste en la aplicación de las tecnologías anti ataques informáticos que se puedan configurar durante el desarrollo del trabajo dentro de la institución.

Detección: En la fase de detección esta metodología presenta tres sub fases, la primera hace referencia al acceso de personal no autorizado, luego al almacenamiento de datos, y por último a las actividades inusuales que se puedan presentar durante el uso del sistema de información. En la fase de acceso de personal no autorizado esta metodología propone un control de que todos aquellos usuarios que no cumplan con el perfil para el acceso a un determinado capital tecnológico de la institución no deben ingresar, su ingreso se considera como un acto inseguro y un acto punible, para ello, se lleva un control mediante el uso de claves complejas y de concientización al usuario sobre el uso dedichas claves. En la siguiente fase denominada almacenamiento de datos, la metodología contempla un conjunto de actividades seguras para que los usuarios puedan almacenar los datos específicamente datos de alto nivel de importancia para la

institución, para ello el usuario debe tener un acceso privilegiado para almacenar y crear copias de seguridad en el servidor del sistema de información, por último, en la fase actividades inusuales, se lleva un control de las actividades sospechosas, actividades que no corresponden a procesos normales, actividades complejas y que impliquen poner en riesgo la seguridad de todo el sistema de información.

Respuesta y recuperación: En la fase de respuesta y recuperación esta metodología contempla 6 sus fases, los cuales son: notificación a los usuarios, mantenimiento del funcionamiento de las operaciones ediles, realizar un reporte de ataques que hayan ocurrido, responder a los ataques, reparación y restauración de hardware y software y, por último, informar a los usuarios. En la etapa de notificación a los usuarios, a ellos se les alcanza un conjunto de respuestas sobre seguridad y ataques que pudieran ocurrir o que hayan ocurrido en tiempos históricos y, cómo estos ataques han sido enfrentados, así como también, como la información ha sido recuperada. En la etapa de mantenimiento del funcionamiento se llevan a cabo procesos de análisis y verificación de los procesos funcionales que desarrolla cada usuario en función a su labor. En la etapa de realizarun reporte de ataques, los usuarios tienen que llevar un control cada vez que se realiza un ataque interno o externo, en este caso se identifica la fecha, el tipo de ataque y el origen. En la etapa de responder a los ataques, los usuarios deben aplicartodos los conocimientos respecto al ataque ocurrido, ellos deben de hacer frente haciendo uso de sus conocimientos y las tecnologías de información, así como también, registrar los resultados en la etapa de reparación y restauración de hardware y software, los usuarios deben realizar un mantenimiento de estos dos componentes importantes del sistema con cierta periodicidad, generalmente cada seis meses para hardware, y mensualmente para software. En la fase de informar a los usuarios se elaboran documentaciones en donde se describen todo lo acontecido a esta etapa con la finalidad de tenerlos como datos históricos.

III. RESULTADOS

Se consideraron los Procesos o área a evaluar al área que fue evaluada, es decir la unidad Informática de la Municipalidad provincial de Yungay ubicada en la plaza de armas de la ciudad de Yungay. Los procesos que se evaluaron fueron:

- Distribución Red: Encargada del sistema de información del sistema de información de la institución edil.

- Áreas principales de la municipalidad, estas áreas son los siguientes: La red informática abarca las siguientes áreas: Alcaldía, Gerencia Municipal, Secretaría General, Procuraduría Pública, Gerencia de Asesoría Jurídica, Gerencia de Planificación y Presupuesto, Gerencia de Administración y Finanzas, Gerencia de Administración Tributaria y Rentas, Gerencia de Infraestructura y Desarrollo Local, Gerencia de Desarrollo Económico y Ambiental, Gerencia de Desarrollo Social, Oficina de Control Interno, Soporte técnico y Administración de Redes.

El responsable del área de la seguridad informática de esta importante institución edil está a cargo del Área de Informática, la Alcaldía y la Gerencia Municipal. Para el desarrollo de la metodología, se consideró la Aplicación de la Metodología NIST SP 800 30. La metodología del Marco de seguridad basado en NIST SP-800 implica el desarrollo de varias fases: Identificación de las amenazas, evaluación de las amenazas, Identificación de vulnerabilidades, análisis de controles, determinación de probabilidades, análisis del impacto, determinación del riesgo, recomendación de controles y la documentación de resultados

Identificación de amenazas: En esta fase se han identificado los elementos tecnológicos que dispone la institución edil, tales como hardware y software, las áreas involucradas, la información que desarrollan o gestionan, se han identificado las vulnerabilidades, riesgos y amenazas que se generan con el uso de las tecnologías de la información en cada una de las áreas más principales de la municipalidad.

Identificación de vulnerabilidades: Las vulnerabilidades identificadas en las áreas más principales de la municipalidad provincial de Yungay son las referidas a la información, es decir a la confidencialidad, integridad y disponibilidad; así como también, las diversas conductas que adoptan los usuarios de las computadoras en el uso de la documentación sensible de la institución edil, se ha identificado los niveles de uso del personal con referencia al sistema de información, la existencia de software de protección antivirus, la disponibilidad de políticas de restricciones hacia uso del sistema y acceso a la documentación hacia el personal.

Análisis de controles: En esta fase se han analizado los controles sobre la cantidad de usuarios de computadora por cada área de la municipalidad que tiene acceso al equipo en donde se maneja y almacena información privilegiada e información sensible, así como también el manejo del perfil y contraseñas de cada uno de los usuarios.

Determinación de probabilidades. Para la determinación de las probabilidades de la ocurrencia de ataques, las motivaciones que generan dichos ataques, así como la capacidad de amenazas y la naturaleza de la vulnerabilidad se ha elaborado una tabla de probabilidades de que pueda ocurrir la amenaza.

Análisis del impacto. Para la fase de análisis del impacto se ha evaluado el riesgo real, sí han alcanzado informaciones y recomendaciones de control sobre todo en el uso de la información de importancia para la municipalidad con la finalidad de que se pueda reducir los riesgos hasta un nivel bastante aceptable.

Determinación del riesgo. En la fase de determinación del riesgo se ha realizado la adecuación de los controles actuales y se han realizado las planificaciones sobre el manejo de la información en función de la integridad, disponibilidad y confidencialidad. También se ha identificado el nivel del riesgo en el uso de la información y de la tecnología informática.

Recomendación de controles. En la fase de recomendación de los controles se ha realizado la recomendación de las revisiones periódicas de las políticas de seguridad de la municipalidad, sobre la importancia de las actualizaciones periódicas del antivirus, del cambio frecuente y seguro de las contraseñas y de una adecuada adopción del perfil de usuario, así como también las recomendaciones sobre instalaciones de hardware de protección ante ataques informáticos tanto internos como externos y que son utilizados con el uso de internet.

Documentación de resultados: En esta última fase se recomienda a la municipalidad la realización en los procesos y actividades con la finalidad de mejorar la seguridad de la información, así como también, que cada uno de los elementos de la institución edil deben valorar continuamente los riesgos y vulnerabilidades generados con el uso de la tecnología.

Estadística de resultados

Respuesta a objetivo específico 1: Diagnosticar el estado situacional de la seguridad informática en la Municipalidad Provincial de Yungay, 2021. El proceso realizado con los datos se encuentra en el anexo.

Estado situacional de la información respecto a la confidencialidad

Tabla 2

Estado situacional de la confidencialidad de la información

y1=mi	f1	y1f1	y21	y21f1
5	13	65.0	25.0	325.0
11	6	66.0	121.0	726.0
14	5	70.0	196.0	980.0
17	3	51.0	289.0	867.0
19	1	19.0	361.0	361.0
Sumas	**28**	**271.0**	**992**	**3259.0**

Fuente: Instrumentos

Cálculo de la varianza

$$S_1^2 = \sqrt{\frac{\sum y_1^2 f_1 - \frac{(\sum y_1 f_1)^2}{n}}{n-1}} = \sqrt{\frac{3259.0 - \frac{(271.0)^2}{28}}{27}} = 4.854$$

Cálculo de la media

$$\bar{x}_1 = \frac{\sum y_1 f_1}{n} = \frac{271.0}{28} = 9.68$$

El estado situacional de la información respecto a confidencialidad en la Municipalidad Provincial de Yungay es 9.68, lo que indica que es malo con una varianza de 4.854

Estado situacional de la información respecto a la integridad

Tabla 3

Estado situacional de la integridad de la información

y1=mi	f1	y1f1	y21	y21f1
5	10	50.0	25.0	250.0
11	9	99.0	121.0	1089.0
14	5	70.0	196.0	980.0
17	2	34.0	289.0	578.0
19	2	38.0	361.0	722.0
Sumas	**28**	**291.0**	**992.0**	**3619.0**

Fuente: Instrumentos

Cálculo de la varianza

$$S_1^2 = \sqrt{\frac{\sum y_1^2 f_1 - \frac{(\sum y_1 f_1)^2}{n}}{n-1}} = \sqrt{\frac{3619.0 - \frac{(291.0)^2}{28}}{27}} = 4.693$$

Cálculo de la media

$$\bar{x}_1 = \frac{\sum y_1 f_1}{n} = \frac{291.0}{28} = 10.39$$

El estado situacional de la información respecto a integridad en la Municipalidad Provincial de Yungay es 10.39, lo que indica que es malo con una varianza de 4.693

Estado situacional de la información respecto a la disponibilidad

Tabla 4

Estado situacional de la disponibilidad de la información

y1=mi	f1	y1f1	y21	y21f1
5	10	50.0	25.0	250.0
11	7	77.0	121.0	847.0
14	6	84.0	196.0	1176.0
17	3	51.0	289.0	867.0
19	2	38.0	361.0	722.0
Sumas	**28**	**300.0**	**992.0**	**3862.0**

Fuente: Instrumentos

Cálculo de la varianza

$$S_1^2 = \sqrt{\frac{\sum y_1^2 f_1 - \frac{(\sum y_1 f_1)^2}{n}}{n-1}} = \sqrt{\frac{3862.0 - \frac{(300.0)^2}{28}}{27}} = 4.693$$

Cálculo de la media

$$\bar{x}_1 = \frac{\sum y_1 f_1}{n} = \frac{300.0}{28} = 10.71$$

El estado situacional de la información respecto a la disponibilidad en la Municipalidad Provincial de Yungay es 10.71 lo que indica que es malo con una varianza de 4.693

Tabla 5

Promedio del estado situacional de la información

y1=mi	f1	y1f1	y21	y21f1
5	11	55.0	25.0	275.0
11	7	77.0	121.0	847.0
14	5	70.0	196.0	980.0
17	3	51.0	289.0	867.0
19	2	38.0	361.0	722.0
Sumas	**28**	**291.0**	**992.0**	**3691.0**

Fuente: Instrumentos

Cálculo de la varianza

$$S_1^2 = \sqrt{\frac{\sum y_1^2 f_1 - \frac{(\sum y_1 f_1)^2}{n}}{n-1}} = \sqrt{\frac{38691.0 - \frac{(291.0)^2}{28}}{27}} = 4.969$$

Cálculo de la media

$$\bar{x}_1 = \frac{\sum y_1 f_1}{n} = \frac{300.0}{28} = 10.71$$

El estado situacional de la información en general en la Municipalidad Provincial de Yungay es 10.39 lo que indica que es malo con una varianza de 4.969.

Respuesta a objetivo específico 2: Planificar las fases del Modelo de Seguridad Informática basado en NIST SP 800 – 30

Planificación de las fases del modelo de seguridad informática

Identificación de vulnerabilidades: En esta fase se han identificado los activos de información de la institución edil en las siguientes áreas:

Tabla 6

Cantidad de documentación importante por áreas

N°	Área	Cantidad de Documento Importante
01	Alcaldía	25
02	Gerencia Municipal	18
03	Gerencia de Planificación y Presupuesto	20
04	Gerencia de Administración y Finanzas	16
05	Gerencia de Administración Tributaria y Rentas	12
06	Gerencia de Infraestructura y Desarrollo Local	13
07	Gerencia de Desarrollo Económico y Ambiental	14
08	Gerencia de Desarrollo Social, Oficina de Control Interno	9
09	Secretaría General	6
10	Procuraduría Pública	10
11	Gerencia de Asesoría Jurídica	7
	Total	125

En total se han identificado 125 documentos en formato digital y muchos de ellos en formato impreso, todos ellos muy importantes para la municipalidad y que deben ser protegidos, sobre todo los que se encuentran en formato digital. Los responsables son las gerencias de cada área. La identificación de la cantidad de hardware y software se dan en la siguiente tabla:

Tabla 7

Cantidad de Hardware

N°	ÁREA	Hardware
01	Alcaldía	04
02	Gerencia Municipal	04
03	Gerencia de Planificación y Presupuesto	04
04	Gerencia de Administración y Finanzas	06
05	Gerencia de Administración Tributaria y Rentas	06
06	Gerencia de Infraestructura y Desarrollo Local	06
07	Gerencia de Desarrollo Económico y Ambiental	05
08	Gerencia de Desarrollo Social, Oficina de Control Interno	05
09	Secretaría General	02
10	Procuraduría Pública	03
11	Gerencia de Asesoría Jurídica	02
	TOTAL	47

La cantidad de hardware que existe en la municipalidad de 47, están contabilizados las computadoras de escritorio e impresoras. En la cantidad de los activos de información se cuantifica el software en función a tipos, ya sean de sistema operativo, de trabajo en la municipalidad, y de acceso a internet, así como también el software antivirus que utiliza el sistema. Respecto a los riesgos de los activos esta metodología aplica la identificación de los riesgos por cada área y por persona, para ello analiza los procesos que realizan cada uno de ellos y, cómo lo están utilizando en función a las normas establecidas. En las responsabilidades del activo se determina la responsabilidad de cada área y de cada usuario, todo ello, en función a la seguridad del sistema de información. Se identificaron los siguientes elementos de hardware de la municipalidad, la siguiente tabla contiene los elementos de hardware identificados:

Tabla 8

Elementos de hardware.

Hardware	Cantidad	Estado	Foto
Servidor HP Proliant MI350G10	01	Bueno. Es la parte central de la red cuya topología es de tipo Estrella. Es responsable del área de Informática. Contiene todo el software necesario. Nivel de seguridad: medio alto,	
Computadoras clientes HP	35	Bueno. Se encentra en período de vida de 1año.Nivel de seguridad: Medio. Lo disponen todas las áreas de la municipalidad	
Laptops HP	10	Bueno. Se encentra en período de vida de 1 año. Nivel de seguridad: Medio, está distribuidoen 7 áreas de la municipalidad	
Impresora Multifuncional HP Láser M528dn Red	01	Bueno. Se encuentra en período de vida de 02 años. Nivel de seguridad: Medio alto. La impresora se encuentra conectada la red y permite la impresión a todas las áreas	
Router Cisco 880 Series 5 Ethernet Lan (rj-45) C881-		Router Cisco 880 Series 5 Ethernet Lan (rj-45) C881-	

Fuente: Municipalidad de Yungay

Identificación de amenazas: Se encontró que la municipalidad provincial dispone de un plan de seguridad y gestión de riesgos, pero que no hace uso de las normas internacionales, que las conexiones al sistema eléctrico son los adecuados, pero se ha identificado la presencia de cables en el piso y paredes.

En el caso de que se detecte una ocurrencia de un incidente de seguridad a hardware,software o documentación, no siempre comunica al jefe de dicha área, en casos de un ataque de robo de información, los usuarios casi siempre avisan a los responsables de la seguridad informática. Los problemas u errores

encontrados en los procesos de información en todas las unidades de la municipalidad son reportados en un 56.2%. El acceso a sitios no recomendados de internet por parte de los usuarios, así como a las redes sociales y correos han generado que se generen y ocurran riesgos de ataques de diversas formas al sistema de información de la Municipalidad Provincial. El acceso a redes sociales se encuentra normado, no obstante, los usuarios lo usan en horas laborales inherentes a sus funciones, se utilizan para enviar mensajes a los usuarios de la municipalidad, proveedores, mensajes entre compañeros de trabajo, mensajes entre trabajador y administrativo, etc.

Aunque se han implementado controles en ciertos procesos de seguridad informática, control al personal, controlar ciertos documentos y activos ediles, el riesgo de seguridad está latente. Todos los procesos comunicacionales e intercambios de información, tanto dentro de las instalaciones y sistemas de la Municipalidad Provincial, así como externas a ella, se han tratado de asegurarlas en función de la importancia y valía de la información protegida, sobre todo los documentos confidenciales de la municipalidad, pero se evidencia problemas de seguridad en el cuidado de la información documentaria a nivel digital e incluso físico.

La longitud de contraseñas utilizadas por los usuarios de la municipalidad tiene un promedio de 9 caracteres, hacen uso de combinación de caracteres, y se cumple en un 91%, El problema que se presenta como riesgo es que el cambio de contraseña se realiza con una frecuencia muy larga cuyo promedio es de 6 meses, un 7% de los usuarios no cambian en ese periodo. todos los usuarios usan contraseñas, específicamente, los usuarios que trabajan con información sensible para la municipalidad.

Se ha podido evidenciar que el sistema de información utilizado en las áreas en la municipalidad el acceso restringido se cumple moderadamente, lo cual está poniendo en riesgo la integridad, la accesibilidad o disponibilidad, así como la confidencialidad de la documentación importante que se generan en cada una de las áreas ediles.

También se ha podido evidenciar que no todos los usuarios disponen del mismo nivel de uso del sistema de información, unos son más expertos que otros, sobre todo, frente a los ataques que el sistema pueda sufrir.

Los programas de computadoras que dispone la municipalidad son los siguientes: Windows 10, Suite Ofimática Office 2016 (Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Access), antivirus ESET NOD32, Software CAD,Software de Internet, de redes sociales, etc.

Identificación de vulnerabilidades: Se han identificado los siguientes riesgos y vulnerabilidades:

Tabla 9

Identificación de vulnerabilidades

N°	Riesgos y amenazas	Cantidad	Nivel
01	Personal con falta de capacitación de seguridad	03	Medio
02	Manejo de perfiles de usuario	05	bajo
03	Manejo de contraseñas	04	Medio
04	Conocimiento de importancia de información	04	Medio
05	Accesos a páginas de Internet indebidas	06	Alto
06	Actualización escasa de software antivirus	01	Medio
07	Accesos no controlados a redes sociales	05	Leve
08	Uso inadecuado de correo electrónico	04	Alto
09	Nivel de seguridad de hardware	06	Medio
10	Nivel de seguridad de software	04	Leve
11	Conocimiento de las políticas de seguridad	07	Leve
12	Capacitación al personal en seguridad	05	Medio
13	Riesgo de la integridad de la información	04	Medio
14	Riesgo de la disponibilidad de la información	04	Medio
15	Riesgo de la confidencialidad de la información	04	Medio

Análisis de controles: En esta fase de análisis de controles, se ha Evidenciado que la Municipalidad Provincial de Yungay, actualmente está desarrollando el control de manera limitada y con ciertas deficiencias al personal, software y hardware. Así mismo, también se ha planificado el control del personal en función a sus respectivos procesos, al software en la dimensión de seguridad, al hardware, también en función de seguridad, a las políticas de seguridad, y al control de la información en sus dimensiones de confidencialidad, integridad y disponibilidad.

Los Controles actuales son los siguientes:

Tabla 10

Controles actuales

N°	Control	Procesos
01	Control de Personal	Capacitación en seguridad
		Manejo de perfiles de usuario
		Manejo de contraseñas
		Conocimiento de importancia de información
		Accesos a páginas de Internet indebidas
02	Control de Software	Actualización de software antivirus
		Accesos controlados a redes sociales
		Uso de correo electrónico
		Nivel de seguridad de software
03	Control de Hardware	Nivel de seguridad de hardware
		Mantenimiento y actualización de hardware

Los Controles planificados son los siguientes:

Tabla 11

Controles planificados

N°	Control	Procesos
01	Control de Personal	Capacitación en seguridad
		Manejo de perfiles de usuario
		Manejo de contraseñas
		Conocimiento de importancia de información
		Accesos a páginas de Internet indebida
02	Control de Software	Actualización de software antivirus
		Accesos controlados a redes sociales
		Uso de correo electrónico
		Nivel de seguridad de software
03	Control de Hardware	Nivel de seguridad de hardware
		Mantenimiento y actualización de hardware
04	Políticas de Seguridad	Conocimiento de las políticas de seguridad
		Cumplimiento de las políticas de seguridad
05	Control de Información	Riesgo de la integridad de la información
		Riesgo de la disponibilidad de la información
		Riesgo de la confidencialidad de la información

Determinación de probabilidades. En esta fase se han determinado las motivaciones para los ataques, las capacidades de las amenazas de los atacantes son considerado medio o moderado, la naturaleza de las vulnerabilidades también es moderado, estos han sido identificados en el objetivo específico anterior. Las probabilidades sobre las motivaciones para los ataques, capacidad de las amenazas, naturaleza de las vulnerabilidades son las siguientes:

Tabla 12

Determinación de probabilidades

N°	Atacante	Motivación	Probabilidad de ataques
01	Proveedor	Conocer a la empresa proveedora de la competencia	0.18
		Conocer los precios	0.12
		Conocer fortalezas, debilidades, oportunidades y amenazas	0.10
		Conocer los productos y servicios	0.15
		Otros	0.12
02	Empresa licitadora y otros	Acceso a información	0.15
		Accesos a datos de redes sociales	0.25
		Acceso a datos de correo electrónico	0.20
		Nivel de seguridad de software	0.15
		Acceso a información	0.30
		Conocimiento de las políticas de seguridad	0.10
		Cumplimiento de las políticas de seguridad	0.10
		Alterar la integridad de la información	0.15
		Acceder a la disponibilidad de la información	0.25
		Acceder a datos confidenciales de la información	0.20

Se ha podido evidenciar que las probabilidades de ataques en función a las motivaciones y capacidades de está aquí son generadas probablemente por los proveedores y las empresas que licita un determinado proyecto de construcción social, tienes interés en conocer los documentos de licitación de obra públicas, con la finalidad de obtener ventajas de conocimiento sobre el monto del proyecto y de esta manera ganar la licitación, la cual es un método fraudulento y que no se ajusta algo normativas del Estado peruano.

Tabla 13

Ranking de probabilidades

N°	Motivación	Atacante	Probabilidad de ataques
1	Acceso a información	Empresa licitadora y otros	0.30
2	Accesos a datos de redessociales	Empresa licitadora y otros	0.25
3	Acceder a la disponibilidadde la información	Empresa licitadora y otros	0.25
4	Acceso a datos de correoelectrónico	Empresa licitadora y otros	0.20
5	Acceder a datos confidenciales de lainformación	Empresa licitadora y otros	0.20
6	Conocer a la empresa proveedora de la competencia	Proveedor	0.18
7	Conocer los productos yservicios	Proveedor	0.15
8	Acceso a información	Empresa licitadora y otros	0.15
9	Nivel de seguridad de software	Empresa licitadora y otros	0.15
10	Alterar la integridad de la información	Empresa licitadora y otros	0.15
11	Conocer los precios	Proveedor	0.12
12	Otros	Proveedor	0.12
13	Conocer fortalezas, debilidades, oportunidades y amenazas	Proveedor	0.10
14	Conocimiento de las políticas de seguridad	Empresa Licitadora y otros	0.10
15	Cumplimiento de las políticas de seguridad	Empresa Licitadora y otros	0.10

Análisis del impacto. En la fase de análisis del impacto se ha evaluado el riesgo real que puede afectar al sistema de información de la municipalidad, asimismo se han establecido las recomendaciones de control, en donde se alcance e identifique los controles que podrían minimizar el riesgo identificado reduciéndolo hasta un nivel considerable o aceptable.

Tabla 14

Análisis de impacto

N°	Riesgos y amenazas	Impacto	Control
01	Personal con falta de capacitación de seguridad	Incremento de la vulnerabilidad en el uso de los sistemas de información	Realizar programa de capacitación en seguridad
02	Manejo de perfiles de usuario	Posibilidad de hackeo interno y externo	Perfeccionar los perfiles de usuario
03	Manejo de contraseñas	Incremento de la vulnerabilidad en el uso de los sistemas de información	Realizar programa de capacitación en seguridad
04	Conocimiento de importancia de información	Incrementa el cuidado de la información	Concientizar sobre la importancia de la información
05	Accesos a páginas de Internet indebidas	Incrementa riesgos de ataques externos	Mejorar el control de este tipo de acceso
06	Actualización escasa de software antivirus	Incrementa riesgos de ataques externos e internos	Actualizarlo mensualmente
07	Accesos no controlados a redes sociales	Incrementa riesgos de ataques externos	Mejorar el control de este tipo de acceso
08	Uso inadecuado de correo electrónico	Incrementa riesgos de ataques externos	Mejorar el control de este tipo de acceso
09	Nivel de seguridad de hardware	Incrementa riesgos de ataques externos	Mejorar el control de este tipo de acceso
10	Nivel de seguridad de software	Incrementa riesgos de ataques externos	Mejorar el control de este tipo de acceso
11	Conocimiento de las políticas de seguridad	Incrementa el cuidado de la información	Concientizar sobre la importancia de la información
12	Capacitación al personal en seguridad	Incrementa las capacidades para hacer frentes a ataques	Programar las capacitaciones enfocadas hacia la seguridad
13	Riesgo de la integridad de la información	Pérdida, robo y secuestro de información	Aplicar las políticas de seguridad
14	Riesgo de la disponibilidad de la información	Pérdida, robo y secuestro de información	Aplicar las políticas de seguridad
15	Riesgo de la confidencialidad de la información	Pérdida, robo y secuestro de información	Aplicar las políticas de seguridad

Determinación del riesgo. Para la fase de determinación del riesgo se ha tenido en cuenta las probabilidades de riesgos que se han identificado con la finalidad de explotar las amenazas, la magnitud de los impactos, realizar mejoras en los controles actuales y planificados, así como también, con los análisis encontrados se han establecido el nivel de riesgo que se ha encontrado en la Municipalidad Provincial de Yungay, la cual ha sido un riesgo medio o moderado.

Tabla 15

Análisis de impacto

N°	Riesgos y amenazas	Impacto	Probabilidad de riesgo
01	Personal con falta de capacitación de seguridad	Incremento de la vulnerabilidad en el uso de los sistemas de información	Medio
02	Manejo de perfiles de usuario	Posibilidad de hackeo interno y externo	bajo
03	Manejo de contraseñas	Incremento de la vulnerabilidad en el uso de los sistemas de información	Medio
04	Conocimiento de importancia de información	Incrementa el cuidado de la información	Medio
05	Accesos a páginas de Internet indebidas	Incrementa riesgos de ataques externos	Alto
06	Actualización escasa de software antivirus	Incrementa riesgos de ataques externos e internos	Medio
07	Accesos no controlados a redes sociales	Incrementa riesgos de ataques externos	Leve
08	Uso inadecuado de correo electrónico	Incrementa riesgos de ataques externos	Alto
09	Nivel de seguridad de hardware	Incrementa riesgos de ataques externos	Medio
10	Nivel de seguridad de software	Incrementa riesgos de ataques externos	Leve
11	Conocimiento de las políticas de seguridad	Incrementa el cuidado de la información	Leve
12	Capacitación al personal en seguridad	Incrementa las capacidades para hacer frentes a ataques	Medio
13	Riesgo de la integridad de la información	Pérdida, robo y secuestro de información	Medio
14	Riesgo de la disponibilidad de la información	Pérdida, robo y secuestro de información	Medio
15	Riesgo de la confidencialidad de la información	Pérdida, robo y secuestro de información	Medio

Recomendación de controles. De acuerdo con el método NIST, en la fase de recomendación de controles, sea recomendado desarrollar análisis y revisiones de las políticas de seguridad, sobre todo en los niveles de hardware, software, personal y en las políticas de seguridad de la institución.

Tabla 16

Recomendación de controles

N°	Riesgos y amenazas	Control
01	Personal con falta de capacitación de seguridad	Realizar programa de capacitación en seguridad
02	Manejo de perfiles de usuario	Perfeccionar los perfiles de usuario
03	Manejo de contraseñas	Realizar programa de capacitación en seguridad
04	Conocimiento de importancia de información	Concientizar sobre la importancia de la información
05	Accesos a páginas de Internet indebidas	Mejorar el control de este tipo de acceso
06	Actualización escasa de software antivirus	Actualizarlo mensualmente
07	Accesos no controlados a redes sociales	Mejorar el control de este tipo de acceso
08	Uso inadecuado de correo electrónico	Mejorar el control de este tipo de acceso
09	Nivel de seguridad de hardware	Mejorar el control de este tipo de acceso
10	Nivel de seguridad de software	Mejorar el control de este tipo de acceso
11	Conocimiento de las políticas de seguridad	Concientizar sobre la importancia de la información
12	Capacitación al personal en seguridad	Programar las capacitaciones enfocadas hacia la seguridad
13	Riesgo de la integridad de la información	Aplicar las políticas de seguridad
14	Riesgo de la disponibilidad de la información	Aplicar las políticas de seguridad

Documentación de resultados: En la última fase que corresponde a la documentación de resultados, se ha alcanzado la información sobre los riesgos y sus respectivos niveles encontrados, con sus respectivas valoraciones.

Tabla 17

Niveles de riesgos en cantidad y porcentajes

Niveles de riesgos	Cantidad	%
Bajo	4	26.7
Medio	9	60.0
Alto	2	13.3
TOTAL	**15**	**100.0**

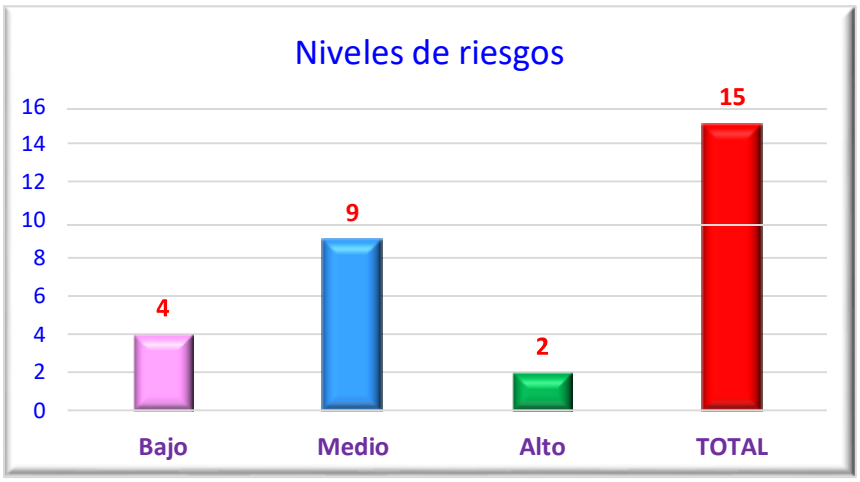


Figura 1. Niveles de riesgos

Se han encontrado 4 riesgos con nivel bajo, 9 riesgos con nivel medio o moderado,y 2 riesgos de tipo alto, en total se han encontrado 15 riesgos en el uso del sistema de información en la Municipalidad provincial de Yungay.

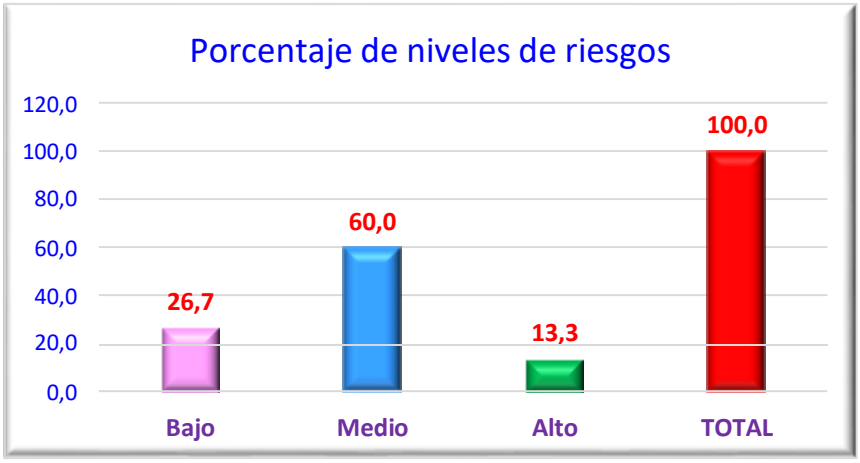


Figura 2. Niveles de riesgos en porcentajes

Se han encontrado 26.7% de riesgos con nivel bajo, 60.0% de riesgos con nivel medio o moderado, y 13.3% de riesgos de tipo alto, en total se han encontrado 15 riesgos en el uso del sistema de información en la Municipalidad Provincial de Yungay.

Respuesta a objetivo específico 3

Elaborar Modelo de Seguridad Informática basado en NIST SP 800 – 30.

El modelo de Seguridad Informática basado en NIST SP 800 – 30 se encuentra en anexos, y ha sido desarrollado teniendo en cuenta las fases y riesgos encontrados enel sistema de información de la Municipalidad provincial de Yungay

Respuesta a objetivo general

Proponer un Modelo de Seguridad Informática basado en NIST SP 800 - 30 para proteger la información en la Municipalidad Provincial de Yungay, 2021

La propuesta del Modelo de Seguridad Informática basado en NIST SP 800 – 30 va a contribuir a que cada uno de los usuarios tomen conciencia de la seguridad informática y se mejore la protección de la información desde las dimensiones de confidencialidad, integridad y disponibilidad.

IV. ANÁLISIS Y DISCUSIÓN

Medina (2017) concluyó que los objetos estudiados fueron atacados por diversas técnicas de malware, que la ejecución del ransomware modificaba los archivos, que uno de los aportes fue la profundización del funcionamiento de las distintas versiones de ransomware del tipo cifrador y donde se determinó un patrón de funcionamiento muy similar. Que se descubrieron propagación del virus por la red. En general el estado situacional de las instituciones financieras fue bueno, pero que fueron atacados esporádicamente. Este Proyecto coincide con nuestra investigación en la parte de la Seguridad Informática, relacionado con la propagación de virus en la red, para la protección de datos.

Jara (2018) encontró como resultados: el nivel de riesgo encontrado antes fue de 9.96, mientras que en el después fue de 5.90. Los controles fueron aplicados en el pretest con 92.1% y en el postest con 99.1%. Concluyó que la implementación del sistema de Gestión de Seguridad de la Información influyó en el proceso de gestión, que también influyó positivamente en la evaluación del riesgo en el proceso de gestión del riesgo, y que también influyó en el tratamiento del riesgo en el proceso de gestión del riesgo en el espacio estudiado. Esta investigación también coincide con la nuestra, en el sentido que nuestro proyecto propone la seguridad de los datos y por ende los controles que se ejecutarán disminuirán los riesgos sobre vulnerabilidad.

Cabrera (2018) concluyó que los trabajadores administrativos del espacio estudiado no consideraron a la seguridad como una prioridad alineada con sus propias estrategias; que la investigación, contribuyó a que la Municipalidad, en especial el personal de las áreas de Gerencia y Tesorería, tomen conciencia de la importancia en sus dimensiones de confiabilidad, integridad y disponibilidad para la institución,y que se fomentó la cultura de seguridad. Éste estudio no coindice con nuestra investigación, debido a que la Municipalidad Provincial de Yungay si tiene como prioridad a la seguridad de la Información. Por otro lado, se coincide con la investigación de Cabrera en el sentido de que ambas investigaciones proponemos un Modelo de Seguridad Informática.

Armas y Pérez (2018) concluyó que de acuerdo con la aplicación del MAGERIT se encontró que el CID de la Información para su valoración como criterio. Que la identificación de los procesos involucrados y los activos y la evaluación de los riesgos y amenazas de cada uno de ellos y a los que están expuestos, se encontró que en su mayoría estuvieron entre un estado de intolerable y extremo riesgo. El estudio de Armas y Pérez coincide con nuestro estudio en el sentido de que, en la Municipalidad Provincial de Yungay, la información, también se encuentran expuestos a la vulnerabilidad. A su vez estos estudios coinciden en sus procesos, debido a que estuvieron orientados a Municipalidades.

Ortigoza et al. (2019) concluyó que la institución no estableció o no contó con los protocolos obligatorios que garanticen los principios de la seguridad informática de confidencialidad, integridad y disponibilidad. Que se evidenció que la información y los equipos de la institución no estuvieron protegidos. Éste estudio coincide con nuestro estudio, debido a que la Municipalidad Provincial de Yungay tampoco cuenta con los Protocolos de seguridad informática.

Monteza (2019) concluyó que no se contaron con las medidas de seguridad adecuadas o de tenerlos no se encuentran correctamente definidos. Que respecto a la identificación, clasificación y valorización de los activos de información del proceso de recaudación y fiscalización tributaria en el área de rentas existieron varios activos de información con nivel de criticidad alta en un 72% que deben ser protegidos. Que respecto a la identificación de los riesgos de los activos de información del proceso de recaudación y fiscalización tributaria en el área de rentas existieron varios activos de información que tienen un nivel de riesgo alto con un 44% y medio con 56%, en ese sentido, se recomendó implementar controles y medidas de seguridad. Que la propuesta en el área de rentas se puede reducir cuantitativamente los riesgos de los activos de información en un nivel aceptable.

El estudio de Monteza coincide con nuestro estudio en que los procesos se desarrollaron para las Municipalidades. Utilizando Monteza en su estudio la norma ISO/IEC 27001:2013 con la finalidad de dar protección a su información, mientras que mi estudio se basó en la norma NIST SP 800 - 30 va a contribuir a que cada uno de los usuarios tomen conciencia de la seguridad informáticay se mejore la protección de la información desde las dimensiones de confidencialidad,integridad y disponibilidad.

Medrano (2019) concluyó que se clasificaron las amenazas, vulnerabilidades y la estimación de los riesgos de acuerdo a los criterios de confidencialidad, disponibilidad e integridad, que se definieron las políticas y controles para reducir los riesgos de la confiabilidad e integridad de la información y la protección de los activos y los intereses del objeto de estudio, que se analizaron los riesgos, se identificaron las vulnerabilidades y amenazas que enfrentaron los activos de información del espacio estudiado. El estudio de Medrano coincide con nuestro estudio en el sentido de que fueron realizados para Municipalidades. Así mismo, ambos concluimos con una propuesta de Modelo de Seguridad Informática.

Blas y Pretell (2020) concluyeron que se logró controlar los accesos a los recursos informáticos con la finalidad de incrementar la disponibilidad de la información, definieron políticas de cifrado con fines de aumento de la integridad de la información, establecieron la seguridad física, en las operaciones y se definieron medidas para adquirir, desarrollar y dar mantenimiento al sistema de información edil, el correcto funcionamiento de los niveles de seguridad y su interacción con los usuarios. El estudio de Blas y Pretell coincide con nuestro estudio, debido a que ambos estudios lo relacionamos con Municipalidades. Así mismo ambos estudios concluimos con una propuesta de Modelo de Seguridad Informática. La diferencia es que utilizamos diferentes normas de seguridad informática.

V. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Se concluye que se logró diagnosticar el estado situacional de la seguridad informática en la Municipalidad Provincial de Yungay, 2021, utilizando la norma NIST SP 800 - 30 el cual va ha contribuir a que cada uno de los usuarios tomen conciencia de la seguridad informática.

Se concluye que se logró Planificar las fases del Modelo de Seguridad Informática basado en NIST SP 800 – 30, verificando el estado situacional de la información respecto a confidencialidad que fue de 9.68, lo que indica que fue malo, respecto a integridad de la información fue 10.39, es decir fue malo, y el estado situacional de la información respecto a la disponibilidad fue 10.71, lo cual fue malo. El estado situacional de la información en general fue 10.39. Se han encontrado 4 riesgos con nivel bajo, 9 riesgos con nivel medio o moderado,y 2 riesgos de tipo alto, en total se han encontrado 15 riesgos en el uso del sistema de información en la Municipalidad provincial de Yungay. Se han encontrado 26.7% de riesgos con nivel bajo, 60.0% de riesgos con nivel medio o moderado, y 13.3% de riesgos de tipo alto, en total se han encontrado 15 riesgos en el uso del sistema de información en la Municipalidad Provincial de Yungay.

Se concluye que el modelo de Seguridad Informática basado en NIST SP 800 – 30 ha sido desarrollado teniendo en cuenta las fases y riesgos encontrados en el sistema de información de la Municipalidad Provincial de Yungay.

VI. RECOMENADCIONES

Se recomienda a la Alcaldía, la Gerencia Municipal y el Área de Informática que deben de adoptar las medidas de seguridad correspondientes al estado situacional de la información respecto a confidencialidad, para ello deben de solicitar la participación decidida y oportuna de todos los trabajadores ediles involucrados con el uso de sistema de información y el uso de la información importante para la municipalidad.

Se recomienda a la Alcaldía, la Gerencia Municipal y el Área de Informática que deben tener en cuenta que el modelo de Seguridad Informática basado en NIST SP 800 – 30 alcanzado está sujeto a cambios dinámicos, sobre todos, cuando pueden aparecer nuevos tipos de ataques, para ello, se recomienda realizar actualizaciones y capacitaciones en la aparición de nuevos tipos y ataques, sin descuidar los riesgos y vulnerabilidades existentes.

Se recomienda a la Alcaldía, Gerencia Municipal y al Área de Informática que deben de implementar la presente propuesta del Modelo de Seguridad Informática basado en NIST SP 800 -30 porque va a contribuir a que cada uno de los usuarios tomen conciencia de la seguridad informática y se mejore la protección de la información desde las dimensiones de confidencialidad, integridad y disponibilidad. Se debe concientizar a todos los empleados respecto a la importancia de la seguridad de la información.

Se recomienda al Área de Informática debería desarrollar capacitaciones y mejores controles respectoa los riesgos generados en el uso del sistema de información, y debe realizarlo por cada área, para ello debe concretizar la participación de todos los involucrados en la seguridad de la información.

AGRADECIMIENTOS

A Dios por permitirme el objetivo de serprofesional, a la Municipalidad Provincial de Yungay por el espacio y la información facilitada, a la Universidad San Pedro por la formación y enseñanza impartidas, a todos mis amigos, quienes de alguna manera u otra han contribuido en este logro tan importante para mi vida profesional.

Silvia

REFERENCIAS BIBLIOGRÁFICAS

Aguilera, P. (2010). *Seguridad informática. Informática y comunicaciones*. Madrid España: Editex.

Allende, D., & Gui, S. (2011). *Sistema de gestión de la seguridad de la información*. Universidad Oberta de Catalunya, 4-5.

Álvarez, W. A. (2014). *Administración de políticas de seguridad en una red de datos bajo una estructura de red definida a través de la utilización del servidor Pfsense*. Colombia.

Areitio, J. (2008). *Principios básicos de seguridad de la información. In P. in Spain (Ed.), Seguridad de la Información (Clara M. d, p. 527). Magallanes.*

Armas, A. M. y Pérez, F. R. (2018). *Desarrollo de un sistema de gestión de seguridadde la información para minimizar riesgos en los activos de información en la sub gerencia de informática y telecomunicaciones de la Municipalidad Distrital de Independencia 2016.* Tesis de grado. UNASAM, Huaraz, Perú.

Arotinco, B. L. (2017). *Gestión de cambio y configuración basado en el modelo de buenas prácticas de ITIL para mejorar la plataforma informática en el Bancode Crédito*. Tesis de grado. Universidad Nacional Tecnológica de Lima Sur.Perú.

Blas, W. D. y Pretell, G. F. (2020). *Modelo de seguridad de la información para mejorar la gestión informática en la Municipalidad Distrital de Florencia deMora*. Tesis de grado. Universidad Nacional de Trujillo. Perú.

Bonilla, S. M., & González, J. A. (2012). *Modelo de seguridad de la información. Ingenierías* USBMed, 3(1), 6-14. Recuperado el 15 de 4 de 2018, de https://dialnet.unirioja.es/descarga/articulo/4692844.pdf

Borghello, C. F. (2011). *Seguridad Informática: sus implicancias e implementació*n. Argentina: Universidad Tecnológica Nacional de Argentina.

Cabrera, H. P. (2018). *Diseño de un modelo de políticas basado en la norma ISO 27001, para mejorar la gestión de la seguridad de la información en la Municipalidad Distrital de Florida – Bongará Amazona*. Tesis de grado. Universidad Peruana Unión. Tarapoto, Perú.

Carlini, A. (2016). *Ciberseguridad: Un nuevo desafío para la comunidad internacional*. http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO 67- 2016_Ciberseguridad_Desafio_ComunidadInt_ACarlini.pdf

CERT (2013) *Metodología OCTAVE*, [On line]. Disponible en http://www.cert.org/octave/

CISCO (2016). *Informe anual de seguridad.* Informe, Cisco y/o sus filiales, América.

Comer, D. (2015). *Redes globales de información con internet y TCP/IP: PrincipiosBásicos., protocolos y arquitectura, 880.*

Corletti, A. (2016). *Seguridad por niveles. En A. Corletti Estrada, Seguridad en Redes* (pág. 354). Madrid: LEARNING CONSULTING S.L.

Daltabuit, E., Hernández, L., Mallén, G. & Vázquez, José. (2007). *La Seguridad de laInformación.* México: Limusa.

De Pablo, S. A. (2007). *Evaluación de seguridad de información para la plataforma de Banca Virtual en una entidad financiera*. Tesis de Grado. Universidad Central de Caracas. Venezuela.

DELOITTE. (2017). *Seguridad de la información en Ecuador*. Quito: Deloite Ecuador.

Everett, C. (2011). *A risky business: ISO 31000 and 27005 unwrapped. Computer Fraud & Security*, 5-7.

Gómez, Á. (2011). *¿Qué es la Seguridad Informática?* En Á. Gómez, Seguridad Informática Básico (págs. 7-8). Bogotá: Ecoe Ediciones.

Grijalva, D. (2018). *Diseño de un Plan Estratégico de Seguridad de la Información, Mediante la Aplicación de Análisis de Riesgos con la Norma ISO/IEC 27005 Caso de Estudio INAMHI. INNOVA* Research Journal, 30-31.

Hernández, R.; Fernández, C. y Baptista, P. (2010). *Metodología de la investigación*.
Quinta edición. México: Mc Graw Hill. ISBN: 978-607-15-0291-9

INEI. (2017). *Número de municipalidades y población total proyectada al 30 de junio*.
INEI, 2.

ISO/IEC 27001 (2018). *Information security management systems.* ISO.

ISO27001. (2010). *Sistema de Gestión de la Seguridad de la Información*.
Www.Iso27000.Es, 1, 14.

Jara, O. Y. (2018). *Sistema de gestión de seguridad de la información para mejorar elproceso de gestión del riesgo en un gobierno local, 2018.* Tesis de maestría. Universidad César Vallejo. Perú.

Javier, A. (2008). *Seguridad de la información, Redes informática y sistemas de información*. España, Madrid: Cengage Leaning Paraninfo S.A.

Karina, M. (2013). *Guía metodológica para implementar un sistema de seguridad en instituciones. Piura, Perú*: Universidad de Pirua. Facultad de Ingeniería.

Kawamoto, D. (2005). *Faced with a rise in so-called pharming and crimeware attacks,the Anti-Phishing Working Group will expand its charter to include these emerging threats.* India: ZDNet.

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

McKinsey, L., Samandari & Simoes (2006). *Better operational-risk management for banks.* California. McKinsey Quarterly Bulletin.

Medina. F. M. (2017). *Seguridad Informática: virus ransomware, el Secuestro virtualde datos es Posible.* Tesis de grado. Universidad Empresarial Siglo 21.Argentina.

Medrano, Y. A. (2019). *Plan de la seguridad de la información basado en la norma ISO 27001 para la sub gerencia de informática y tecnologías de la información de la Municipalidad de Punta Hermosa*. Tesis de grado. Universidad Nacional Tecnológica de Lima Sur. Perú.

Mell, P., & Scarfone, K. (2007). *Guide to Intrusion Detection*. Recommendations of the National Institute, 3-7.

Montes, M. (2010). *Seguridad Lógica y de accesos y su auditoría*. España Madrid: Universidad Carlos II.

Monteza, L. O. (2019). *Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la Municipalidad Distrital de El Agustino*. Tesis de grado. Universidad Peruana de Ciencias Aplicadas. Lima. Perú.

Morales, J. y. (2006). *Seguridad en Redes Inalámbricas IEEE 802.11.* Criptografía y Seguridad de redes. EBook, 10.

Moreira, T. Y. (2019). *Plan de seguridad informática en redes y la gestión operativa de la Cooperativa de Ahorro y Crédito "San Antonio*". Tesis de grado. Universidad Regional Autónoma de los Andes. Ambato. Ecuador.

Nichosls, R. K. (2006). *Wireless security models. Threats and solutions*. New York: Mc Graw Hill.

Ortigoza, et al. (2019) *Políticas de seguridad informática para la administración de recursos tecnológicos y gestión de la información en la empresa consultoríasy asesorías en seguridad y salud en el trabajo S.A.S (CONSASST), 2019*. tesis de grado. Universidad cooperativa de Colombia.

Ortiz, D. F. (2015). *Desarrollo De Metodología Para Hallazgos De Vulnerabilidades En Redes Corporativas E Intrusiones Controladas*. Trabajo de Grado de Ingeniero Electrónico.

Ríos, J. (2014). *Técnicas y herramientas de análisis de vulnerabilidades de una red. Proyecto de fin de grado*. Escuela Técnica Superior de Ingeniería y Sistemasde Telecomunicación, Madrid.

Roa, J. F. (2013). *Seguridad Informática.* Aravaca, Madrid: McGraw-Hill.

RPP. (2015). *El 90% de ataques cibernéticos en Perú provendría de fuentes internas*.

Economía, pág. 1.

Sullivan, D. (2004). *The Definite Guide to Security Management*. ComputerAssociates.

Veritas, J. (2005). *Information Security Management System* - ISO 27001. ISO / IEC.

Villalon, A. (2004). *El Sistema de Gestión de Seguridad de la Información*.http://www.shutdown.es/ISO17799.pdf

Zauzich, I. (2016). COBIS: *Financial Agilitty Partners*. Obtenido de Cloud Banking:http://blog.cobiscorp.com/banca-en-la-nube-cloud-banking

ANEXOS Y APÉNDICES

ANEXO 01: MATRIZ DE CONSISTENCIA

Tabla Matriz de Consistencia: Modelo de Seguridad informática para la seguridad de la información: Municipalidad Provincial de Yungay, 2021

Problema	Hipótesis	Objetivo	Variables	Metodología
¿Cómo elaborar un Modelo de Seguridad Informática basado en NIST SP 800 - 30 para proteger la información en la Municipalidad Provincial de Yungay, 2021?	La Investigación tiene un alcance de carácter descriptivo, por lo que no se plantea una hipótesis, debido a que no se intenta correlacionar o explicar causalidad de variables y el objetivo a alcanzar está claro. Por tal razón se considera una hipótesis implícita.	**Objetivo General:** Proponer un Modelo de Seguridad Informática basado en NIST SP 800 - 30 para proteger la información en la Municipalidad Provincial de Yungay, 2021 **Objetivos Específicos** ✓ Diagnosticar el estado situacional de la seguridad informática en la Municipalidad Provincial de Yungay, 2021. ✓ Planificar las fases del Modelo de Seguridad Informática basado en NIST SP 800 - 30 ✓ Elaborar Modelo de Seguridad Informática basado en NIST SP 800 - 30 para proteger la información en la Municipalidad Provincial de Yungay, 2021.	**Variable 1** Seguridad de la Información	**Tipo de Investigación:** Nivel: Descriptivo **Diseño:** No experimental **Población:** 28 trabajadores **Técnicas e Instrumentos:** Encuesta

ANEXO 02: MATRIZ OPERACIONAL

Tabla Matriz Operacional: Modelo de Seguridad informática para la seguridad de la información: Municipalidad Provincial de Yungay, 2021

Variables	Definición Conceptual	Dimensiones	Indicadores
Seguridad de la Información	Para ISOTools Excellence (2017), la definición de la seguridad de la información tributa a una disciplina "que se encarga de la implementación técnica de la protección de la información, el despliegue de las tecnologías que establecen de forma que se aseguran las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo (…) es la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y los esquemas normativos, que nos exigen niveles de aseguramiento de procesos y de tecnología para elevar el nivel de confianza en la creación, utilización, almacenaje, transmisión, recuperación y disposición final de la información". (ISOTools Excellence, 2017)	Identificación Protección Detección Respuesta y recuperación Confidencialidad Integridad Disponibilidad	✓ Priorización de acciones ✓ Prevención ✓ Disuasión ✓ Eliminación ✓ Minimización del impacto / limitación del impacto ✓ Corrección ✓ Recuperación ✓ Monitorización ✓ Detección ✓ Concientización ✓ Administración ✓ Implantación de controles seleccionados

ANEXO 03: ENCUESTA

Bach. Cochachin Jara Silvia Soledad

Estimado encuestado: Sírvase responder con absoluta sinceridad la siguiente encuesta, que corresponde al estudio de un Modelo de Seguridad informática para mejorar la seguridad de la información: Municipalidad Provincial de Yungay, 2021. Sírvase responder la encuesta con responsabilidad y honestidad. Este proceso es totalmente anónimo, se reitera el pedido de absoluta honestidad en sus respuestas. Muchas Gracias por su participación.

CUESTIONARIO

N°	DIM	CUESTIONARIO	ESCALA				
			1	2	3	4	5
MODELO DE SEGURIDAD INFORMÁTICA							
01	**Identificación**	¿Cómo valora la identificación de los activos de información por el Modelo de Seguridad Informática en la Municipalidad Provincial de Yungay, 2021?					
02		¿Cómo califica la identificación de los riesgos de activos de información por el Modelo de Seguridad Informática en la Municipalidad Provincial de Yungay, 2021?					
03		¿Cómo evalúa la identificación de las responsabilidades del activo de información por el Modelo de Seguridad Informática en la información en la Municipalidad Provincial de Yungay, 2021?					
04	**Protección**	¿Cómo considera la protección de los usuarios del activo de información por el Modelo de Seguridad Informática en la Munipalidad Provincial de Yungay, 2021?					

05		¿Cómo evalúa la protección de los programas de seguridad el Modelo de Seguridad Informática en la Municipalidad Provincial de Yungay, 2021?					
06		¿Cómo califica la protección de las Políticas de eliminación segura por el Modelo de Seguridad Informática en la Municipalidad Provincial de Yungay, 2021?					
07		¿Cómo evalúa la capacitación en ciberseguridad por el Modelo de Seguridad Informática en la Municipalidad Provincial de Yungay, 2021?					
08		¿Cómo califica la comprobación de riesgos personales por el Modelo de Seguridad Informática en la Municipalidad Provincial de Yungay, 2021?					
09		¿Cómo considera la protección de datos por el Modelo de Seguridad Informática en la Municipalidad Provincial de Yungay, 2021?					
10	**Detección**	¿Cómo califica la contribución en la detección del acceso a personal autorizado por el Modelo de Seguridad Informática en la Municipalidad Provincial de Yungay, 2021?					
11		¿Cómo valora la contribución en la detección de almacenamiento de datos por el Modelo de Seguridad Informática en la Municipalidad Provincial de Yungay, 2021?					
12		¿Cómo evalúa la contribución en la detección de las actividades inusuales por el Modelo de Seguridad Informática en la Municipalidad Provincial de Yungay, 2021?					
13	**Respuesta y recuperación**	¿Cómo califica la respuesta y recuperación en la notificación a los usuarios por Modelo de Seguridad Informática en la Municipalidad Provincial de Yungay, 2021?					
14		¿Cómo considera la respuesta y recuperación en el mantenimiento del funcionamiento de las operaciones ediles por el Modelo de Seguridad Informática en la Municipalidad Provincial de Yungay, 2021?					
15		¿Cómo valora la respuesta y recuperación en el reporte de ataques por el Modelo de Seguridad Informática en la Municipalidad Provincial de Yungay, 2021?					

16		¿Cómo evalúa la respuesta y recuperación en la contención de ataques por el Modelo de Seguridad Informática en la ¿Municipalidad Provincial de Yungay, 2021?					
17		¿Cómo califica la respuesta y recuperación en la reparación y restauración de hardware y software por el Modelo de Seguridad ¿Informática en la Municipalidad Provincial de Yungay, 2021?					
18		¿Cómo considera la respuesta y recuperación en la información a los usuarios por el Modelo de Seguridad Informática en la Municipalidad Provincial de Yungay, 2021?					

LEYENDA

1 Malo 2 Regular 3 Bueno 4 Muy bueno 5 Excelente

N°	DIM	CUESTIONARIO	ESCALA				
			1	2	3	4	5
SEGURIDAD DE LA INFORMACIÓN							
01	**Confidencialidad**	¿Cómo Valora la confidencialidad respecto a la cantidad de usuarios autorizados como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?					
02		¿Cómo califica la confidencialidad con referencia a la cantidad de información confidencial accesible como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?					
03		¿Cómo evalúa la confidencialidad en la cantidad de información confidencial hackeados como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?					
04		¿Cómo valora la confidencialidad sobre la cantidad de información confidencial recuperados como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?					
05		¿Cómo valora la confidencialidad con referencia grado de daño causado por el acceso a la información confidencial como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?					
06	**Integridad**	¿Cómo valora la integridad de la cantidad de información que debe mantenerse integro como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?					
07		¿Cómo evalúa la integridad sobre la cantidad de información no íntegros como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?					
08		¿Cómo considera la integridad con referencia al nivel de integridad de fuentes de información como medida de seguridad en la ¿Municipalidad Provincial de Yungay, 2021?					
09		¿Cómo califica la integridad respecto a la cantidad de información recuperados de su integridad como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?					
10		¿Cómo califica la integridad del nivel de daño causado por falta a la integridad de la información en la Municipalidad Provincial de Yungay, 2021?					

11	**Disponibilidad**	¿Cómo valora la disponibilidad sobre la cantidad de información disponible como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?					
12		¿Cómo evalúa la disponibilidad de la cantidad de información no disponible como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?					
13		¿Cómo considera la disponibilidad con referencia al nivel de disponibilidad de la información como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?					
14		¿Cómo califica la disponibilidad sobre la cantidad de información no disponibles recuperados en la Municipalidad Provincial de Yungay, 2021?					
15		¿Cómo valora la disponibilidad con referencia al nivel de daño causado por la no disponibilidad de la información en la Municipalidad Provincial de Yungay, 2021?					

LEYENDA

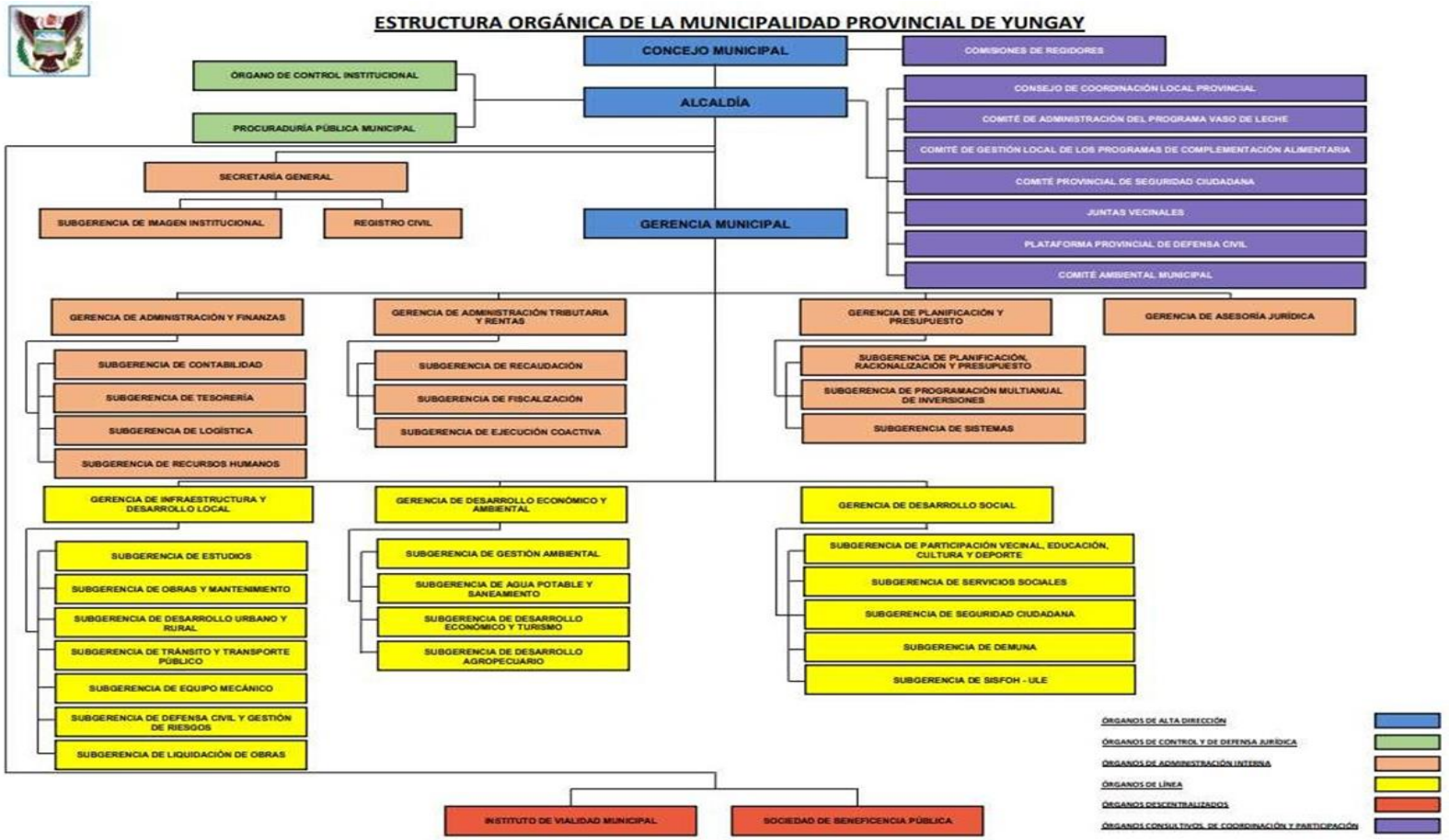
1 Malo 2 Regular 3 Bueno 4 Muy bueno 5 Excelente

Anexo 04 Alfa de Cronbach

N°	MODELO DE SEGURIDAD INFORMÁTICA																					
	Identificación			TOT	Protección						TOT	Dirección			TOT	Respuesta y recuperación						TOT	TOT
	1	2	3		4	5	6	7	8	9		10	11	12		13	14	15	16	17	18		
1	3	2	1	6	1	2	1	2	1	2	9	1	1	1	3	2	1	5	1	2	1	12	30
2	2	3	1	6	2	3	4	1	1	3	14	1	2	1	4	4	1	3	2	4	2	16	40
3	2	4	1	7	4	4	5	5	5	4	27	5	4	5	14	4	5	2	1	2	4	18	66
4	4	2	3	9	4	4	5	3	3	2	21	3	4	3	10	3	3	2	5	4	4	21	61
5	1	4	5	10	4	2	4	1	1	4	16	5	4	5	14	4	5	1	4	2	4	20	60
6	2	1	1	4	2	1	1	2	1	1	8	1	2	1	4	1	1	2	2	1	2	9	25
7	2	5	1	8	4	2	2	2	1	5	16	1	4	1	6	2	1	1	3	1	4	12	42
8	5	4	5	14	3	2	2	3	1	4	15	2	2	3	7	4	3	2	5	2	5	21	57
9	4	5	4	13	4	4	5	2	4	5	24	4	4	4	12	4	4	2	1	4	2	17	66
10	2	4	5	11	4	4	5	5	5	4	27	5	4	5	14	4	1	1	4	4	4	18	70
Var				9.36							42				18.4							15.4	51.7
																						Suma de varianzas	85.17
																						Varianza General	234.21
																						Valor de Alfa	0.848

N°	SEGURIDAD DE LA INFORMACIÓN																		
	Confidencialidad					TOT	Integridad					TOT	Disponibilidad					TOT	TOT
	1	2	3	4	5		6	7	8	9	10		11	12	13	14	15		
1	11.0	5.0	5.0	5.0	11.0	37.0	5.0	11.0	5.0	5.0	11.0	37.0	5.0	5.0	11.0	5.0	5.0	31	105.00
2	11.0	11.0	14.0	5.0	5.0	46.0	11.0	11.0	11.0	5.0	5.0	43.0	5.0	5.0	11.0	5.0	11.0	37	126.00
3	11.0	5.0	5.0	11.0	11.0	43.0	5.0	5.0	5.0	17.0	11.0	43.0	5.0	14.0	11.0	5.0	5.0	40	126.00
4	11.0	19.0	19.0	5.0	5.0	59.0	5.0	19.0	19.0	5.0	5.0	53.0	14.0	5.0	5.0	11.0	14.0	49	161.00
5	11.0	5.0	5.0	11.0	14.0	46.0	14.0	5.0	5.0	11.0	14.0	49.0	19.0	11.0	17.0	14.0	19.0	80	175.00
6	19.0	17.0	19.0	14.0	19.0	88.0	19.0	17.0	19.0	14.0	19.0	88.0	11.0	14.0	5.0	11.0	19.0	60	236.00
7	11.0	5.0	5.0	11.0	14.0	46.0	11.0	5.0	5.0	11.0	14.0	46.0	5.0	11.0	5.0	5.0	14.0	40	132.00
8	19.0	5.0	17.0	14.0	11.0	66.0	19.0	5.0	17.0	14.0	11.0	66.0	5.0	14.0	19.0	5.0	5.0	48	180.00
16	5.0	5.0	5.0	11.0	5.0	31.0	5.0	11.0	5.0	14.0	5.0	40.0	5.0	11.0	5.0	5.0	5.0	31	102.00
17	11.0	19.0	17.0	19.0	5.0	71.0	11.0	14.0	17.0	19.0	5.0	66.0	11.0	19.0	17.0	11.0	14.0	72	209.00
Var						274						225.3						285.1	155.2
																	Suma de varianzas		784.37
																	Varianza General		1805.76
																	Valor de Alfa		0.848

Anexo 05: Organigrama



Anexo 06

Modelo de seguridad informática basado en NIST SP 800 – 30 para la Municipalidad Provincial de Yungay, 2021

MARCO NIST SP-800-30

El presente Modelo de seguridad informática tiene por objetivo garantizar la seguridad de manera integral y de forma específica los de datos e información de la Municipalidad Provincial de Yungay. Para los efectos del presente modelo, se va a desarrollar un conjunto de procesos y actividades obligatorias, orientaciones, que deben analizar y aplicar todos los colaboradores de la institución edil, es responsabilidad de la administración de la administración, del Área de Informática y de todos los usuarios, estaratentos y vigilar su estricto cumplimiento en el ámbito de su competencia, para ello debentomar medidas preventivas y correctivas para que se cumplan en su totalidad.

El alcalde de la municipalidad conjuntamente con la gerencia municipal, así como con el área de informática son responsables directos de la seguridad de la información de la institución edil, ellos son quienes están a cargo del uso del sistema informático y su respectiva seguridad, apoyan y capacitan a cada uno de los usuarios de sus respectivas áreas. la información que se genera en la municipalidad, no todas son muy importantes, pero sí existen informaciones que son muy importantes para la toma de decisiones, sobre todo en la información que hace referencia a compras y a licitaciones para proyectos de inversión social.

Debido a que la municipalidad genera información muy importante para la toma de sus decisiones en diversas áreas y en su integralidad como institución edil, en ese sentido, sehace muy necesario que la municipalidad disponga de un sistema y nivel de seguridad adecuado a sus funciones sociales, en donde se cuide a la información, sobre todo, cuando está en juegos considerables cantidades de inversiones de dinero y la gobernabilidad de toda una comunidad.

MODELO DEL MARCO DE SEGURIDAD NIST SP-800

Acceso de la información

Toda la información de las diversas unidades o áreas de la Municipalidad Provincial de Yungay debe de ser clasificada como: Confidencial, Integridad y Disponibilidad. Para la presente propuesta del modelo del marco de seguridad basado en NIST SP 800 – 30, las informaciones digitales implican definir a la clasificación de la información en varias fases propias de esta metodología enfocada hacia la seguridad de la información.

Confidencial: La información en cualquiera de sus modalidades digitales o físicas, pro principalmente digitales deben ser accesibles solo al personal edil quienes están debidamente autorizados mediante documentación para el cumplimiento de sus funciones. Tiene acceso el personal que lo genera y la gerencia de la municipalidad. Información confidencial son los documentos de proyectos que implican grandes montos de inversión, licitaciones, liquidaciones, informes de avance, contraloría, rendición de cuentas, etc.

Integridad: La integridad indica y el documento es considerado muy importante para lainstitución edil debe mantenerse completo, sin cortes ni variaciones, que nadie haya modificado la totalidad del mensaje, ni tampoco variado sus datos. los responsables de laintegridad de la información son la alcaldía, la gerencia municipal y el área informática.

Disponibilidad: La disponibilidad hace referencia a que el documento debe estar disponible cada vez que los usuarios adecuados y debidamente asignados puedan utilizarlo en el momento en el que desee sin ningún tipo de restricción de tipo físico o informático. Tiene acceso todo el personal implicado y la gerencia de la municipalidad.

La seguridad de la información implica que toda información debe ser controlada e inspeccionada por cada usuario y en cada área de la institución edil, se debe también teneren cuenta la seguridad a nivel de hardware, software y almacenamiento de la información.todos son responsables de la seguridad en sus respectivos niveles, de manera tal que unaadecuada seguridad se va a

garantizar si todos participan conscientemente en ella.

Metodología de la propuesta

La metodología del Marco de seguridad basado en NIST SP-800, como metodología se aplica en las siguientes fases (ISO/IEC 27001, 2018), y como tal se deben aplicar en a lainstitución edil con la finalidad de asegurar la seguridad de la información:

Caracterización del sistema: En esta parte de debe de establecer los alcances de lo quese va a evaluar en función al riesgo a lo que están sujetos la información de la municipalidad, la caracterización debe realizarse al hardware, software, documentacionesy políticas de seguridad.

Identificación de amenazas: En la fase de identificación de amenazas se deben identificar a los agentes internos y externos con capacidades potenciales de amenazas que podrían estar explotando las debilidades o vulnerabilidades del sistema de información de la municipalidad, en este caso, las amenazas deben ser identificadas en función a los usuarios del sistema de información, esto significa, las conductas que adopta cada usuario en el uso del sistema, la conducta sobre las normas de seguridad; Se analiza la seguridad que corresponde al hardware y al software; también se identifican amenazas externas como las inundaciones, sismos, incendios, tormentas, huaycos, etc.

Identificación de vulnerabilidades: La fase de identificación consiste en identificar los activos de información de la institución edil, establecer los riesgos en la que se encuentran los diversos activos de la institución y las responsabilidades que se tiene por cada uno delos activos. en la identificación de los activos consiste en determinar la cantidad de hardware, la cantidad de software, y la cantidad de personal que está a cargo de toda esta tecnología. En la cantidad de los activos de información se cuantifica el software en función a tipos, ya sean de sistema operativo, de trabajo en la municipalidad, y de accesoa internet, así como también el software antivirus que utiliza el sistema. Respecto a los riesgos de los activos esta metodología aplica la identificación de los riesgos por cada área y por persona, para ello analiza los procesos que

realizan cada uno de ellos y, cómolo están utilizando en función a las normas establecidas. En las responsabilidades del activo se determina la responsabilidad de cada área y de cada usuario, todo ello, en función a la seguridad del sistema de información.

Análisis de controles: En esta fase se analizan los controles de seguridad que debe estar utilizando todo el sistema de información de la municipalidad con la finalidad de reducirla probabilidad de ataques como ocurrencias de alguna amenaza debido a la vulnerabilidad que presenta, en esta fase se busca reducir el impacto de los ataques, para ello, las autoridades correspondientes deben desarrollar controles técnicos relacionados con hardware, software y documentación, así como con las políticas de seguridad. se deben llevar a cabo controles de prevención de ataques a sistemas específicos, para ello se debe contar con hardware y software que permita el control sistemático de la seguridad de la información, estos controles preventivos deben prever cualquier futuro ataque y no dar espacio para que eso suceda, esto lo deben lograr mediante accesos al sistema con contraseñas adecuadas, con codificación criptográfica y una adecuada autenticación, se debe controlar adecuadamente los perfiles de cada usuario y el cumplimiento del acceso a la información así como su respectivo uso.

Determinación de Probabilidades: Mediante el estudio de las fases anteriores, los encargados de la seguridad de la información de la municipalidad deben determinar la probabilidad de ocurrencia de una amenaza la cual constituye la vulnerabilidad del sistema, esta determinación debe realizarse mediante la consideración de 3 factores, primero la motivación y la capacidad de las fuentes de amenaza, la motivación está generada por el conocimiento hacia los archivos o documentos de compra y de licitaciones pública, mientras que la capacidad está ligada a las potencialidades que dispone el atacante para realizar su delito. Segundo, la naturaleza de la vulnerabilidad, en esta parte se debe determinar sin la vulnerabilidad se debe a Harvard, software, los recursos humanos, para evitar ello, se debe realizar los controles respectivos indicado en las fases anteriores, para realizar la determinación de las probabilidades se elabora una tabla de identificación de vulnerabilidades y en función a ella se determinan las probabilidades de

ataques para cada vulnerabilidad, con esta tabla se genera un ranking de vulnerabilidades. Tercero, se deben analizar y realizar los controles actuales.

Análisis de impacto: En la fase de análisis de impacto se deben analizar los niveles de impactos relacionados con la importancia de la información de la institución edil, sobre

todos aquellos documentos que implican compras y situaciones públicas, la evaluación debe ser del tipo cualitativa y cuantitativa en función a la situación crítica en que se encuentran los activos de información. se deben vincular los riesgos con los componentes de seguridad y determinar el impacto que debe tener cada vulnerabilidad en los objetivos de la empresa o institución medida, sobre todo en la parte de activos, se debe calcular la magnitud del impacto en el caso de ocurrencia o no de una probable amenaza.

Determinación del riesgo: Para determinar el riesgo se hace uso del ranking de probabilidades de ocurrencia de la amenaza, la magnitud del impacto y la pertinencia o adecuación de los controles de seguridad que se ha utilizado para reducir o minimizar los riesgos de eventuales ataques hacia el sistema de seguridad de la institución edil. Se puede utilizar cuadros y tablas estadísticas para esquematizar y simplificar la determinación del riesgo.

Recomendaciones de control: En la fase de recomendaciones de control se debe llevar a cabo controles al recurso humano, al software, al hardware, a la documentación, todo ello en comparación frecuente con las políticas de seguridad establecidas por las autoridades de la Municipalidad Provincial de Yungay. En esta fase se debe realizar el análisis de costo beneficio, así como también se puede utilizar otras ratios, cómo el valor prente neto y la tasa interna de retorno para demostrar la factibilidad de los costos incurridos en la seguridad de la información y ligados a la reducción del nivel de riesgo.

Documentación de Resultado: Como etapa final, esta metodología exige que se debe documentar el resultado, para ello se recomienda iniciar con una definición de las amenazas y vulnerabilidades, cuantificación de los riesgos, expresar las recomendaciones para la implementación de controles y que éstos deban estar debidamente documentados, se debe incluir al resultado

cuantificaciones estadísticas sobre la aplicación de la metodología y los beneficios de su aplicación en la reducción de los riesgos y vulnerabilidades relacionados con la seguridad de la información en la municipalidad.

Acciones adicionales y pertinentes a realizar

Capacitación de usuarios: Es responsabilidad de las autoridades ediles promover frecuentemente la importancia de la seguridad a todos los usuarios de los sistemas de información. Se recomienda capacitar a los empleados y trabajadores de la municipalidad en los aspectos de la seguridad de la información, específicamente en el robo de información. El programa de concientización en seguridad debe de contener continuas capacitaciones y charlas, adicionalmente se puede emplear diversos métodos como afiches, llaveros, etc., los cuales recuerden permanentemente al usuario el papel importante que cumplen en el mantenimiento de la seguridad de la información. Los usuarios deben de ser informados anualmente sobre la importancia de la seguridad de la información. Un resumen escrito de la información básica debe de ser entregada nuevamente a cada empleado y una copia firmada debe de ser guardada en sus archivos.

PERFILES DEL MARCO DE SEGURIDAD NIST SP-800

Respuesta ante incidentes de seguridad

El jefe de Informática debe ser plenamente identificado por todos los empleados de la Municipalidad. Si un empleado de la municipalidad detecta o sospecha la ocurrencia de un incidente de seguridad, tiene la obligación de notificarlo al jefe de dicha área. Si se sospecha la presencia de un ataque de robo de información, el usuario debe desconectar el equipo de la red de datos, notificar al área de informática quien trabajará en coordinación con el área de soporte técnico, para la eliminación del virus antes de restablecer la conexión a la red de datos. Si un empleado detecta una vulnerabilidad en laseguridad de la información debe notificarlo al personal encargado de la administración de la seguridad, asimismo, está prohibido para el empleado realizar pruebas de dicha vulnerabilidad o aprovechar ésta para propósito alguno.

Informática y Alcaldía deben documentar todos los reportes de incidentes de seguridad. Cualquier error o falla en los sistemas debe ser notificado a soporte técnico, quién determinará si el error es indicativo de una vulnerabilidad en la seguridad. El personal encargado de operar los sistemas de información debe registrar todos los errores y fallas que ocurren en el procesamiento de información o en los sistemas de comunicaciones. Estos registros deben incluir lo siguiente: Nombre de la persona que reporta la falla, Hora y fecha de ocurrencia de la falla, Descripción del error o problema, responsable de solucionar el problema, Descripción de la respuesta inicial ante el problema, Descripciónde la solución al problema, Hora y fecha en la que se solucionó el problema.

Los registros de fallas deben ser revisados semanalmente. Los registros de errores no solucionados deben permanecer abiertos hasta que se encuentre una solución al problema. Además, estos registros deben ser almacenados para una posterior verificación independiente.

Control de información

Todo medio de almacenamiento secundario (Disco duro, USB, otros medios, copias de backup, etc.), deben presentar una etiqueta con la clasificación correspondiente. La información en formato digital clasificada como de acceso "Disponibilidad", puede ser almacenada en cualquier sistema de la Municipalidad. Sin embargo, se deben tomar las medidas necesarias para no mezclar información "General" con información correspondiente a otra clasificación.

Todo usuario, antes de transmitir información clasificada como "Confidencial o "Integridad", debe asegurarse que el destinatario de la información esté autorizado a recibir dicha información. Todo usuario que requiere acceso a información clasificada como "Confidencial o "Integridad", debe ser autorizado por el personal que lo genero o propietario de la misma. Las autorizaciones de acceso a este tipo de información deben ser documentadas.
Los activos de información correspondiente a distintos niveles de clasificación, deben ser almacenados en distintos contenedores, de no ser posible dicha

distinción, se asignará el nivel más crítico de la información identificada a todo el contenedor de información. El ambiente donde se almacena la información clasificada como “Confidencialidad”, debe contar con adecuados controles de acceso y asegurado cuando se encuentre sin vigilancia. El acceso debe ser permitido solo al personal formalmente autorizado. Personal de limpieza debe ingresar al ambiente acompañado por personal autorizado. Solo el personal formalmente autorizado debe tener acceso a información clasificada como “Confidencial o“Integridad”.

Intercambios de información y correo electrónico

Los mensajes de correo electrónico deben ser considerados de igual manera que un memorándum formal, son considerados como parte de los registros de la municipalidad y están sujetos a monitoreo y auditoria. Los sistemas de correo electrónico no deben ser utilizados para lo siguiente: Enviar cadenas de mensajes, enviar mensajes relacionados aseguridad, exceptuando al personal encargado de la administración de la seguridad de la información, actividades ilegales, no éticas o impropias, actividades no relacionadas con el negocio de la municipalidad, diseminar direcciones de correo electrónico a listas públicas.

No usar reglas de reenvío automático a direcciones que no pertenecen a la organización.No existe control sobre los mensajes de correo electrónico una vez que estos se encuentran fuera de la red de la municipalidad. Se deben establecer controles sobre el intercambio de información de la municipalidad con terceros para asegurar la confidencialidad e integridad de la información, y que se respete la propiedad intelectual de la misma. Debe tomarse en consideración: Acuerdos para el intercambio de software,seguridad de medida en tránsito, controles sobre la transmisión mediante redes.

Seguridad de instalaciones de procesamiento de datos

Implementar medidas de seguridad física para asegurar la integridad de los datos y documentos. Las medidas de protección deben ser consistentes con el nivel de clasificación de los activos y el valor de la información procesada y almacenada en las computadoras. El acceso a cualquier instalación de cómputo debe estar restringidoúnicamente al personal autorizado. Las visitas

deben ser identificadas y se debe mantenerun registro escrito de las mismas. Estas visitas deben ser en compañía de un empleado durante la permanencia en las instalaciones de cómputo. La visita de los proveedores de mantenimiento, a quienes se les otorga acceso continuo a las áreas sensibles, estén siempre acompañados por un empleado autorizado de la municipalidad, puede resultar poco práctico en algunos casos.

Todo el personal en las instalaciones de cómputo debe de portar un carné, placa o ficha de identificación. Sistemas automatizados de seguridad para acceso físico deben de ser instalados en centros de cómputo principales. El retiro de cualquier equipo o medio electrónico de las instalaciones de cómputo debe de ser aprobado por escrito por personalautorizado.

Administración de comunicaciones y operaciones

Todas las comunicaciones e intercambios de información, tanto dentro de las instalaciones y sistemas de la Municipalidad como externas a ella, deben ser aseguradas, de acuerdo al valor de la información protegida. Todos los procedimientos de operación de los sistemas deben ser documentados y los cambios realizados a dichos procedimientos deben ser autorizados por la autoridad respectiva. Todos los procedimientos de encendido y apagado de los equipos deben ser documentados; dichos procedimientos deben incluir el detalle de personal clave a ser contactado en caso de fallas no contempladas en el procedimiento regular documentado.

Todas las tareas programadas en los sistemas para su realización periódica, deben ser documentadas. Este documento debe incluir tiempo de inicio, tiempo de duración de la tarea, procedimientos en caso de falla, entre otros. Todos los cambios operacionales realizados en los sistemas de la municipalidad, a excepción de los cambios de emergencia, deben seguir los procedimientos de cambios establecidos.

Protección contra virus

Es responsabilidad del Área de Informática de realizar esfuerzos para determinar el origen de la infección por virus informático, para evitar la reinfección de los equipos de la municipalidad. El programa antivirus debidamente actualizado debe encontrarse habilitado en todas las computadoras de la municipalidad y debe ser actualizado periódicamente. En caso de detectar fallas en el funcionamiento de dichos programas

éstas deben ser comunicadas al área de soporte técnico. El programa antivirus debe ser configurado para realizar revisiones periódicas para la detección de virus en los medios de almacenamiento de las computadoras de la municipalidad. Debe contarse con un procedimiento para la actualización periódica de los programas antivirus y el monitoreo de los virus detectados. Es obligación del personal de la municipalidad, emplear sólo losprogramas cuyas licencias han sido obtenidas por la municipalidad y forman parte de su plataforma estándar. Asimismo, se debe evitar compartir directorios o archivos con otrosusuarios; en caso de ser absolutamente necesario, coordinar con la administración de la municipalidad.

Control de acceso de datos

La información manejada por los sistemas de información y las redes asociadas debe estar adecuadamente protegida contra modificaciones no autorizadas, divulgación o destrucción. El uso inteligente de controles de acceso previene errores o negligencias delpersonal, así como reduce la posibilidad del acceso no autorizado. Cada usuario de una computadora en la municipalidad debe de ser identificado de manera única, y el acceso del usuario, así como su actividad en los sistemas debe de ser controlado, monitoreado yrevisado. Cada usuario de un sistema debe tener un código de identificación que no sea compartidocon otro usuario. Para lograr el acceso a los sistemas automatizados, se requiere que el usuario provea una clave que solo sea conocida por él. Debe establecerse un procedimiento para asegurar que el código de identificación de un usuario sea retirado detodos los sistemas cuando un empleado es despedido o transferido. Los terminales y computadoras personales deben bloquearse

luego de quince (15) minutos de inactividad.El usuario tendrá que autenticarse antes de reanudar su actividad. El usuario debe ser instruido en el uso correcto de las características de seguridad del terminal y funciones de todas las plataformas, estaciones de trabajo, terminales, computadoras personales, etc., ydebe cerrar la sesión o bloquear la estación de trabajo cuando se encuentre desatendida.

Todas las computadoras de la municipalidad deben proveer pistas de auditoría del ingresoa los sistemas y violaciones de los mismos. A partir de estos datos, los custodios de los

sistemas deben elaborar reportes periódicos los cuales deben ser revisados por el área de seguridad informática. Estos reportes también deben incluir la identidad del usuario, y la fecha y hora del evento. Si es apropiado, las violaciones deben ser reportadas al gerente del individuo. Violaciones repetitivas o significantes o atentados de accesos deben ser reportados al gerente a cargo de la persona y al área de seguridad de la información.

Seguridad de contraseñas

Todas las contraseñas deben tener una longitud mínima de ocho (8) caracteres y no debencontener espacios en blanco. Las contraseñas deben ser difíciles de adivinar. Palabras de diccionario, identificadores de usuario y secuencias comunes de caracteres, tales como “12345678” o “QWERTY”, no deben ser empleadas. Así mismo, detalles personales como los nombres de familiares, número de documento de identidad, número de teléfono o fechas de cumpleaños no deben ser usadas salvo acompañados con otros caracteres adicionales que no tengan relación directa. Las contraseñas deben incluir al menos un carácter no alfanumérico. Las contraseñas deben contener al menos un carácter alfabéticoen mayúscula y uno en minúscula.

Todas las contraseñas deben expirar dentro de un periodo que no exceda los noventa (90) días. Cada gerente debe determinar un máximo periodo de vigencia de las contraseñas, elcual es recomendable no sea menos de (30) días. No debe permitirse la reutilización de ninguna de las 5 últimas contraseñas. Esto asegura que los usuarios no utilicen las mismascontraseñas en intervalos

regulares. Los usuarios no deben poder cambiar sus contraseñasmás de una vez al día. A los usuarios con privilegios administrativos, no se les debe permitir la reutilización de las últimas 13 contraseñas.

Todos los empleados ediles están obligados a proteger sus contraseñas, debiéndose seguirlas siguientes regulaciones: Bajo ninguna circunstancia, se debe escribir las contraseñas en papel, o almacenarlas en medios digitales no encriptados. Las contraseñas no deben ser divulgadas a ningún otro usuario salvo bajo el pedido de un gerente, con autorizacióndel área de seguridad informática y auditoría interna. Si se divulga la contraseña, esta debe ser cambiada durante el próximo ingreso. El usuario autorizado es responsable de todas las acciones realizadas por alguna persona a quién se le ha comunicado la contraseña o identificador de usuario. Los sistemas no deben mostrar la contraseña en pantalla o en impresiones, para prevenir que éstas sean observadas o recuperadas. Las contraseñas deben estar siempre encriptados cuando se encuentren almacenadas o cuando sean transmitidas a través de redes. El control de acceso a archivos, bases de datos, computadoras y otros sistemas de recursos mediante contraseñas compartidas está prohibido.

Los empleados deben tener acceso únicamente al conjunto de transacciones en línea requeridas para ejecutar sus tareas asignadas. Este conjunto de transacciones debe estar claramente definido para prevenir alguna ocurrencia de fraude y malversación. El acceso para la ejecución de transacciones sensibles debe ser controlado mediante una adecuada segregación de tareas. Por ejemplo, los usuarios que tengan permiso para registrar instrucciones de pago no deben poder verificar o aprobar su propio trabajo.

Es responsabilidad del propietario de la información y de los administradores de sistemas ver que los privilegios de acceso estén alineados con las necesidades del negocio, sean asignados basándose en requerimientos y que se comunique la lista correcta de accesos al Área de Informática. En las situaciones donde los usuarios con accesos a informaciónaltamente sensible sean despedidos, los supervisores deben coordinar directamente con el área de seguridad informática para eliminar el acceso de ese usuario. Se debe buscar el desarrollo de soluciones técnicas para evitar el uso de accesos privilegiados

innecesarios. Luego del despido o renuncia de algún empleado, es responsabilidad del jefe del empleado revisar cualquier archivo físico o digital elaborado o modificado por el usuario. El gerente debe también asignar la propiedad de dicha información a la persona relevante,así como determinar la destrucción de los archivos innecesarios.

Todos los usuarios que tienen acceso a las cuentas privilegiadas deben tener sus propias cuentas personales para uso del negocio. Por ende, los administradores de sistemas y empleados con acceso a cuentas privilegiadas deben usar sus cuentas personales para realizar actividades de tipo no privilegiadas. Las cuentas de usuario que no son utilizadaspor noventa (90) días deben ser automáticamente deshabilitadas. Las cuentas que no hansido utilizadas por un periodo largo demuestran que el acceso de información de ese

sistema no es necesario. Los custodios de la información deben informar al propietario de la información la existencia de las cuentas inactivas. Todos los accesos a los sistemasde información deben estar controlados mediante un método de autenticación incluyendouna combinación mínima de identificador de usuario/contraseña. Dicha combinación debe proveer la verificación de la identidad del usuario.

Control de acceso a redes

Los sistemas de red son vulnerables y presentan riesgos inherentes a su naturaleza y complejidad. Los accesos remotos y conexiones con redes externas, exponen a los sistemas de la Municipalidad a niveles mayores de riesgo. Asegurando que todos los enlaces de una red cuenten con adecuados niveles de seguridad, se logra que los activos más valiosos de las unidades de negocio estén protegidos de un ataque directo o indirecto.Todas las conexiones realizadas entre la red interna de la municipalidad e Internet, deben ser controladas por un firewall para prevenir accesos no autorizados. El área de seguridad de información debe aprobar todas las conexiones con redes o dispositivos externos.

El acceso desde Internet hacia la red interna de la municipalidad no debe ser permitido sin un dispositivo de fuerte autenticación o certificado basado en utilización de contraseñas dinámicas. El esquema de direccionamiento interno de la red no debe ser visible desde redes o equipos externos. Esto evita que "hackers" u otras personas puedenobtener fácilmente información sobre la estructura de red de la municipalidad y computadoras internas. Los accesos a los recursos de información deben solicitar como mínimo uno de los tres factores de autenticación: Factor de conocimiento: algo que solo el usuario conoce. Contraseña o PIN. Factor biométrico: algo propio de las características biológicas del usuario. Lectores de retina o identificadores de voz.

Las estaciones de trabajo y computadoras personales deben ser bloqueadas mediante la facilidad del sistema operativo, mientras se encuentren desatendidas. Todas las conexiones de red internas y externas deben cumplir con el marco de Seguridad de la Municipalidad sobre servicios de red y control de acceso. Es responsabilidad del área desistemas de información y seguridad de información determinar lo siguiente: Elementos de la red que pueden ser accedidos. El procedimiento de autorización para la obtención de acceso. Controles para la protección de la red.

Todos los servicios habilitados en los sistemas deben contar con una justificacióncoherente con las necesidades de las funciones administrativas u operativas de losusuarios. Los riesgos asociados a los servicios de red deben determinarse y ser resueltos antes de la implementación del servicio. Está prohibido conectar sin permiso a los recursos informáticos del sistema de información municipal. Está prohibido conectarse alsistema de información municipal a través de otros medios que no sean los definidos por los responsables del sistema.

Está prohibido intentar obtener información que no le compete, tampoco a la documentación confidencial de la municipalidad. Está totalmente prohibido intentar acceder a áreas restringidas de los Sistemas de Información o del sistema de información de la municipal. Está totalmente prohibido hacer intento o descifrar las claves, sistemas oalgoritmos de cifrado y cualquier otro

elemento de seguridad que intervenga en los procesos telemáticos. Está prohibido ingresar a las redes sociales sin previa autorizaciónde la autoridad correspondiente. La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Lo autoriza el personal que tiene la autoridadpara ello.

Control de acceso al sistema operativo

Los usuarios que posean privilegios de súper usuario, deben utilizar el mismo identificador con el que se autentican normalmente en los sistemas. Los administradoresdeben otorgarle los privilegios especiales a los identificadores de los usuarios que lo necesiten. Todos los usuarios deben poseer un único identificador. El uso de identificadores de usuario compartidos debe estar sujeto a autorización. Cada cuenta de usuario debe poseer una contraseña asociada, la cual solo debe ser conocida por el dueño del identificador de usuario.

Seguridad adicional puede ser añadida al proceso, como identificadores biométricos o generadores de contraseñas dinámicas. Las aplicaciones críticas deben estar sujetas a 8 periodos de acceso restringidos, el acceso a los sistemas en un horario distinto debe ser deshabilitado o suspendido. Los sistemas, durante el proceso de autenticación, deben mostrar avisos preventivos sobre los accesos no autorizados a los sistemas. Los identificadores de los usuarios deben ser bloqueados luego de 3 intentos fallidos de autenticación en los sistemas, el desbloqueo de la cuenta debe ser realizado manualmentepor el administrador del sistema.

Los sistemas deben ser configurados para no mostrar ninguna información que pueda facilitar el acceso a los mismos, luego de intentos fallidos de autenticación.

Control de acceso de aplicación

Para la generación de cuentas de usuario en los sistemas, así como para la asignación de perfiles, el gerente del área usuaria es el responsable de presentar

la Solicitud de Usuariosy/o Perfiles de Acceso a los Sistemas de Cómputo, al área de Seguridad Informática, quien generará los Usuarios y Contraseñas correspondientes, para luego remitirlas a Unidad de Capacidades Humanas, para que éste a su vez los entregue al Usuario Final, con la confidencialidad requerida.

Se debe otorgar a los usuarios acceso solamente a la información mínima necesaria parala realización de sus labores. Esta tarea puede ser realizada utilizando una combinación de: Seguridad lógica de la aplicación. Ocultar opciones no autorizadas en los sistemas. Restringir el acceso a línea de comando. Limitar los permisos a los archivos de los sistemas (solo lectura). Controles sobre la información de salida de los sistemas (reportes,consultas en línea, etc.)

Los sistemas que procesan información muy crítica deben ser aislados físicamente de sistemas que procesan información menos crítica. Los relojes de todos los sistemas debenser sincronizados para asegurar la consistencia de todos los registros de auditoría. Los administradores de los sistemas deben realizar monitoreo periódico de los sistemas comoparte de su rutina diaria de trabajo, este monitoreo no debe estar limitado solamente a la utilización y performance del sistema sino debe incluir el monitoreo del acceso de los usuarios a los sistemas. La actividad de los usuarios vinculada al acceso a información clasificada como “Confidencial o “Integridad”, debe ser registrada para su posterior inspección. El propietario de la información debe revisar dicho registro mensualmente.

Seguridad respecto a computación móvil y teletrabajo

Los usuarios que realizan trabajo en casa con información de la municipalidad, pueden tener el concepto errado de que la seguridad de información solo es aplicable en el trabajoen oficina, sin tomar en cuenta que algunas amenazas de seguridad son comunes en ambosentornos de trabajo y que incluso existen algunas nuevas amenazas en el trabajo en casa.La utilización de programas para el control remoto de equipos está prohibida a menos quese cuente con el consentimiento formal del administrador de seguridad. La utilización

inapropiada de este tipo de programas puede facilitar el acceso de un intruso a los sistemasde información de la municipalidad.

Medidas de seguridad adicionales deben ser implementadas para proteger la informaciónalmacenada en dispositivos móviles. Entre las medidas a tomarse se deben incluir: Encriptación de los datos. Contraseñas de encendido. Concientización de usuarios.Protección de la data transmitida hacia y desde dispositivos móviles. Medidas de autenticación adicionales para obtener acceso a la red de datos.

Con el propósito de evitar los problemas relacionados a virus informáticos y propiedad de los datos existentes en computadoras externas, solamente equipos de la municipalidaddeben ser utilizados para ser conectados a su red de datos. La única excepción a este puntoes la conexión hacia el servidor de correo electrónico para recepción y envío del correo electrónico.

Responsabilidades personales

Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado. Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros. Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario. Si un usuario tiene sospechas de que su

acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato y éste reportar al responsable de la administración de la red.

En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 30 días. En caso contrario, se le podrá denegar el acceso y se deberá contactar con el jefe inmediato para solicitar al administrador de la reduna nueva clave. El usuario debe proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren

contenidos los datos. Los usuarios sólo podrán crear archivos que contengan datos de carácter personal para un uso temporal y siempre necesario para el desempeño de su trabajo.

Los archivos temporales nunca serán ubicados en unidades locales de disco de la computadora de trabajo y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon. Los usuarios deben notificar a su jefe inmediato cualquier incidencia que detecten que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de listados y USB, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos. Los usuarios únicamente introducirán datos identificativos y direcciones o teléfonos de personas en las agendas de contactos de las herramientas ofimáticas (por ejemplo, en Outlook)

Uso apropiado de los recursos

Los Recursos Informáticos, Datos, Software, sistema de red están disponibles exclusivamente para cumplimentar las obligaciones y propósito de los procesos operativos. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso. Está prohibido el uso de estos recursos para actividades no relacionados con el propósito del negocio, o bien con la extralimitación en su uso. Están prohibidos las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los Estándares de los Recursos Informáticos propios de la municipalidad.

Está prohibido introducir en los Sistemas de Información o la Red Corporativa contenidosobscenos, amenazadores, inmorales u ofensivos. Está prohibido introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos. El personal contratadopor la municipalidad tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los Sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.

Está prohibido intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos. Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo. Cualquier archivo introducido en la red corporativa o en el puesto de trabajo del usuario a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual del control de virus. Todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados. Está prohibido poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, ni dañar o alterar los recursos informáticos.

Anexo 06 Procesamiento de datos

Seguridad de la información: antes confidencial

Tabla 18. cantidad de usuarios autorizados

01. ¿Cómo Valora la confidencialidad respecto a la cantidad de usuarios autorizados como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?		
RESPUESTA	**f**	**h**
Malo	14	50.0
Regular	5	17.9
Normal	6	21.4
Bueno	2	7.1
Excelente	1	3.6
TOTAL	**28**	**100.0**

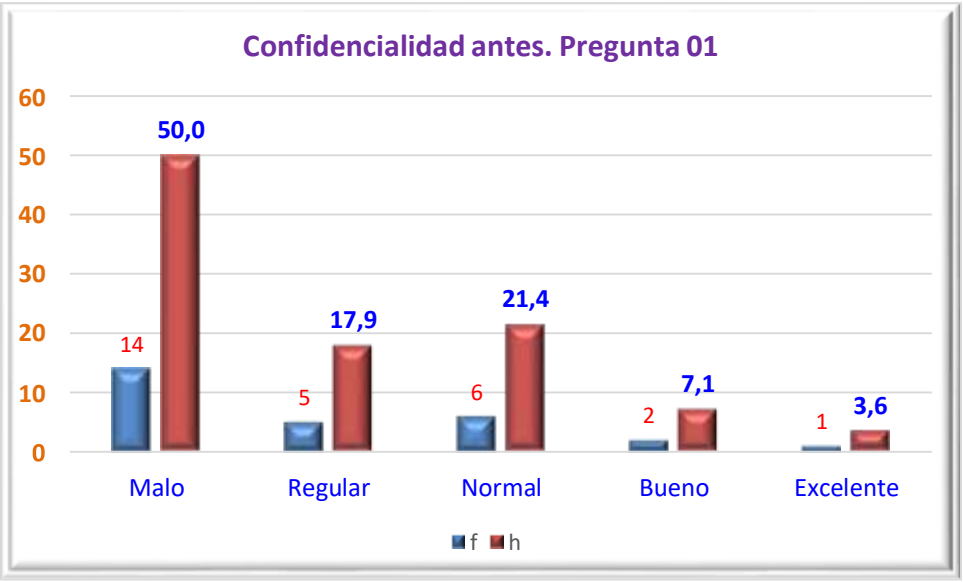


Figura 3. cantidad de usuarios autorizados

Ante la pregunta 1 sobre cómo Valora la confidencialidad respecto a la cantidad de usuarios autorizados como medida de seguridad en la Municipalidad Provincial de Yungay, 2021; 14 encuestados (50.0%) indicaron malo, 05 encuestados (17.9%) regular, 06 encuestados (21.4%) señalaron normal, 02 de los encuestados (7.1%)señalaron bueno y 01 de ellos (3.6%) indicaron excelente.

Tabla 19. cantidad de información confidencial accesible

02. ¿Cómo califica la confidencialidad con referencia a la cantidad de información confidencial accesible como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?		
RESPUESTA	**f**	**h**
Malo	13	46.4
Regular	7	25.0
Normal	4	14.3
Bueno	3	10.7
Excelente	1	3.6
TOTAL	**28**	**100.0**

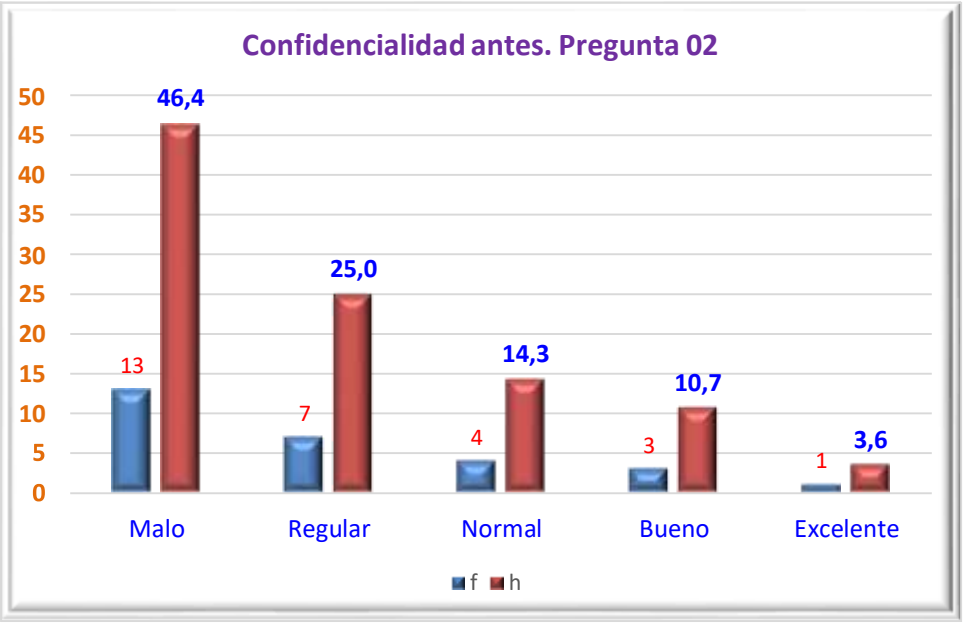


Figura 4. cantidad de información confidencial accesible

Ante la pregunta 2 sobre cómo califica la confidencialidad con referencia a la cantidad de información confidencial accesible como medida de seguridad en la Municipalidad Provincial de Yungay, 2021; 13 encuestados (46.4%) indicaron malo, 07 encuestados (25.0%) regular, 04 encuestados (14.3%) señalaron normal, 03 de los encuestados (10.7%) señalaron bueno y 01 de ellos (3.6%) indicaron excelente.

Tabla 20. cantidad de información confidencial hackeados

03. ¿Cómo evalúa la confidencialidad en la cantidad de información confidencial hackeados como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?		
RESPUESTA	**f**	**h**
Malo	15	53.6
Regular	4	14.3
Normal	4	14.3
Bueno	3	10.7
Excelente	2	7.1
TOTAL	**28**	**100.0**

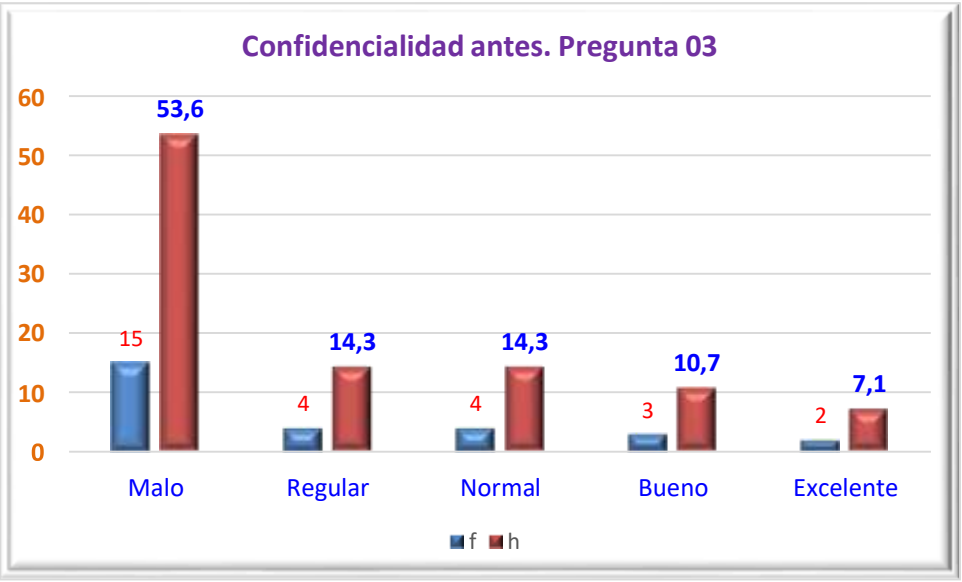


Figura 5. cantidad de información confidencial hackeados

Ante la pregunta 3 sobre cómo evalúa la confidencialidad en la cantidad de información confidencial hackeados como medida de seguridad en la Municipalidad Provincial de Yungay, 2021; 15 encuestados (53.6%) indicaron malo, 04 encuestados (14.3%) regular, 04 encuestados (14.3%) señalaron normal, 03 de los encuestados (10.7%) señalaron bueno y 02 de ellos (7.1%) indicaron excelente.

Tabla 21. cantidad de información confidencial recuperados

04. ¿Cómo valora la confidencialidad sobre la cantidad de información confidencial recuperados como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?		
RESPUESTA	**f**	**h**
Malo	13	46.4
Regular	6	21.4
Normal	5	17.9
Bueno	3	10.7
Excelente	1	3.6
TOTAL	**28**	**100.0**

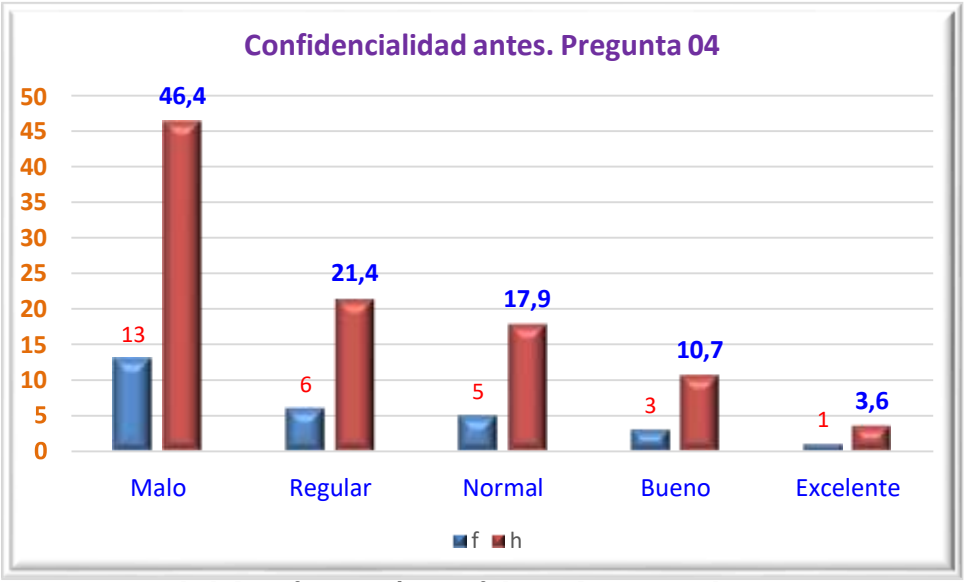


Figura 6. cantidad de información confidencial recuperados

Ante la pregunta 4 sobre cómo valora la confidencialidad sobre la cantidad deinformación confidencial recuperados como medida de seguridad en la Municipalidad Provincial de Yungay, 2021; 13 encuestados (46.4%) indicaron malo, 06 encuestados (21.4%) regular, 05 encuestados (17.9%) señalaron normal, 03 de los encuestados (10.7%) señalaron bueno y 01 de ellos (3.6%) indicaron excelente.

Tabla 22. referencia grado de daño causado por el acceso a la información

05. ¿Cómo valora la confidencialidad con referencia grado de daño causado por el acceso a la información confidencial como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?		
RESPUESTA	**f**	**h**
Malo	10	35.7
Regular	7	25.0
Normal	6	21.4
Bueno	4	14.3
Excelente	1	3.6
TOTAL	**28**	**100.0**

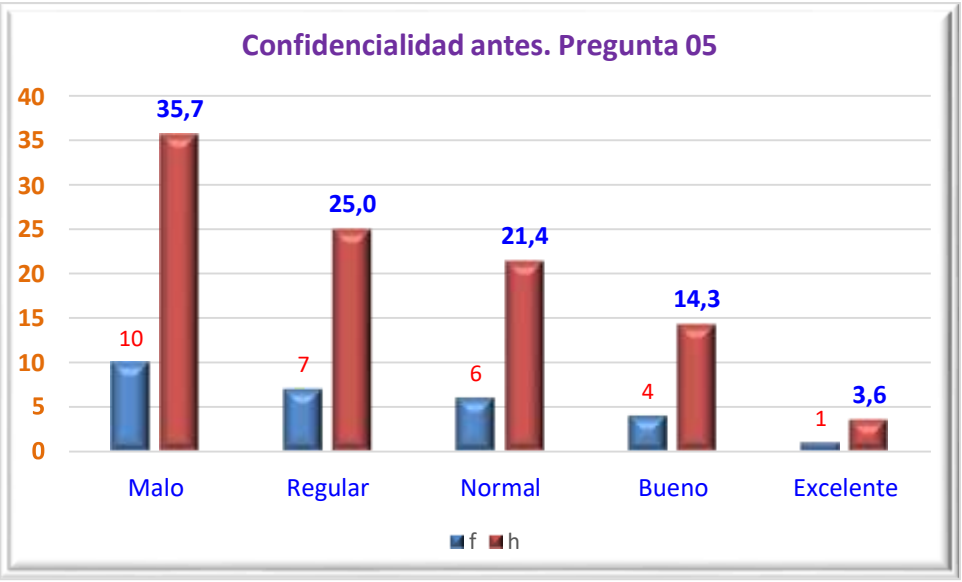


Figura 7. referencia grado de daño causado por el acceso a la información

Ante la pregunta 5 sobre cómo valora la confidencialidad con referencia grado de daño causado por el acceso a la información confidencial como medida de seguridad en la Municipalidad Provincial de Yungay, 2021; 10 encuestados (35.7%) indicaron malo, 07 encuestados (25.0%) regular, 06 encuestados (21.4%) señalaron normal, 04 de los encuestados (14.3%) señalaron bueno y 01 de ellos (3.6%) indicaron excelente.

Integridad

Tabla 23. cantidad de información que debe mantenerse integro

06. ¿Cómo valora la integridad de la cantidad de información que debe mantenerse integro como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?		
RESPUESTA	**f**	**h**
Malo	10	35.7
Regular	12	42.9
Normal	4	14.3
Bueno	1	3.6
Excelente	1	3.6
TOTAL	**28**	**100.0**

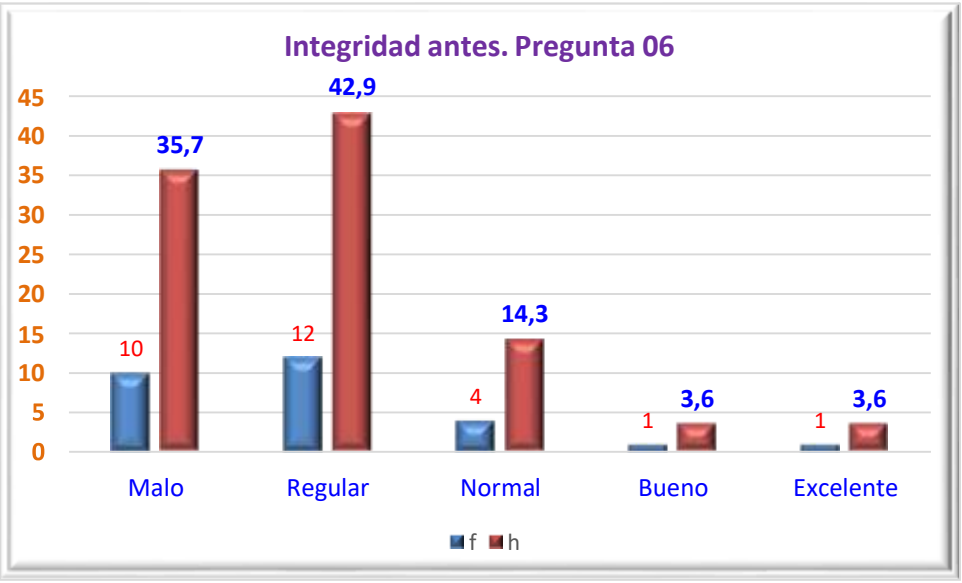


Figura 8. cantidad de información que debe mantenerse integro

Ante la pregunta 6 sobre cómo valora la integridad de la cantidad de información que debe mantenerse integro como medida de seguridad en la Municipalidad Provincial de Yungay, 2021; 10 encuestados (35.7%) indicaron malo, 12 encuestados (42.9%) regular, 04 encuestados (14.3%) señalaron normal, 01 de los encuestados (3.6%) señalaron bueno y 01 de ellos (3.6%) indicaron excelente

Tabla 24. cantidad de información no íntegros

07. ¿Cómo evalúa la integridad sobre la cantidad de información no íntegros como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?		
RESPUESTA	**f**	**h**
Malo	10	35.7
Regular	9	32.1
Normal	5	17.9
Bueno	2	7.1
Excelente	2	7.1
TOTAL	**28**	**100.0**

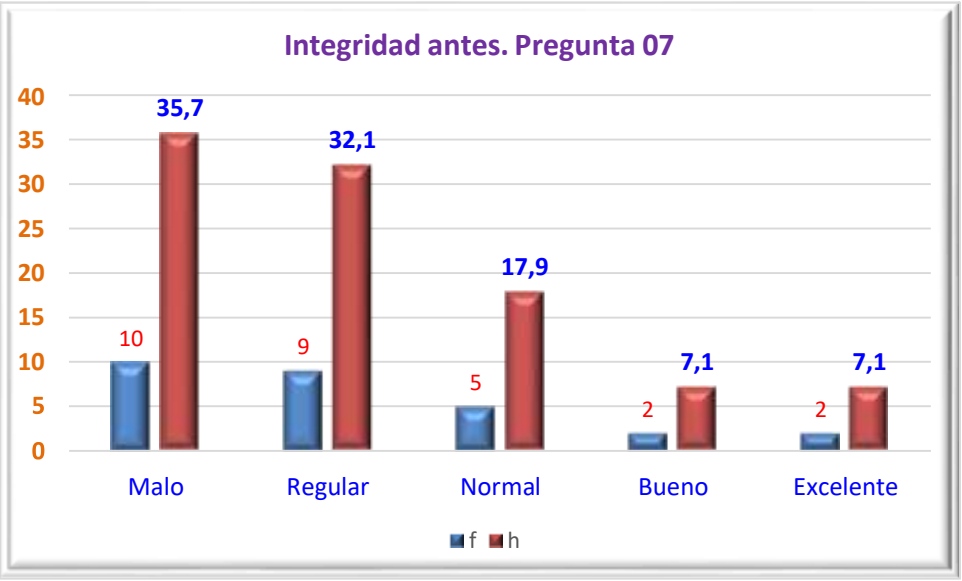


Figura 9. cantidad de información no íntegros

Ante la pregunta 7 sobre cómo evalúa la integridad sobre la cantidad de información no íntegros como medida de seguridad en la Municipalidad Provincial de Yungay, 2021; 10 encuestados (35.7%) indicaron malo, 9 encuestados (32.1%) regular, 05 encuestados (17.9%) señalaron normal, 02 de los encuestados (7.1%) señalaron bueno y 02 de ellos (7.1%) indicaron excelente.

Tabla 25. referencia al nivel de integridad de fuentes de información

08. ¿Cómo considera la integridad con referencia al nivel de integridad de fuentes de información como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?		
RESPUESTA	**f**	**h**
Malo	9	32.1
Regular	9	32.1
Normal	6	21.4
Bueno	3	10.7
Excelente	1	3.6
TOTAL	**28**	**100.0**

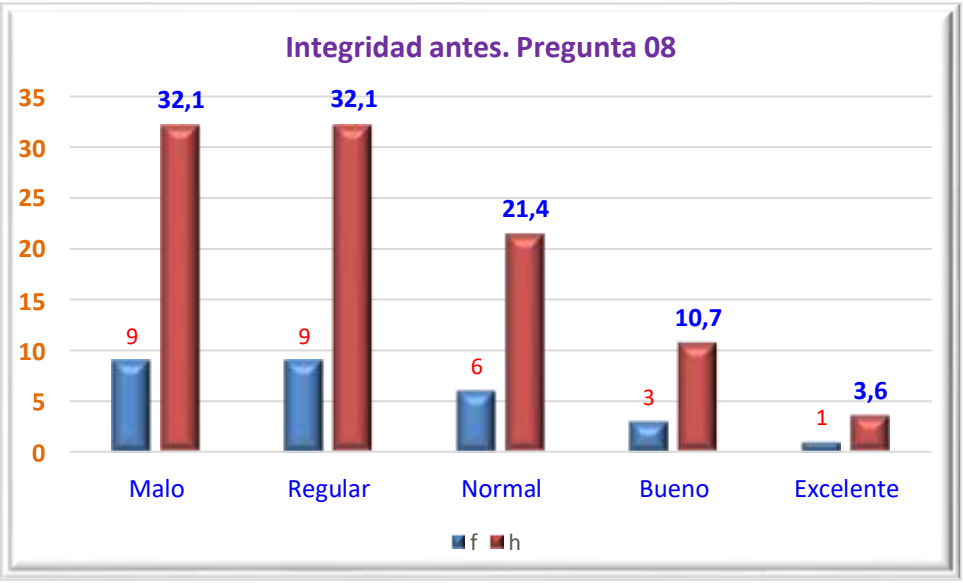


Figura 10. cantidad de información no íntegros

Ante la pregunta 8 sobre cómo considera la integridad con referencia al nivel de integridad de fuentes de información como medida de seguridad en la Municipalidad Provincial de Yungay, 2021; 9 encuestados (32.1%) indicaron malo, 9 encuestados (32.1%) regular, 06 encuestados (21.4%) señalaron normal, 03 de los encuestados (10.7%) señalaron bueno y 01 de ellos (3.6%) indicaron excelente

Tabla 26. cantidad de información recuperados de su integridad

09. ¿Cómo califica la integridad respecto a la cantidad de información recuperados de su integridad como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?		
RESPUESTA	**f**	**h**
Malo	12	42.9
Regular	9	32.1
Normal	4	14.3
Bueno	1	3.6
Excelente	2	7.1
TOTAL	**28**	**100.0**

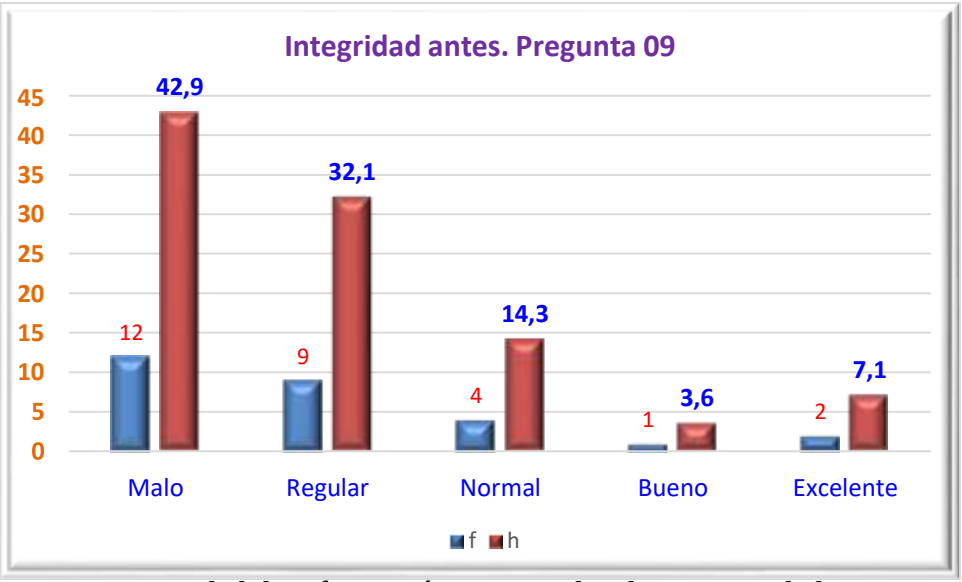


Figura 11. cantidad de información recuperados de su integridad

Ante la pregunta 9 sobre cómo califica la integridad respecto a la cantidad de información recuperados de su integridad como medida de seguridad en la Municipalidad Provincial de Yungay, 2021; 12 encuestados (42.9%) indicaron malo, 9 encuestados (32.1%) regular, 04 encuestados (14.3%) señalaron normal, 01 de los encuestados (3.6%) señalaron bueno y 02 de ellos (7.1%) indicaron excelente.

Tabla 27. nivel de daño causado

10. ¿Cómo califica la integridad del nivel de daño causado por falta a la integridad de la información en la Municipalidad Provincial de Yungay, 2021?		
RESPUESTA	**f**	**h**
Malo	10	35.7
Regular	8	28.6
Normal	5	17.9
Bueno	3	10.7
Excelente	2	7.1
TOTAL	**28**	**100.0**

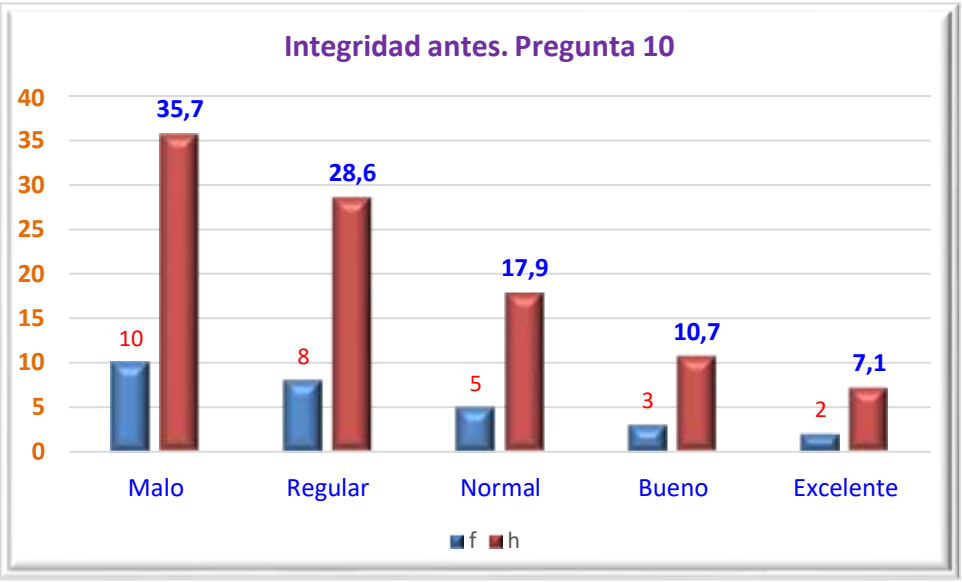


Figura 12. nivel de daño causado

Ante la pregunta 10 sobre cómo califica la integridad del nivel de daño causado por falta a la integridad de la información en la Municipalidad Provincial de Yungay, 2021; 10 encuestados (35.7%) indicaron malo, 08 encuestados (28.6%) regular, 05 encuestados (17.9%) señalaron normal, 03 de los encuestados (10.7%) señalaron bueno y 02 de ellos (7.1%) indicaron excelente

Disponibilidad

Tabla 28. cantidad de información disponible

11. ¿Cómo valora la disponibilidad sobre la cantidad de información disponible como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?		
RESPUESTA	**f**	**h**
Malo	12	42.9
Regular	7	25.0
Normal	5	17.9
Bueno	3	10.7
Excelente	1	3.6
TOTAL	**28**	**100.0**

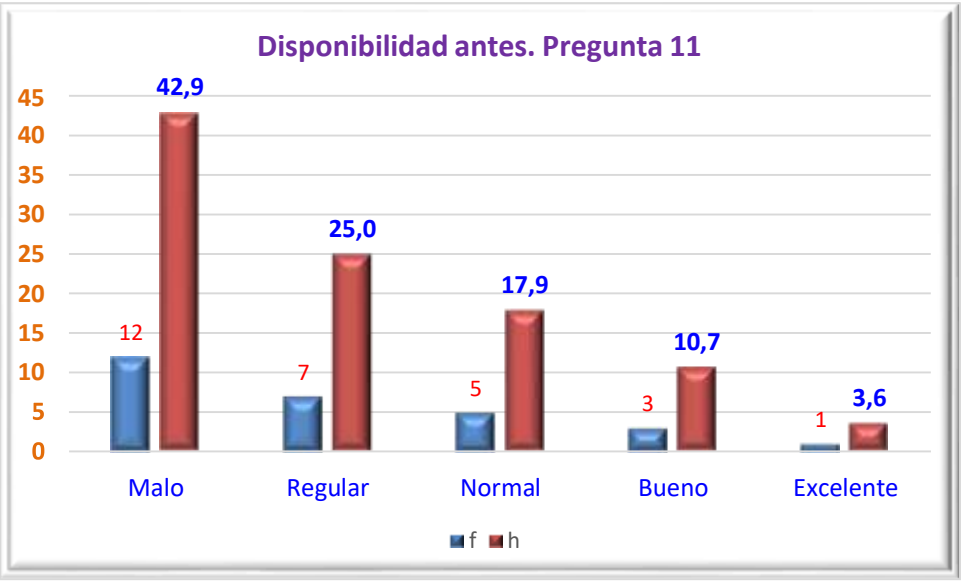


Figura 13. cantidad de información disponible

Ante la pregunta 11 sobre cómo valora la disponibilidad sobre la cantidad de información disponible como medida de seguridad en la Municipalidad Provincial deYungay, 2021; 12 encuestados (42.9%) indicaron malo, 07 encuestados (25.0%) regular, 05 encuestados (17.9%) señalaron normal, 03 de los encuestados (10.7%) señalaron bueno y 01 de ellos (3.6%) indicaron excelente

Tabla 29. cantidad de información no disponible

12. ¿Cómo evalúa la disponibilidad de la cantidad de información no disponible como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?		
RESPUESTA	**f**	**h**
Malo	10	35.7
Regular	9	32.1
Normal	6	21.4
Bueno	2	7.1
Excelente	1	3.6
TOTAL	**28**	**100.0**

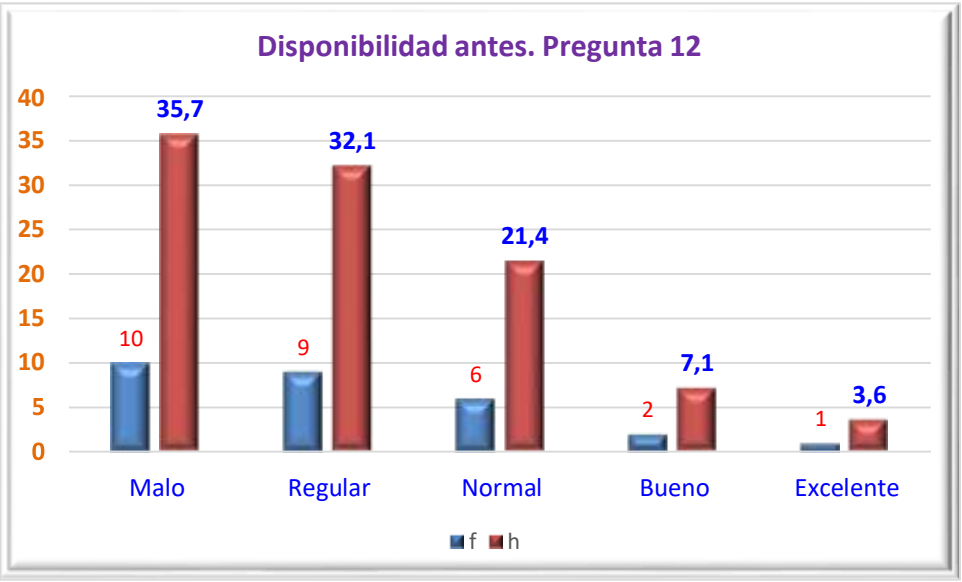


Figura 14. cantidad de información no disponible

Ante la pregunta 12 sobre cómo evalúa la disponibilidad de la cantidad de información no disponible como medida de seguridad en la Municipalidad Provincial de Yungay, 2021; 10 encuestados (35.7%) indicaron malo, 09 encuestados (32.1%) regular, 06 encuestados (21.4%) señalaron normal, 02 de los encuestados (7.1%) señalaron buenoy 01 de ellos (3.6%) indicaron excelente.

Tabla 30. referencia al nivel de disponibilidad

13. ¿Cómo considera la disponibilidad con referencia al nivel de disponibilidad de la información como medida de seguridad en la Municipalidad Provincial de Yungay, 2021?		
RESPUESTA	**f**	**h**
Malo	9	32.1
Regular	8	28.6
Normal	6	21.4
Bueno	3	10.7
Excelente	2	7.1
TOTAL	**28**	**100.0**

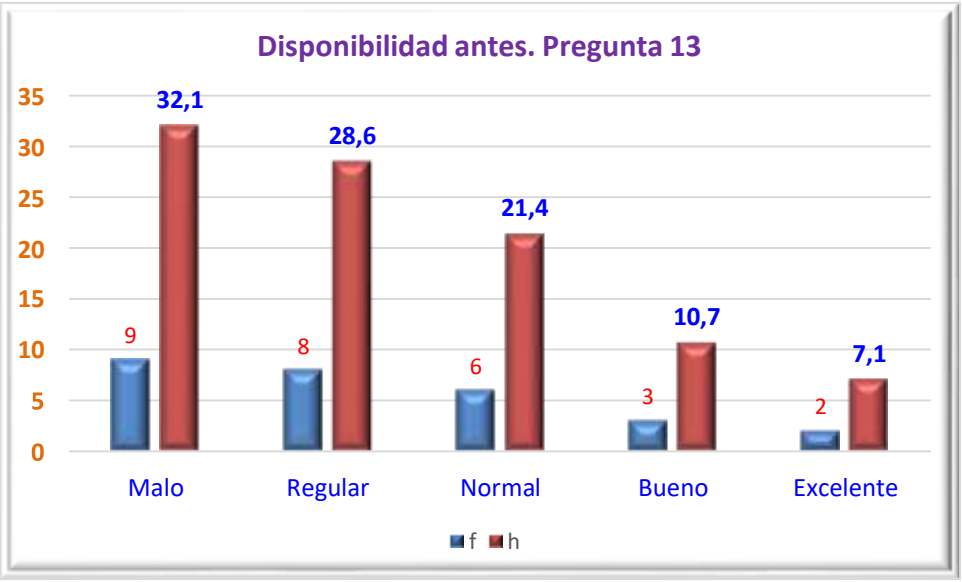


Figura 15. referencia al nivel de disponibilidad

Ante la pregunta 13 sobre cómo considera la disponibilidad con referencia al nivel de disponibilidad de la información como medida de seguridad en la Municipalidad Provincial de Yungay, 2021; 09 encuestados (32.1%) indicaron malo, 08 encuestados (28.4%) regular, 03 encuestados (10.7%) señalaron normal, 02 de los encuestados (7.1%) señalaron bueno y 01 de ellos (3.6%) indicaron excelente

Tabla 31. cantidad de información no disponibles recuperados

14. ¿Cómo califica la disponibilidad sobre la cantidad de información no disponibles recuperados en la Municipalidad Provincial de Yungay, 2021?		
RESPUESTA	**f**	**h**
Malo	11	39.3
Regular	8	28.6
Normal	5	17.9
Bueno	2	7.1
Excelente	2	7.1
TOTAL	**28**	**100.0**

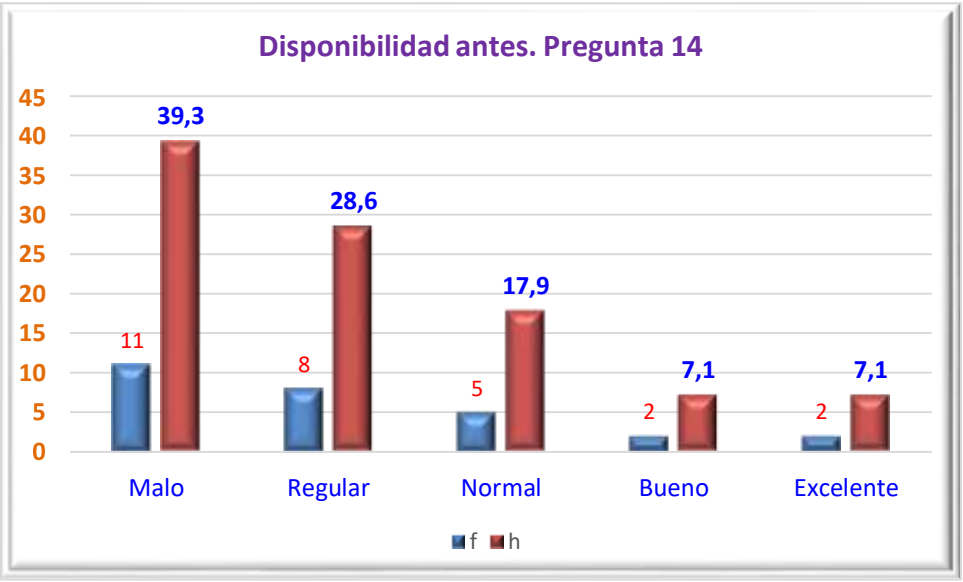


Figura 16. cantidad de información no disponibles recuperados

Ante la pregunta 14 sobre cómo califica la disponibilidad sobre la cantidad deinformación no disponibles recuperados en la Municipalidad Provincial de Yungay, 2021; 11 encuestados (39.3%) indicaron malo, 08 encuestados (28.6%) regular, 05 encuestados (17.9%) señalaron normal, 02 de los encuestados (7.1%) señalaron bueno y 02 de ellos (7.1%) indicaron excelente.

Tabla 32. referencia al nivel de daño causado

15. ¿Cómo valora la disponibilidad con referencia al nivel de daño causado por la no disponibilidad de la información en la Municipalidad Provincial de Yungay, 2021?		
RESPUESTA	**f**	**h**
Malo	9	32.1
Regular	6	21.4
Normal	7	25.0
Bueno	4	14.3
Excelente	2	7.1
TOTAL	**28**	**100.0**

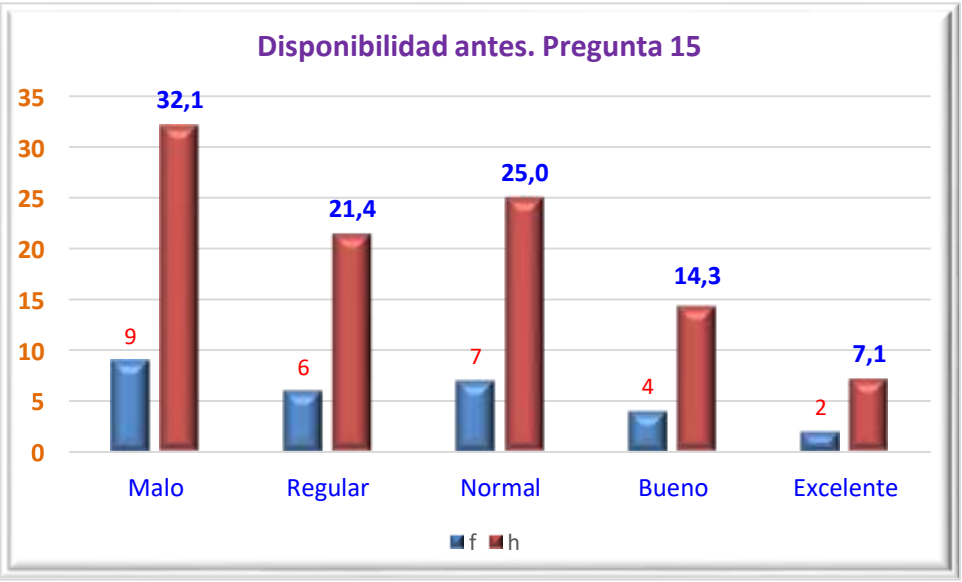


Figura 17. referencia al nivel de daño causado

Ante la pregunta 15 sobre cómo valora la disponibilidad con referencia al nivel de daño causado por la no disponibilidad de la información en la Municipalidad Provincial de Yungay, 2021; 09 encuestados (32.1%) indicaron malo, 06 encuestados (21.4%) regular, 07 encuestados (25.0%) señalaron normal, 04 de los encuestados (14.3%) señalaron bueno y 02 de ellos (7.1%) indicaron excelente.

FORMATO DE PUBLICACIÓN EN REPOSITORIO

USP
UNIVERSIDAD SAN PEDRO

REPOSITORIO INSTITUCIONAL DIGITAL

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE DOCUMENTOS DE INVESTIGACIÓN

1. Información del Autor

Apellidos y Nombres	DNI	Correo Electrónico
Cochachin Jara Silva Soledad	72098183	silvia150691@gmail.com

2. Tipo de Documento de Investigación

X Tesis	Trabajo de Suficiencia Profesional	Trabajo Académico	Trabajo de Investigación

3. Grado Académico o Título Profesional [1]

Bachiller	X Título Profesional	Título Segunda Especialidad	Maestría	Doctorado

4. Título del Documento de Investigación

"Modelo de Seguridad informatica para la seguridad de la informacion: Municipalidad Provincial de Yungay, 2021"

5. Programa Académico

Ingeniería Informatica y Sistemas

6. Tipo de Acceso al Documento

X Abierto o Público [2] (info:eu-repo/semantics/openAccess)	Acceso restringido [3] (info:eu-repo/semantics/restrictedAccess) (*)	
(*) En caso de restringido sustentar motivo		

A. Originalidad del Archivo Digital

Por el presente dejo constancia que el archivo digital que entrego a la Universidad, es la versión final del trabajo de investigación sustentado y aprobado por el Jurado Evaluador y forma parte del proceso que conduce a obtener el grado académico o título profesional.

B. Otorgamiento de una licencia CREATIVE COMMONS [5]

El autor, por medio de este documento, autoriza a la Universidad, publicar su trabajo de investigación en formato digital en el Repositorio Institucional Digital, al cual se podrá acceder, preservar y difundir de forma libre y gratuita, de manera íntegra a todo el documento. [6]

Lugar	Día	Mes	Año
Chimbote	22	08	2023

Huella Digital

Firma

Importante

1. Según Resolución de Consejo Directivo N° 033-2016-SUNEDU-CD, Reglamento del Registro Nacional de Trabajos de Investigación para optar Grados Académicos y Títulos Profesionales, Art. 8, inciso 8.2.
2. Ley N° 30035. Ley que regula el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto y D.S. 006-2015-PCM.
3. Si el autor eligió el tipo de acceso abierto o público, otorga a la Universidad San Pedro una licencia no exclusiva, para que se pueda hacer arreglos de forma en la obra y difundir en el Repositorio Institucional Digital. Respetando siempre los Derechos de Autor y Propiedad Intelectual de acuerdo y en el Marco de la Ley 822.
4. En caso de que el autor elija la segunda opción, únicamente se publicará los datos del autor y resumen de la obra, de acuerdo a la directiva N° 004-2016-CONCYTEC-DEGC [Numerales 5.2 y 6.7] que norma el funcionamiento del Repositorio Nacional Digital
5. Las licencias Creative Commons (CC) es una organización internacional sin fines de lucro que pone a disposición de los autores un conjunto de licencias flexibles y de herramientas tecnológicas que facilitan la difusión de información, recursos educativos, obras artísticas y científicas, entre otros. Estas licencias también garantizan que el autor obtenga el crédito por su obra.
6. Según el inciso 12.2, del artículo 12° del Reglamento del Registro Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales-RENATI "Las universidades, instituciones y escuelas de educación superior tienen como obligación registrar todos los trabajos de investigación y proyectos, incluyendo los metadatos en sus repositorios institucionales precisando si son de acceso abierto o restringido, los cuales serán posteriormente recolectados por el Repositorio Digital RENATI, a través del Repositorio ALICIA".

Nota. - En caso de falsedad en los datos, se procederá de acuerdo a ley (Ley 27444, art. 32, núm. 32.3).

REPORTE DE SIMILITUD

Modelo de Seguridad informática para la seguridad de la información: Municipalidad Provincial de Yungay, 2021

INFORME DE ORIGINALIDAD

19%	19%	2%	7%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorioacademico.upc.edu.pe Fuente de Internet	2%
2	repositorio.ucv.edu.pe Fuente de Internet	1%
3	hdl.handle.net Fuente de Internet	1%
4	ri.uaemex.mx Fuente de Internet	1%
5	repositorio.unasam.edu.pe Fuente de Internet	1%
6	repositorio.uandina.edu.pe Fuente de Internet	1%
7	repositorio.untels.edu.pe Fuente de Internet	1%
8	laseguridaddelainformacionsoniafran.wordpress.com Fuente de Internet	1%
9	dspace.unitru.edu.pe Fuente de Internet	

		1 %
10	seguridadinforiuteb.blogspot.com Fuente de Internet	1 %
11	repositorio.usanpedro.edu.pe Fuente de Internet	<1 %
12	issuu.com Fuente de Internet	<1 %
13	cdn.www.gob.pe Fuente de Internet	<1 %
14	sites.google.com Fuente de Internet	<1 %
15	(3-7-15) http://181.65.148.115/transparencia/mof.pdf Fuente de Internet	<1 %
16	es.scribd.com Fuente de Internet	<1 %
17	repository.ucc.edu.co Fuente de Internet	<1 %
18	repositorio.unu.edu.pe Fuente de Internet	<1 %
19	repositorio.unne.edu.ar Fuente de Internet	1 %

20	Submitted to Universidad ESAN -- Escuela de Administración de Negocios para Graduados Trabajo del estudiante	<1 %
21	evavazb2tic.wordpress.com Fuente de Internet	<1 %
22	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	<1 %
23	idoc.pub Fuente de Internet	<1 %
24	repositorio.itm.edu.co Fuente de Internet	<1 %
25	repositorio.uladech.edu.pe Fuente de Internet	<1 %
26	docplayer.es Fuente de Internet	<1 %
27	www.chancaytours.com Fuente de Internet	<1 %
28	repository.unad.edu.co Fuente de Internet	<1 %
29	alicia.concytec.gob.pe Fuente de Internet	<1 %
30	1library.co Fuente de Internet	<1 %

31	repositorio.ups.edu.pe Fuente de Internet	<1 %
32	www.researchgate.net Fuente de Internet	<1 %
33	Submitted to Universidad Peruana de Las Americas Trabajo del estudiante	<1 %
34	repositorio.unheval.edu.pe Fuente de Internet	<1 %
35	Submitted to Instituto Superior de Artes, Ciencias y Comunicación IACC Trabajo del estudiante	<1 %
36	www.coursehero.com Fuente de Internet	<1 %
37	moam.info Fuente de Internet	<1 %
38	repositorio.uss.edu.pe Fuente de Internet	<1 %
39	www.revistasjdc.com Fuente de Internet	<1 %
40	Submitted to Universidad Nacional de Barranca Trabajo del estudiante	<1 %
41	www.umce.cl Fuente de Internet	<1 %

42	filadd.com Fuente de Internet	<1 %
43	Submitted to Universidad San Ignacio de Loyola Trabajo del estudiante	<1 %
44	muniyungay.gob.pe Fuente de Internet	<1 %
45	www.enpresadigitala.net Fuente de Internet	<1 %
46	infosegur.wordpress.com Fuente de Internet	<1 %
47	tesis.unap.edu.pe Fuente de Internet	<1 %
48	Submitted to Pontificia Universidad Catolica del Peru Trabajo del estudiante	<1 %
49	William-Rogelio Marchand-Nino, Hector Huaman Samaniego. "Information Security Culture Model. A Case Study", 2021 XLVII Latin American Computing Conference (CLEI), 2021 Publicación	<1 %
50	empleoarg.blogspot.com Fuente de Internet	<1 %
51	repositorio.tec.mx Fuente de Internet	<1 %

52	repositorio.unjfsc.edu.pe Fuente de Internet	<1 %
53	volcanchess.blogspot.com Fuente de Internet	<1 %
54	worldwidescience.org Fuente de Internet	<1 %
55	www.entrust.com Fuente de Internet	<1 %
56	Submitted to Universidad Privada San Pedro Trabajo del estudiante	<1 %
57	dspace.ucuenca.edu.ec Fuente de Internet	<1 %
58	www.science.gov Fuente de Internet	<1 %
59	Marlene Lucila Guerrero Julio, Carlos Uc Rios. "Evaluación del contexto organizacional en la gestión del riesgo de tecnología de información con un enfoque basado en COBIT", Revista de Investigación en Tecnologías de la Información, 2019 Publicación	<1 %
60	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	<1 %
61	belajaroffice2017.blogspot.com Fuente de Internet	<1 %

62	www.metamira.com Fuente de Internet	<1 %
63	www.muninuevochimbote.gob.pe Fuente de Internet	<1 %

Excluir citas	Apagado	Excluir coincidencias	< 10 words
Excluir bibliografía	Activo		