UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

"Sistema de Seguridad de la Información para el Centro de Operaciones, Emergencia y Monitoreo (COEM) de la Municipalidad Distrital de Bellavista - Sullana"

Tesis para obtener el Título Profesional de Ingeniero en Informática y de Sistemas

Autor

Pulache Rosales, Joan Isaac

Asesor:

Arroyo Tirado, Jorge Luis

Piura - Perú

2019

Palabras claves:

Tema	Seguridad de la Información
Especialidad	Gestión

Keyword:

Topic	Security of the information
Specialty	Management

Líneas de investigación:

Area	Ingeniería y Tecnología
Sub Area	Ingeniería Eléctrica, Electrónica e Informática.
Disciplina	Redes y Telecomunicaciones

Sistema de Seguridad de la Información para el Centro de Operaciones, Emergencia y Monitoreo (COEM) de la Municipalidad Distrital de Bellavista - Sullana

RESUMEN

La presente tesis tuvo por objetivo el desarrollo de un Sistema de Seguridad de la Información para el Centro de Operaciones, Emergencia y Monitoreo (COEM) de la Municipalidad Distrital de Bellavista – Sullana, para proteger los activos digitales que se procesan en dicha entidad pública.

En el desarrollo de la investigación se utilizó el marco de referencia de la Guía de los fundamentos para la dirección de Proyectos (PMBOK) de la Quinta edición, el cual es un marco de trabajo que contiene el estándar de proyectos para la investigación, se hará uso de la fases: Gestión de Integración, Gestión de Alcance y Gestión de Riesgos, la guía para la profesión de la dirección de proyectos en el ámbito de la seguridad informática, se hace uso del estándar ISO 27001: 2013 respecto a lo que se debe implementar para la seguridad de trabajadores y sobre todo de la población del distrito, lo cual garantizaría que los riesgos de los activos de información sean identificados, gestionados, minimizados y documentados. El cual cuenta con la suficiente flexibilidad para adaptarse a cualquier organización, pudiendo seleccionar los procesos a aplicar, modo y técnicas concretas, por lo que facilita el periodo de adaptación de nuevas incorporaciones al equipo de trabajo.

Se llevó a cabo encuestas al jefe del área y al personal del Centro de Operaciones, Emergencia y Monitoreo (COEM) y al jefe de la Unidad de Estadística y Tecnologías de la Información, la interpretación de sus resultados nos sirvió de apoyo para el desarrollo de los controles del ISO 27001:2013; llegando a establecer un conjunto de recomendaciones que favorezcan la implementación del Sistema de Gestión de la seguridad de la entidad pública.

ABSTRACT

The objective of this thesis was the development of an Information Security System for the Operations, Emergency and Monitoring Center (COEM) of the District Municipality of Bellavista - Sullana, to protect the digital assets that are processed in said public entity.

In the development of the research, the reference framework of the Fundamentals Guide for Project Management (PMBOK) of the Fifth Edition was used, which is a framework that contains the standard of projects for research. use of phases: Integration Management, Scope Management and Risk Management, the guide for the project management profession in the field of computer security, using the ISO 27001: 2013 standard regarding what should be done implement for the safety of workers and especially the population of the district, which would ensure that the risks of information assets are identified, managed, minimized and documented. Which has enough flexibility to adapt to any organization, being able to select the processes to apply, mode and specific techniques, so it facilitates the period of adaptation of new additions to the work team.

Surveys were carried out to the head of the area and to the personnel of the Operations, Emergency and Monitoring Center (COEM) and to the head of the Unit of Statistics and Information Technologies, the interpretation of their results served as support for the development of the controls of ISO 27001: 2013; arriving to establish a set of recommendations that favor the implementation of the security management system of the public entity.

ÍNDICE

I. INTRODUCCIÓN

Durante la revisión bibliográfica, se revisaron los antecedentes más relacionados con la presente investigación, entre los que figuran los que a continuación presento:

Se reviso la investigación de Camargo (2017) denominada "Diseño de un Sistemas de Gestión de la Seguridad de la Información (SGSI) en el Área Tecnológica de la Comisión Nacional del Servicio Civil – CNSC basado en la Norma ISO 27000 e ISO 27001", realiza en la Universidad Nacional Abierta y a Distancia, para optar la especialización en Seguridad Informática, recomienda la identificación de activos, la valoración y análisis de riesgos, se realizaron en base a la metodología Magerit v.3, permitiendo así detectar los activos críticos de la entidad, y el impacto que este puede ocasionar cuando se afecte este. Gracias al análisis de riesgos realizado se pudo realizar la declaración de aplicabilidad bajo el anexo A de la norma ISO/IEC 27001, permitiendo así identificar si aplica los controles que dicha norma sugiere, dando como resultado que existen muchos controles que no se encuentran aplicados a la entidad, identificándose que se encuentra en riesgo alto, por falta de controles. El recurso humano de la entidad, es uno de los riesgos más altos para la seguridad de la información, ya que, si no se tienen buenas prácticas y una divulgación acertada sobre la seguridad informática, la entidad puede tener un nivel alto de vulnerabilidad. Se es necesario establecer unas políticas de seguridad que sean aprobadas por los directivos de todas las áreas de la entidad, el cual permita y se garantice la implementación, actualización y cumplimiento de estas.

También se revisó el estudio de Berrío (2016) llamado "Metodología para la evaluación del desempeño de controles en sistemas de gestión de seguridad de la información sobre la norma ISO/IEC 27001", realiza en la Universidad Nacional de Colombia para optar el magister en ingeniería de sistemas, concluye que la implementación de un SGSI requiere estar a la vanguardia de las innovaciones tecnológicas en este aspecto, el área de tecnología si tiene un papel muy destacado, ya que debe proponer herramientas metodológicas tanto para la prevención como para la detección de riesgo relacionados con el aumento de vulnerabilidades informáticas, teniendo en cuenta que la mayoría de áreas de una compañía está conectada a la red.

En la tesis Barragán , Góngora y Martínez (2011) "Implementación de políticas de seguridad informática para la M.I. municipalidad de Guayaquil aplicando la norma ISO/IEC 27002",su objetivo fue formular un modelo de política de seguridad de la información que sirva de punto de partida para la elaboración de políticas

correspondientes tomando como base estándares internacionales, se decidió basar el modelo en la norma ISO/IEC 27002 , como un marco de referencias para la gestión de la seguridad de la información , concluyendo que la forma de conseguir el mayor beneficio en seguridad de la información es contar con una adecuada evaluación de riesgos, que oriente las inversiones, que minimicen el impacto en caso de incidentes , dando a conocer que la seguridad de la información no es una responsabilidad únicamente del área de tecnología , debe fluir desde la alta gerencia hacia todos los procesos de negocios. La presente tesis no apoyo en el alcance del objetivo de sus políticas generales en relación a la consideración de los accesos de los usuarios y de las condiciones del uso de las claves de acceso.

Además, se revisó la tesis de Agramonte (2016), que propuso la investigación de "Auditoría del sistema de seguridad de información en el hospital III José Cayetano Heredia – Castilla; 2016" realiza en Universidad Católica Los Ángeles de Chimbote, escuela profesional de ingeniería de sistemas para optar el título de ingeniero de sistemas en su propuesta de mejora sugiere para mejorar el nivel de la Seguridad Lógica en el Hospital III José Cayetano Heredia – Castilla; 2016, se cumpla mediante un proceso de administración de la seguridad los controles y políticas de seguridad definidas, también incluye realizar monitoreo de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados.

En otra investigación revisada es la De La Cruz (2016) en su investigación "Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la municipalidad provincial de Paita; 2016" realizada en la Universidad Católica Los Ángeles de Chimbote, la investigación tuvo como objetivo general, realizar la propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; en el año 2016. El tipo y diseño de la investigación es no experimental, descriptiva, de corte transversal y cuantitativa, obtuvo los siguientes resultados: el 72.37% de los empleados municipales opinan que SI se encuentran expuestos a riesgos y amenazas, el 100.00% de los empleados municipales encuestados opinan que SI existe factibilidad técnica, económica y operativa de la propuesta, el 100.00% de los empleados municipales encuestados opinaron que NO existen controles pertinentes en cuanto a la seguridad de la información.

Además, se revisó la tesis de Aguirre (2014) en su tesis "Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A." realizado en la Pontificia Universidad Católica del Perú, Facultad de Ciencias e Ingeniería, cuyo objetivo fue diseñar un sistema de gestión de seguridad de información para resguardar la confidencialidad, disponibilidad e integridad de los activos de información involucrados en los procesos institucionales críticos de una entidad pública como es SERPOST según lo indicado por la NTP ISO/IEC 27001:2008 y la NTP-ISO/IEC 17999:2007 de seguridad de información. Utilizando las siguientes metodologías: Guía PMBOK de PMI quinta edición y el Ciclo de Deming - Ciclo PDCA, cuyo resultado esperados en el punto 3 para el objetivo 1, en cuanto a la Política de Seguridad de la Información fue que se acople a las políticas actuales y los objetivos estratégicos de la empresa y logre reflejar las expectativas de la organización en materia de seguridad.

También, Villena (2006) en su tesis "Sistema de gestión de seguridad de información para una institución financiera", el objetivo de esta Tesis Fue Establecer Los Principales Lineamientos De Manera Exitosa, Un Adecuado modelo de sistema de gestión de la información(SGSI) en una institución financiera del Perú, el cual apuntó a asegurar que la tecnología de información usada estaba alineada con la estrategia de negocio y que los activos de información tenían el nivel de protección acorde con el valor y riesgo que representaba para la organización, utilizando como referencia el modelo de seguridad de información de Mc Cumber, por ser uno de los más influyentes, dado que abarca los principales estados de la información, características y medidas de seguridad y así se implanto una adecuada gestión de seguridad de la información en una institución financiera.

Otra investigación revisada fue la de Olivos y Guevara (2017) en su tesis titulada "Formulación de políticas de control de accesos y seguridad física y del entorno basado en la norma técnica peruana NTP-ISO/IEC 17799 para la mejora de la gestión en la oficina central de cómputo – Universidad de Lambayeque", realiza en Universidad de Lambayeque, escuela profesional de ingeniería de sistemas para optar el título de ingeniero de sistemas, indica que para que este proyecto tenga éxito, es de vital importancia que se defina formalmente el comité de Seguridad de la Información, órgano que debería encargarse del proyecto de implementación del SGSI y que deberá contar con

el apoyo de la Universidad de Lambayeque; de modo que se facilite el acceso a la información de todas las áreas pertinentes.

Desde el punto de vista social, el Sistema de Seguridad de la información basado en el ISO 27001 permite a la Municipalidad Distrital de Bellavista - Sullana, garantizar los activos de información de la empresa, minimizar y documentar los riesgos o eventos que atenten en contra de la seguridad de la Información y además brindar el respaldo y seguridad de la información siendo beneficiados los trabajadores de la municipalidad distrital de Bellavista – Sullana, e indirectamente toda la población del distrito en mención, con la implementación de este sistema.

Desde el punto de vista científico, la presente investigación busca conocimientos selectivos y sistematizados para el desarrollo del Sistema de Seguridad de la Información de la Municipalidad Distrital de Bellavista - Sullana, el cual se usa como herramienta de apoyo el ISO 27001 y de Pmbok "Gestión de Integración, Gestión de alcance, Gestión de seguridad", que permite el desarrollo de la gestión de los activos de información de la entidad pública, lo cual destaca la evolución de la gestión de sus activos a un nivel de servicio de calidad, siendo funcional, de fácil uso y auditable en todos sus dominios por lo que minimiza los costos a la organización por su adaptabilidad y mejora.

La principal problemática que tiene la Municipalidad Distrital de Bellavista – Sullana, en no contar con controles y/o políticas para la gestión de la seguridad de la información ya que al no existir estas, la sala de operadores y sala de comunicaciones por citar quedan vulnerables ante una posible fuga de información o perdida de algún equipo costoso. Sin embargo; ¿Qué sucede si los activos de información no son utilizados según su objetivo y son usados para otros fines no autorizados y malintencionados? ¿Qué medidas asumir si nuestros usuarios son ajenos a las políticas de la institución?

El 03 de setiembre del 2018 se da inicio a las labores en el Centro de Operaciones, Emergencia y Monitoreo, en ese momento se inició con 12 trabajadores, siendo su potencial un total de 25 trabajadores con 30 cámaras ubicadas en sitios críticos del distrito metropolitano, sin embargo, son insuficientes debido a los altos índices de diversas incidencias, lo que es altamente posible que esta cantidad aumente. La gran cantidad de información que se genera a diario, con el riesgo de fuga de información o perdida de

algún equipo costoso. Por lo que se toma como prioridad el solucionar este gran inconveniente. Es de gran necesidad contar con un sistema de seguridad de la información que identifique vulnerabilidades, amenazas o riesgos, que forme, capacite y promueve el compromiso en temas de seguridad al personal.

Frente a esta problemática es que se plantea el problema desde el punto de vista interrogativo de la siguiente manera: ¿Cómo desarrollar un Sistema de Seguridad de la Información para el Centro de Operaciones, Emergencia y Monitoreo (COEM) de la Municipalidad Distrital de Bellavista – Sullana?

En ese sentido de dar respuesta a esta interrogante y dar solución a la problemática encontrada, se ha buscado conceptualizar y operacionalizar las siguientes definiciones:

SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

Los activos de información son los recursos que tienen valor o utilidad para la organización, sus operaciones comerciales y su continuidad, los cuales son necesarios para que la organización funcione y alcance los objetivos que propone su dirección. (Aguirre, 2014).

Los activos de información se pueden clasificar en las siguientes categorías:

- Activos de información (Datos, manuales del usuario).
- Documentos de papel (contratos).
- Activos de software (aplicación, software de sistemas).
- Personal (clientes, trabajadores).
- Imagen de la empresa y reputación.
- Servicios (comunicaciones).

SEGURIDAD DE LA INFORMACIÓN

Tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

Está caracterizada por la preservación de los siguientes aspectos (Villena, 2006).

- **Confidencialidad:** Asegurando que la información seas accesible solo por aquellos que están autorizados.
- **Integridad:** Salvaguardando la exactitud de la información en su procesamiento, así

como su modificación autorizada.

- **Disponibilidad:** asegurando que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando sea requerido.

PILARES DE LA SEGURIDAD INFORMÁTICA

Figura 1: Pilares de Seguridad de la Información
Fuente: http://www.itsteziutlan.edu.mx

En la seguridad de la información es importante señalar que su manejo está basado en la Tecnología y debemos saber que puede ser confidencial. Puede ser divulgada, mal utilizada, robada, borrada, saboteada, etc. La información es poder, y según las posibilidades estratégicas que ofrece tener acceso cierta información, esta se clasifica como:

Critica: Es indispensable para la operación de la empresa.
Valiosa: Es un activo de la empresa y muy valioso.
Sensible: Debe ser conocida por las personas autorizadas.

SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN (SGSI)

Es una forma sistemática de administrar la información sensible de una institución, para que permanezca segura. Abarca a las personas, los procesos y las tecnologías de información. La forma total de la Seguridad de la Información, y la integración de diferentes iniciativas de seguridad necesitan ser administradas para que cada elemento

sea completamente efectivo. Aquí es donde entra el Sistema de Gestión de Seguridad de la Información que permite coordinar esfuerzos de seguridad con mayor efectividad (Villena ,2006).

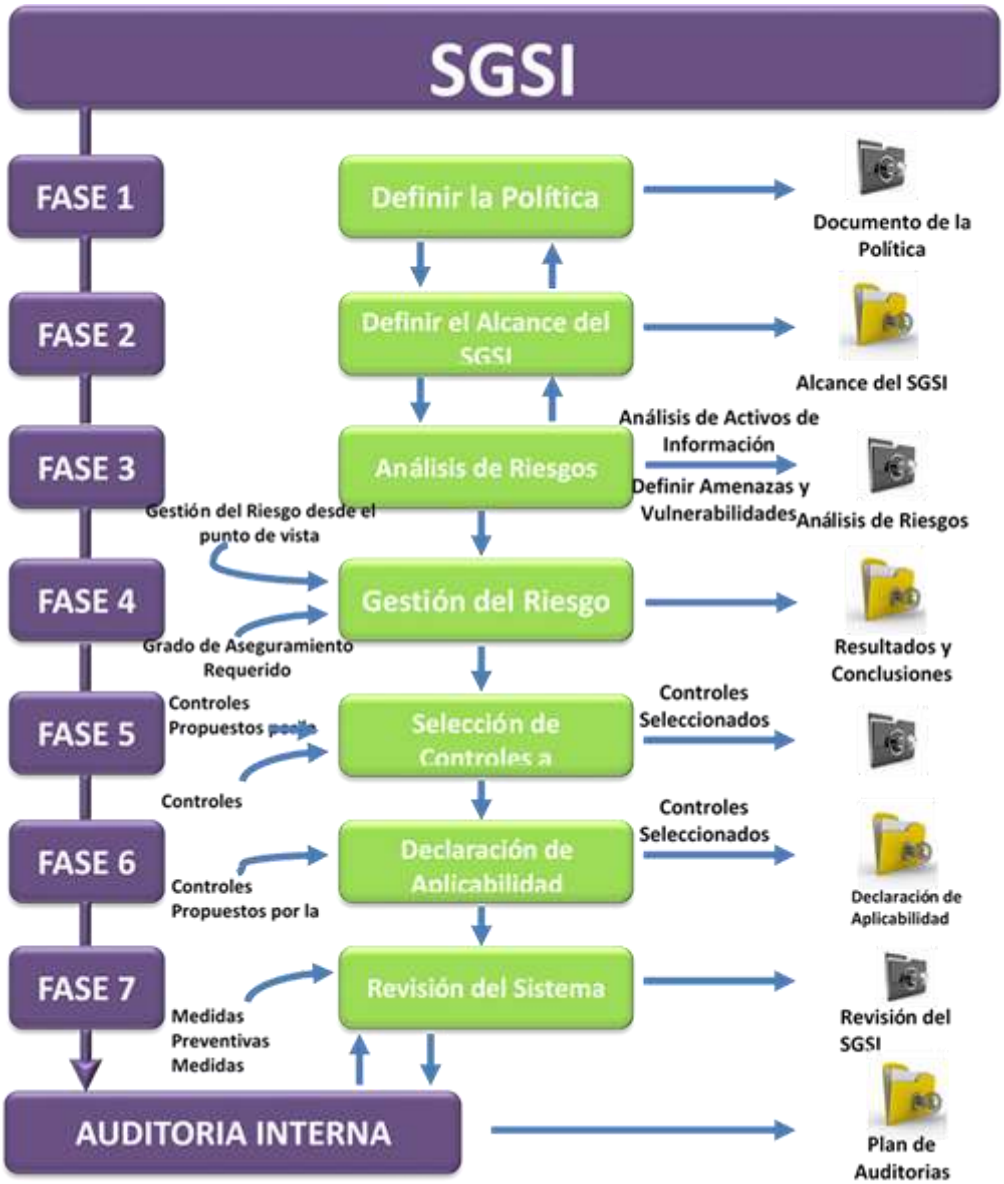


Figura 2: Sistema de Gestión de Seguridad de la Información

Fuente: https://www.grantthornton.com.co

PARA QUÉ SIRVE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización,

con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Figura 3: Riesgos -SGSI

Fuente: http://www.iso27000.es/sgsi.html

Definición del Riesgo

Estimación de grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

El riesgo indica lo que puede que podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema.

Entre las amenazas, existen las vulnerabilidades, los riesgos y los activos de información, una secuencia de causalidad y probabilidad de ocurrencia.

Figura 4: Elementos del Riesgo

Fuente: https://pt.slideshare.net/clauditasuvi/exposicion-7288461/7

Identificar los riesgos

- Identificar todos aquellos activos de información que tienen algún valor para la organización que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios.
- Identificar las amenazas relevantes asociadas a los activos identificados.
- Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas.
- Identificar el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo.

Análisis del Riesgo

Para analizar el riesgo se debe establecer la probabilidad de ocurrencia del mismo, así como sus consecuencias, esto finalmente orientará a la clasificación del riesgo. Esta fase depende de la información obtenida en la etapa de identificación. Existen dos aspectos principales que determinarán el análisis de riesgo:

- Probabilidad: posibilidad de ocurrencia del riesgo, la cual se puede medir con criterios de frecuencia.
- Impacto: consecuencias que pueden ocasionar la materialización del riesgo en la organización

Evaluación del riesgo

La evaluación involucra comparar niveles de riesgo con criterios definidos en el contexto. El objetivo de esta evaluación es la de identificar y evaluar los riesgos, los cuales son calculados por una combinación de valores de activos y niveles de requerimiento de seguridad. Con base en esta comparación, se puede considerar la necesidad de tratamiento; además las decisiones se deben tomar de acuerdo con los requisitos legales, reglamentarios y otros.

La evaluación de riesgos también puede tener como resultado la decisión de no tratar el riesgo de ninguna manera diferente de los controles existentes.

Tratamiento del riesgo

El tratamiento del riesgo se define como el conjunto de decisiones tomadas con cada activo de información.

Las decisiones para tratar el riesgo pueden incluir las siguientes opciones:

Evitar el riesgo: La opción de evitar el riesgo, describe cualquier acción donde las actividades del negocio, o las maneras de conducir la gestión comercial del negocio, se modifican, para así poder evitar la ocurrencia del riesgo.

Las maneras tradicionales para implementar esta opción son:

- Dejar de conducir ciertas actividades.
- Desplazar activos de información de un área riesgosa a otra.
- Decidir no procesar cierto tipo de información y no se consigue la protección adecuada.

La decisión por la opción de “evitar el riesgo” debe ser balanceada contra las necesidades financieras y comerciales de la empresa.

Aceptar el riesgo: Cuando no es posible mitigarlo y se debe continuar la actividad que lo originó.

En muchas ocasiones a la empresa se le presentan circunstancias donde no se pueden encontrar controles ni tampoco es factible diseñarlos o el costo de implantar el control es mayor que las consecuencias del riesgo. En estas

circunstancias una decisión razonable pudiera ser la de inclinarse por la aceptación del riesgo, y vivir con las consecuencias si el riesgo ocurriese.

Cuando la situación se presenta donde es muy costoso para la empresa mitigar el riesgo a través de los controles o las consecuencias del riesgo son devastadoras para la organización, se deben visualizar las opciones de "transferencia de riesgo" o la de "evitar el riesgo".

Reducir el riesgo

Para los riegos donde la opción de reducirlos ha sido escogida, se deben implementar los apropiados controles para disminuirlos a los niveles de aceptación previamente indefinidos por la empresa. Los controles deben obtenerse del anexo "A" del ISO 270001:2013. Al identificar el nivel de los controles es importante considerar los requerimientos de seguridad relacionados con el riesgo, así como la vulnerabilidad y las amenazas previamente identificadas.

Los controles pueden reducir los riesgos valorados en varias maneras:

- Reduciendo la posibilidad que la vulnerabilidad sea explotada por las amenazas.
- Reduciendo la posibilidad de impacto si el riesgo ocurre detectando eventos no deseados, reaccionado y recuperándose de ellos.

Transferir el riesgo: Fuera del apetito de riesgo, el riesgo se comparte con una o varias partes, pueden ser agentes externos.

Figura 5: Gestión de Riesgos

Fuente: http://www.iso27000.es/sgsi_implantar.html

Controles

Son las políticas, procedimientos, prácticas y estructuras organizacionales para reducir riesgos y que además proveen cierto grado de certeza de que se alcanzarán los objetivos del negocio.

Existen varias formas de establecer controles sobre riesgos organizacionales. La siguiente es:

- Disuasivos: su presencia disuade de la comisión de acciones en contra de alguna política o procedimiento establecido y considerado correcto. Por ejemplo: cámaras de vigilancia.
- Preventivos: detectan problemas antes que ocurran por medio de monitoreo constante. Por ejemplo: políticas de contratación.
- Detectivos: detectan y reportan los problemas suscitados por errores u omisiones, en el momento en que éstos ocurren. Por ejemplo: Uso de antivirus.
- Correctivos: minimizan el impacto de una amenaza ya consumada. Por ejemplo: Planes de contingencia. Propios de cada área administrativa y operativa de las organizaciones. (Espinoza, 2013)

PMBOK (QUINTA VERSIÓN)

La Guía del PMBOK es el estándar, reconocido a nivel global y la guía para la Administración de Proyectos y cuyas siglas significan en inglés Project Management Body of Knowledge (el Compendio del Saber de la Gestión de Proyectos en español). Es un estándar reconocido internacionalmente (IEEE Std 1490-2003) que provee los fundamentos de la gestión de proyectos que son aplicables a un amplio rango de proyectos, incluyendo construcción, software, ingeniería, etc.

PMBOK reconoce 5 grupos de procesos básicos y 10 áreas de conocimiento comunes a casi todos los proyectos.

Los procesos se trasladan e interactúan a través de un proyecto o fase. Los procesos son descritos en términos de: Entradas (documentos, planes, diseños, etc.), herramientas y Técnicas (mecanismos aplicados a las entradas) y Salidas (documentos, productos, etc.).

Resumen de los 5 procesos de la dirección de proyectos y las diez áreas de conocimientos.

I.1 GRUPOS DE PROCESOS DE GESTION DE PROYECTOS:

Área de Conocimiento	**Grupos de Procesos de Gestión de Proyectos**				
	Procesos de Iniciación	Procesos de Planificación	Procesos de Ejecución	Procesos de Motorización y Control	Procesos de Cierre
Gestión de la Integración del Proyecto (1)	Desarrollar el Acta de Constitución del Proyecto (1.1)	Desarrollar el Plan de Gestión del Proyecto (1.2)	Dirigir y Gestionar la Ejecución del Proyecto (1.3)	Supervisar y Controlar el Trabajo del Proyecto (1.4) Control Integrado de Cambios (1.5)	Cerrar Proyecto (1.6)
Gestión del Alcance del Proyecto (2)		Planificar la Gestión del Alcance (2.1) Identificar los Requisitos (2.2)		Validar el Alcance (2.5)	

		Definir el Alcance (2.3) Crear EDT (2.4)		Controlar el Alcance (2.6)	
Gestión del Tiempo del Proyecto (3)		Planificar la Gestión del Cronograma (3.1) Definir las Actividades (3.2) Establecimiento de la Secuenciar las Actividades (3.3) Estimar los Recursos de Actividades (3.4) Estimar la Duración de Actividades (3.5) Desarrollar el Cronograma (3.6)		Controlar el Cronograma (3.7)	
Gestión de los Costes del Proyecto (4)		Planificar la Gestión del Alcance (2.1) Identificar los Requisitos (2.2) Definir el Alcance (2.3) Crear EDT (2.4)		Control de Costes (4.4)	

Gestión de la Calidad del Proyecto (5)		Planificar la Gestión de Calidad (5.1)	Realizar Aseguramiento de Calidad (5.2	Controlar la Calidad (5.3)	
Gestión de los Recursos Humanos del Proyecto (6)		Planificar la Gestión de Recursos Humanos (6.1)	Adquirir el Equipo del Proyecto (6.2) Desarrollar el Equipo del Proyecto (6.3) Gestionar el Equipo del Proyecto (6.4)		
Gestión de las Comunicaciones del Proyecto (7)		Planificar las Comunicaciones (7.1)	Gestionar las Comunicaciones (7.2)	Controlar las Comunicaciones (7.3)	
Gestión de los Riesgos del Proyecto (8)		Planificar la Gestión de Riesgos (8.1) Identificar los Riesgos (8.2)		Controlar los Riesgos (8.6)	

		Realizar el Análisis Cualitativo de Riesgos (8.3) Realizar el Análisis Cuantitativo de Riesgos (8.4) Planificar la Respuesta a los riesgos (8.5)			
Gestión de las Adquisiciones del Proyecto (9)		Planificar las Adquisiciones (9.1)	Realizar las Adquisiciones (9.2)	Controlar las Adquisiciones (9.3)	Cerrar las Adquisiciones (9.4)
Gestión de los Grupos de Interés del Proyecto (10)	Identificar a los Grupos de Interés (10.1)	Planificar la Gestión de los Grupos de Interés (10.2)	Gestionar los Grupos de Interés (10.3)	Controlar los Grupos de Interés (10.1)	

Tabla 1: Grupo de Procesos

Fuente: Elaboración propia

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO)

ISO, sus siglas en inglés proviene de los términos (International Standarization Organization) la cual es una entidad internacional que se encarga de la normalización a nivel mundial, las cuales desarrollan bajo diferentes grupos o comités especializados las normativas, modelos o patrones a seguir con el objetivo de definir ciertas características que debe poseer un objeto o producto.

Su finalidad es orientar, coordinar, simplificar y unificar los usos para conseguir menores costes y efectividad.

ISO 27001: 2013

El ISO/ IEC 27001: 2013, es un modelo de gestión de seguridad de la información, el cual se define como un conjunto de lineamientos el cual especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información.

Estos requisitos describen cual es el comportamiento esperado del sistema de Gestión una vez que esté en funcionamiento; por lo tanto, para el desarrollo del proyecto se tomó a la Norma ISO 27001:2013 como marco de referencia en la implementación del Sistema de Gestión de Seguridad de la información.

Figura 6: Evolución de la estructura ISO 27001:2013
Fuente: Presentación Camargo Ramírez

La ISO 27001:2013 cuenta con 114 controles, 14 Dominios de Seguridad y 130 Requisitos de Gestión.

LOS DOMINIOS DEL ISO 27001.

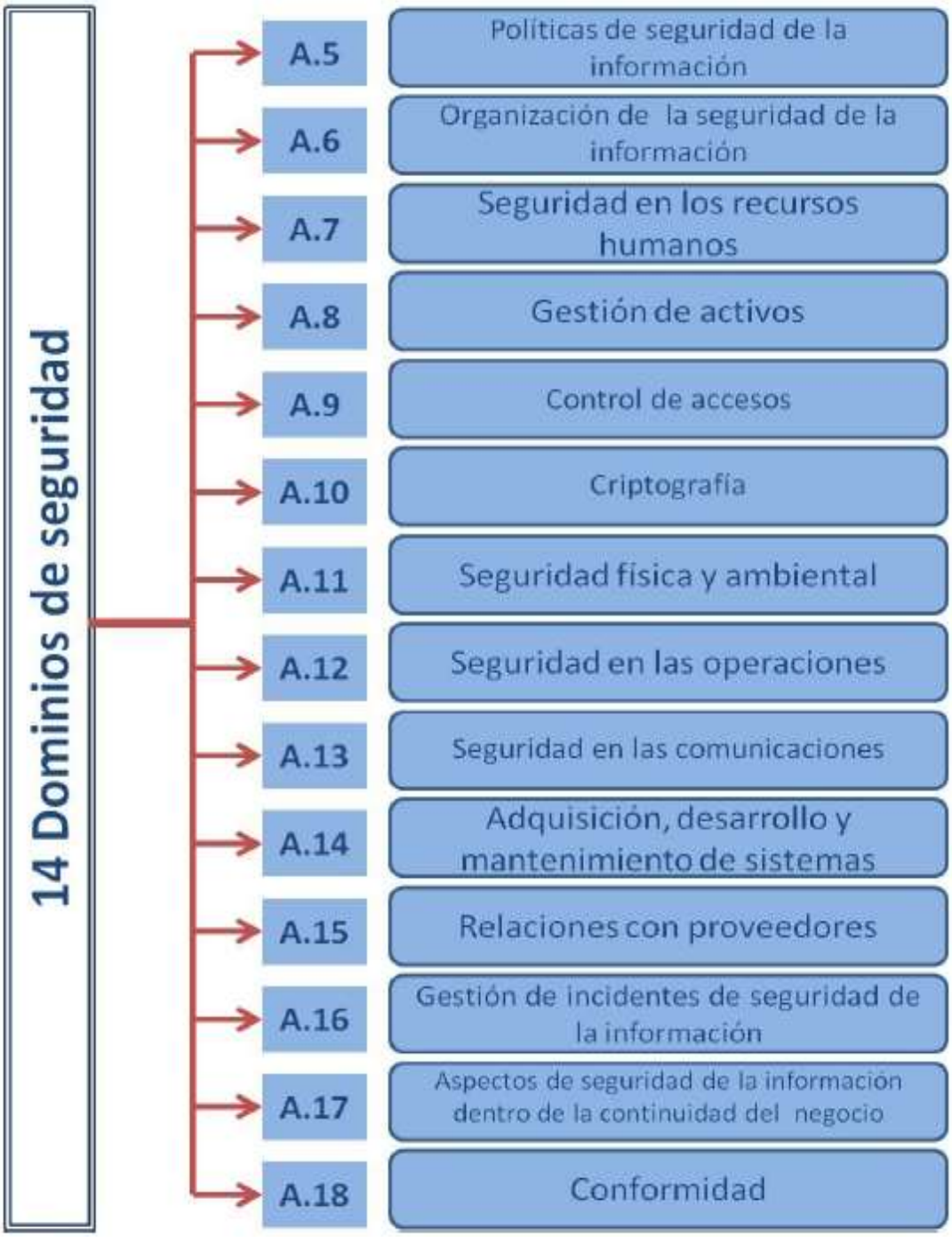


Figura 7: Los Dominios del ISO

Fuente:http://www.isaca.org/chapters7/Madrid/Events/Documents/Principales%20Novedades%20de%20la%20ISO27001ISO%2027002%20-%20Paloma%20Garcia.pdf

Entre los objetivos que busca el autor en la presente investigación tenemos:

Como objetivo general, Desarrollar un SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL CENTRO DE OPERACIONES, EMERGENCIA Y MONITOREO (COEM) DE LA MUNICIPALIDAD DISTRITAL DE BELLAVISTA – SULLANA, para la Gerencia de Seguridad Ciudadana; y como objetivos específicos:

- Analizar y Diagnosticar la situación actual del Centro de Operaciones, Emergencia y Monitoreo (COEM) de la Municipalidad Distrital de Bellavista – Sullana, para establecer controles del sistema de Gestión de Seguridad de la Información.
- Desarrollar la guía de las buenas prácticas para la Gestión de proyectos PMBOK, el cual permite el obtener los entregables tales como; el Acta de Constitución del proyecto y la EDT (Estructura Desagregada de Trabajo) y el área del conocimiento gestión de riesgos para la formalización e inicio del proyecto.
- Desarrollar la guía de buenas prácticas de la Norma ISO 27001:2013 del sistema de Gestión de Seguridad de la Información para la Municipalidad Distrital de Bellavista – Sullana, así como seleccionar los controles de Seguridad de Información para el apoyo salvaguardar los activos de información de la Municipalidad Distrital de Bellavista – Sullana.

II. METODOLOGÍA

El presente trabajo se basa en el tipo de investigación descriptivo no experimental y consiste en analizar los procesos de gestión de la información en la Municipalidad Distrital de Bellavista - Sullana y en base a esa investigación desarrollar el sistema de gestión de la Seguridad de la información; a partir de la recolección de datos basado en encuestas. Es de diseño transversal Porque analiza los datos en un momento determinado.

Las técnicas e instrumentos utilizados en la investigación se describen en la siguiente tabla:

Las técnicas e instrumentos utilizados en la investigación se describen en la siguiente tabla:

Técnica	Instrumento	Justificación	Aplicación
Encuestas	Cuestionario de preguntas (De tipo cerradas de elección única, tanto dicotómica y politómica.).	Permite conocer las expectativas que tienen los usuarios respecto al sistema y necesidades de Información de los usuarios y conocimiento de las consideraciones en seguridad de la información.	Trabajadores del Centro de Operaciones, Emergencia y Monitoreo (COEM) y Área de Estadística y Tecnología de la Información.

Tabla N° 02: Técnicas e instrumentos de recolección de datos

Fuente: elaboración propia

Asimismo, como parte de la metodología de desarrollo se han utilizado los siguientes instrumentos:

PMBOK quinta edición

Gestión Integración:

Elaborar una Acta de Constitución del Proyecto

Desarrollar el Plan de Gestión del Proyecto

Elabora el EDT

Planificar la Gestión de Riesgos

Realizar el Análisis Cuantitativo de Riesgos

Planificar la Respuesta a los Riesgos

ISO 27001:2013

Introducción a la Norma ISO 27001,2013

Análisis de Riesgos

Inventario de Activos

Identificación de Amenaza

Valoración de Riesgo por Activo

Tratamiento del Riesgo

Descripción de la Empresa

Objetivos del Negocio

Situación actual de la Empresa

Definición de la Política de Seguridad de la Información

Informe Final

III. RESULTADOS

El cuestionario realizado al personal de Centro de Operaciones, Emergencia y Monitoreo (COEM); consta de 20 preguntas el cual se encuentra en Anexos, para el análisis, cuyos resultados se muestran a continuación:

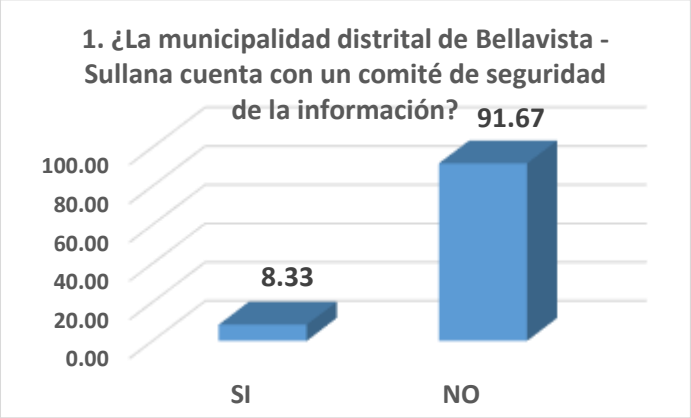


Figura 07: Grafico Comité de Seguridad de la Información

Fuente: Elaboración propia

Análisis: En el gráfico podemos apreciar que del 100% de la encuesta, el 8.33 % de los trabajadores saben que la Municipalidad distrital de Bellavista – Sullana, cuenta con un comité de Seguridad de la Información y un 91.67% indica que no cuentan con un comité de seguridad de la Información.

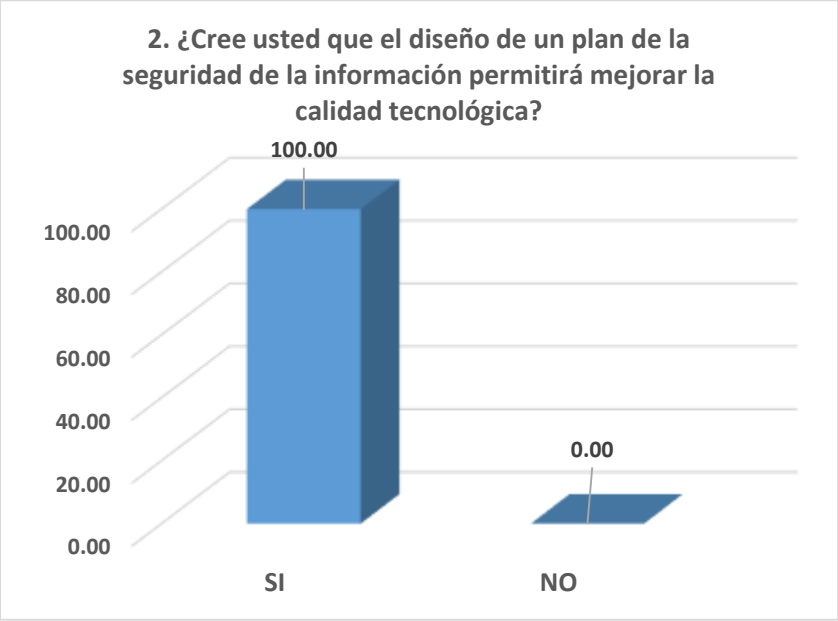
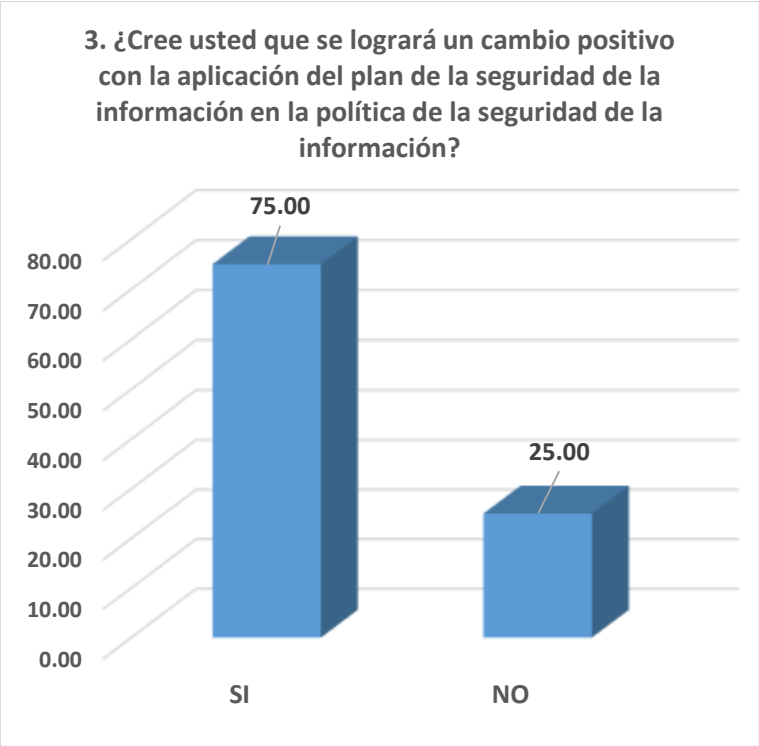


Figura 08: Grafico diseño de plan de Seguridad de la Información

Fuente: Elaboración propia

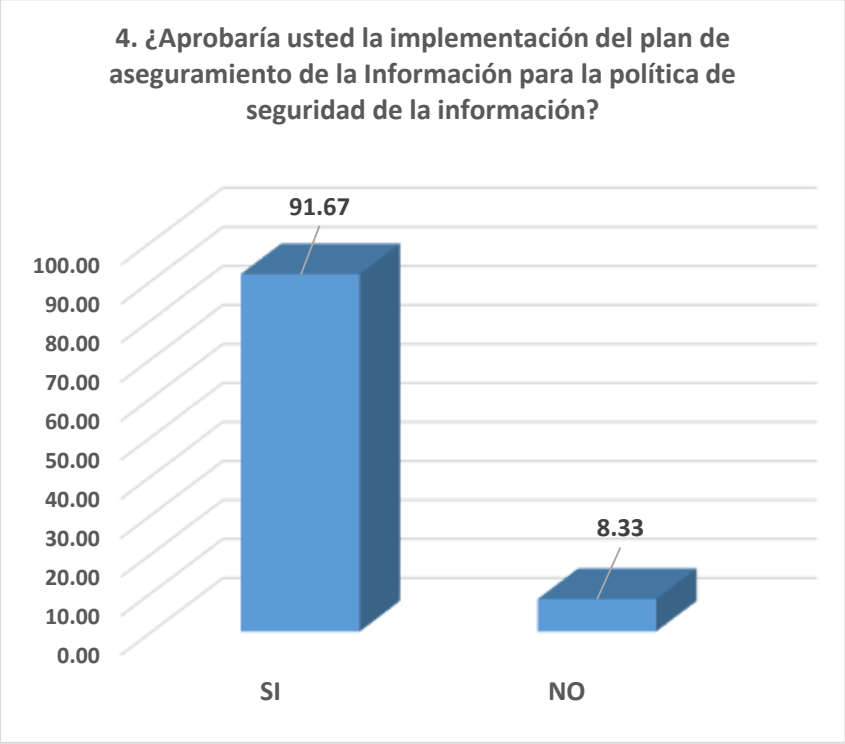
Análisis: El cuadro siguiente se aprecia que el 100% de los trabajadores de la Municipalidad distrital de Bellavista – Sullana, creen que con un diseño de un plan de la seguridad de la información permitirá mejorar la calidad tecnológica, y un 0.0% señalo lo contrario.



Análisis: En el gráfico apreciamos que del 100% de la encuesta, el 75 % de los trabajadores de la Municipalidad distrital de Bellavista – Sullana creen que se logrará un cambio positivo con la aplicación del plan de la seguridad de la información en la política de la seguridad de la información, mientras un 13% no creen.

Figura 09: Grafico Cambio positivo al aplicar plan de seguridad

Fuente: Elaboración propia



Análisis: Se puede observar que el 91.67% de los trabajadores de la Municipalidad distrital de Bellavista – Sullana, indica que aprobaría la implementación del plan de Seguridad de la Información para la política de seguridad de la información, mientras un 8.33% no aprobaría.

Figura 10: Grafico Aprobaría usted la implementación del plan de Seguridad de la Información

Fuente: Elaboración propia

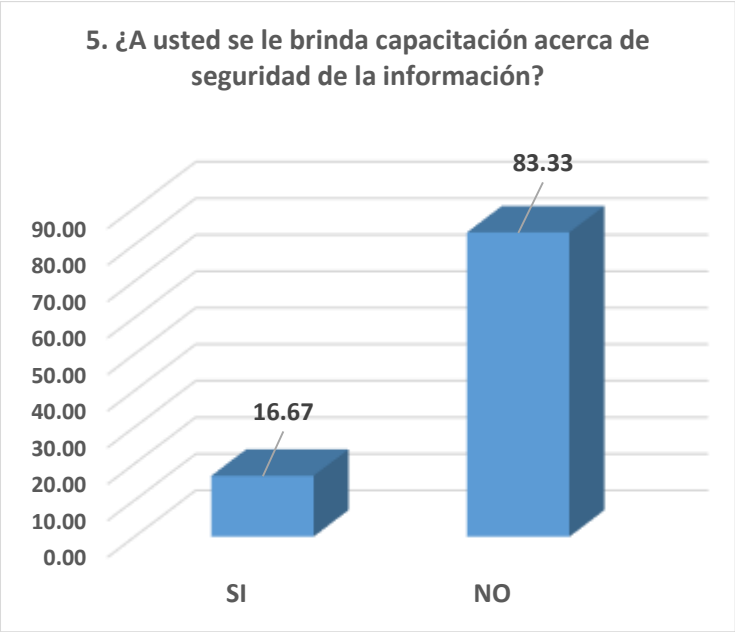


Figura 11: Grafico se le brinda capacitación acerca de seguridad de la información

Fuente: Elaboración propia

Análisis: En el gráfico podemos apreciar que del 100% de la encuesta, el 16.67 % de los trabajadores de la Municipalidad distrital de Bellavista – Sullana indica que se le brinda capacitación acerca de seguridad de la información, mientras un 83.33% no se le brinda dicha capacitación.

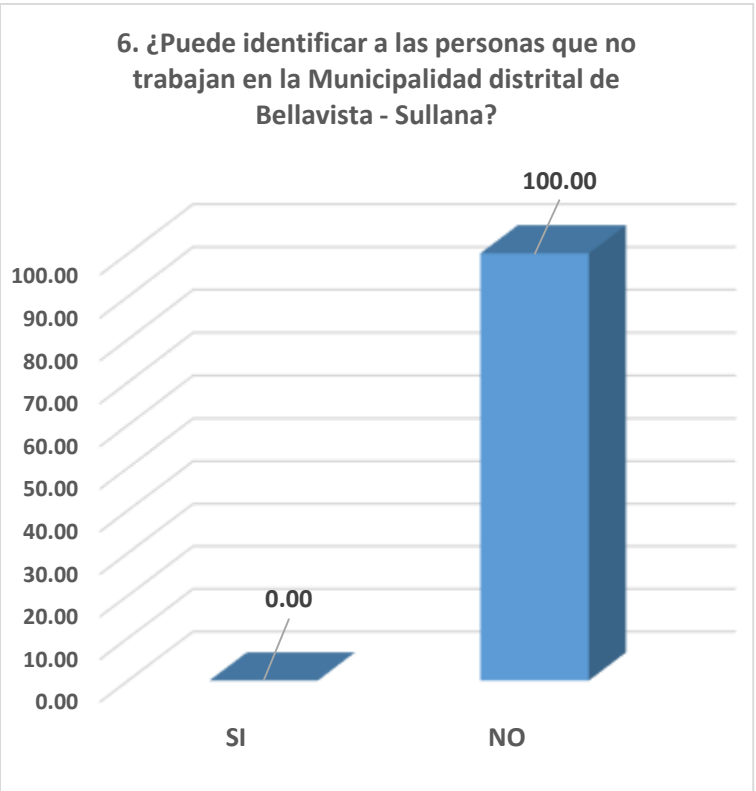


Figura 12: Grafico Puede identificar a las personas que no trabajan en la Municipalidad distrital de Bellavista

Fuente: Elaboración propia

Análisis: Se observa que el 0.0% de los trabajadores de la Municipalidad distrital de Bellavista – Sullana pueden identificar a las personas que no trabajan en la Municipalidad distrital de Bellavista, mientras un 100.00% no puede identificar a estas personas.

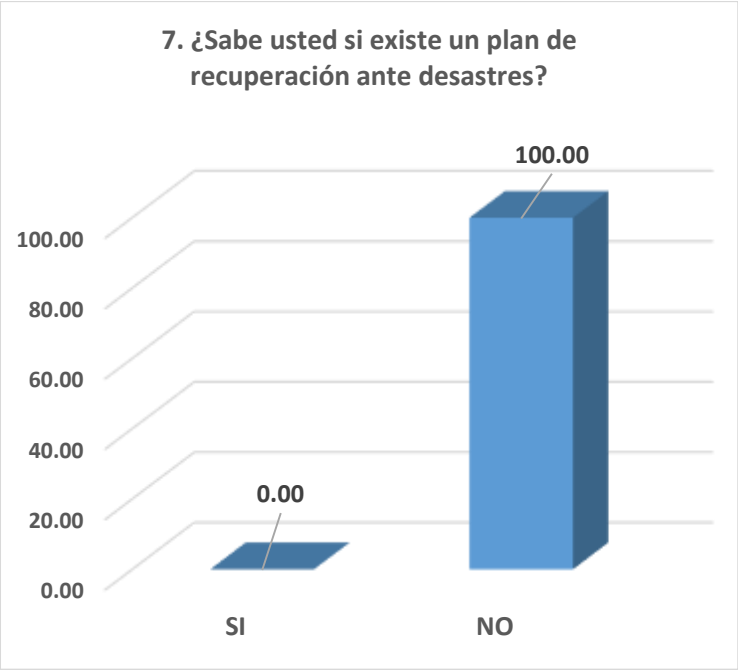


Figura 13: Grafico Sabe usted si existe un plan de recuperación ante desastres

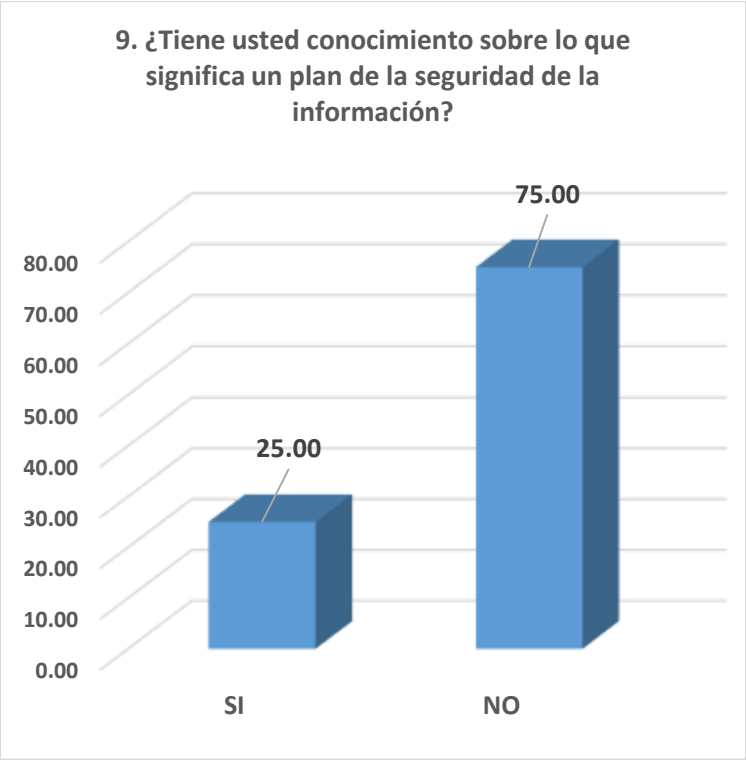
Fuente: Elaboración propia

Análisis: En el gráfico podemos apreciar que del 100% de la encuesta, el 0.0 % de los trabajadores de la Municipalidad distrital de Bellavista – Sullana, saben si existe un plan de recuperación ante desastres, mientras un 100.00% no sabe si existe dicho plan.

Figura 14: Sabe usted si se ha realizado evaluación de riesgos relacionados con la información

Fuente: Elaboración propia

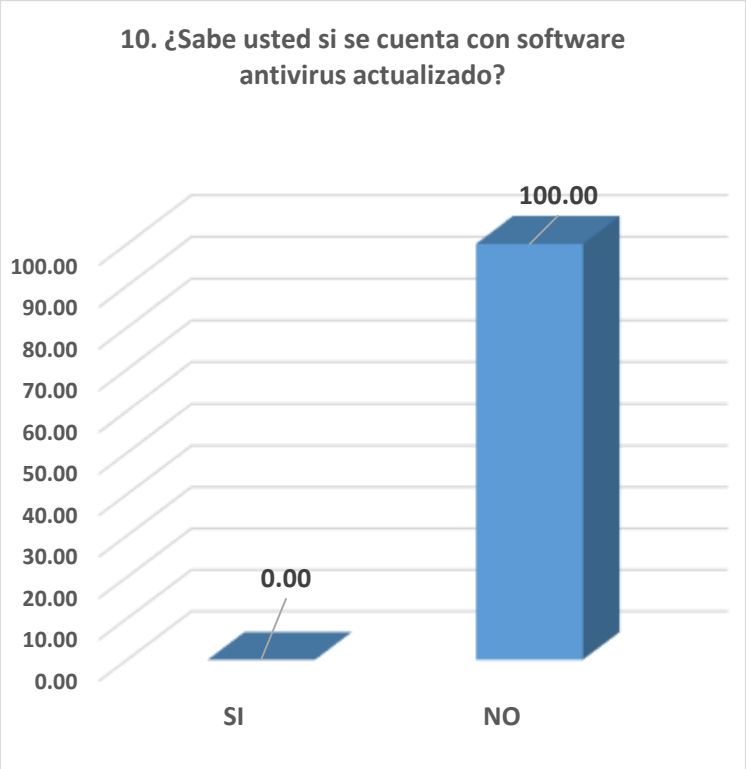
Análisis: En el gráfico podemos apreciar que del 100% de la encuesta, el 0.0 % de los trabajadores de la Municipalidad distrital de Bellavista – Sullana, saben si se ha realizado evaluación de riesgos relacionados con la información, mientras un 100.00% indica lo contrario.



Análisis: En el gráfico podemos apreciar que del 100% de la encuesta, el 25.00 % de los trabajadores de la Municipalidad distrital de Bellavista – Sullana tiene conocimiento lo que significa un plan de la seguridad de la información, mientras un 75.00% no tienen conocimiento que significa un plan de seguridad de la información.

Figura 15: Tiene conocimiento lo que significa un plan de la seguridad de la información

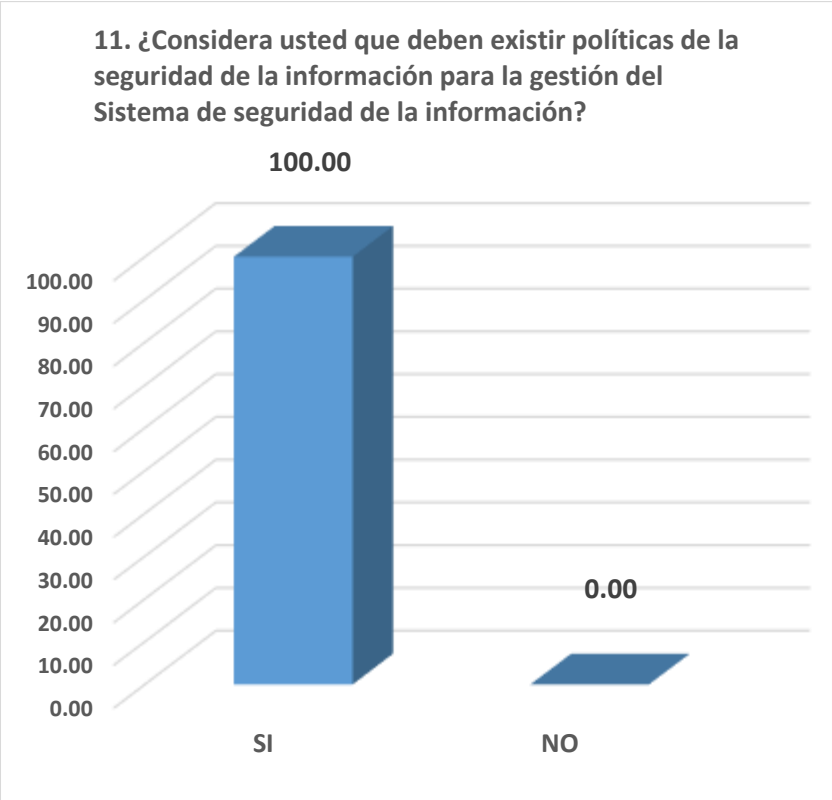
Fuente: Elaboración propia



Análisis: En el gráfico podemos apreciar que del 100% de la encuesta, el 0.0 % de los trabajadores de la Municipalidad distrital de Bellavista – Sullana, sabe que, si se cuenta con software antivirus actualizado, mientras un 100.00% no sabe si cuenta con un antivirus actualizado.

Figura 16: Sabe usted si se cuenta con software antivirus actualizado

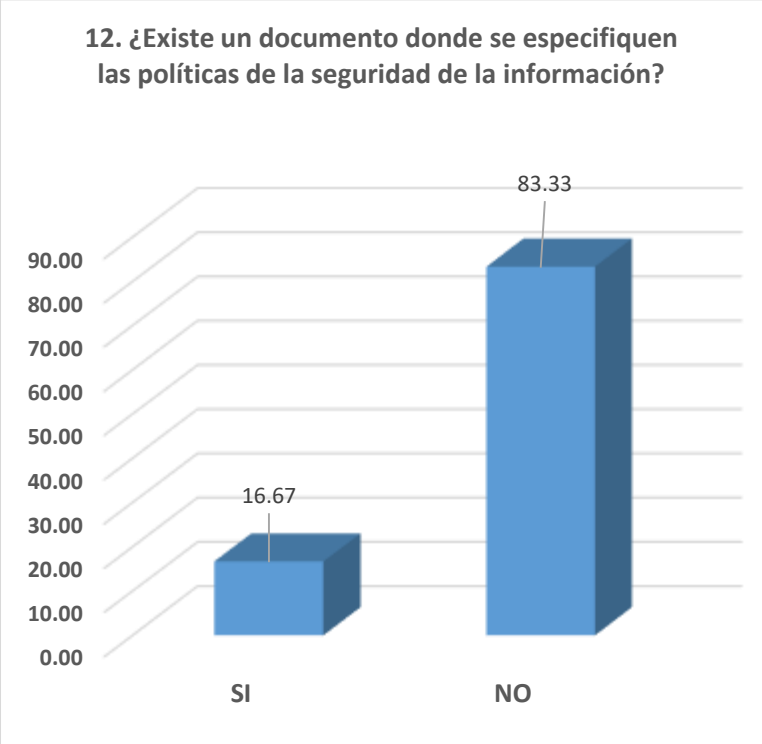
Fuente: Elaboración propia



Análisis: En el cuadro se puede ver que, el 100.00% de los trabajadores de la Municipalidad distrital de Bellavista – Sullana considera que deben existir políticas de seguridad, mientras que un 0.0% señala que no es necesario.

Figura 17: Grafico Comité de Seguridad de la Información

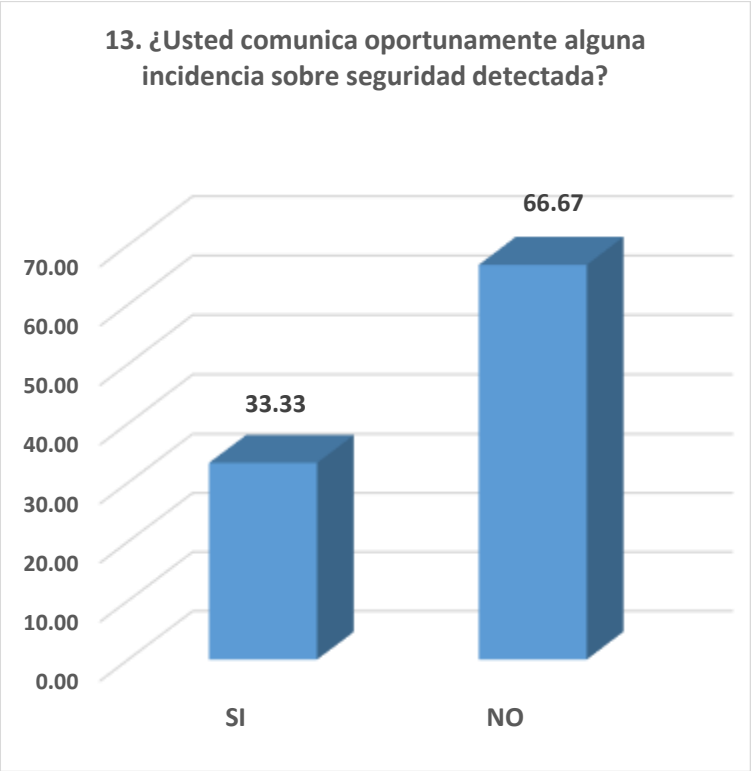
Fuente: Elaboración propia



Análisis: En el gráfico podemos apreciar que el 16.67% de los trabajadores de la Municipalidad distrital de Bellavista – Sullana, indica que existe un documento don se especifican las políticas de la seguridad de la información, y un 83.33% no creen que dicho plan de seguridad mejorara la calidad tecnológica.

Figura 18: Grafico diseño de plan de Seguridad de la Información

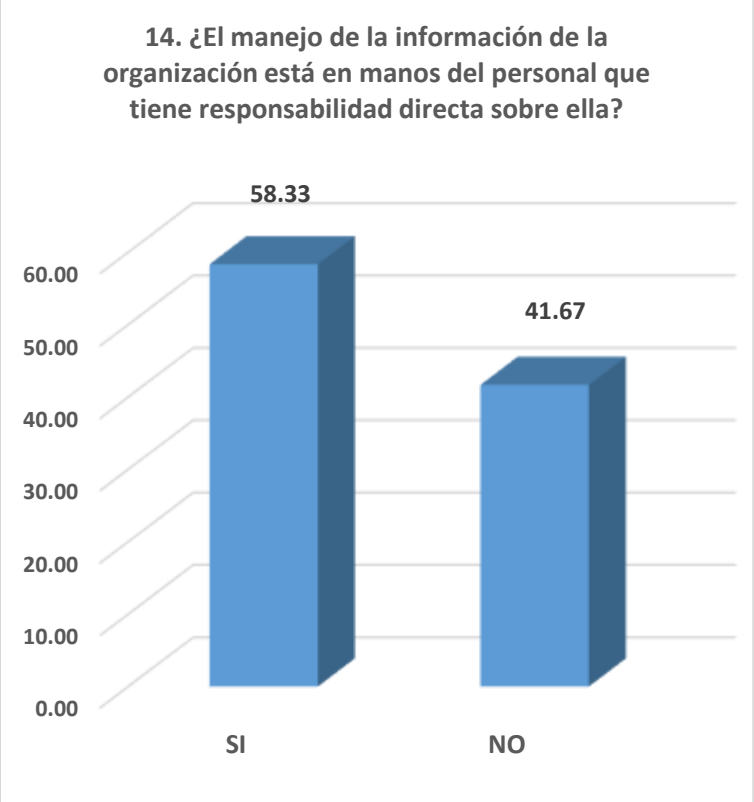
Fuente: Elaboración propia



Análisis: Se observa en el cuadro que un 33.33% de los trabajadores de la Municipalidad distrital de Bellavista – Sullana, indica que comunica oportunamente alguna incidencia sobre seguridad detectada, mientras un 66.67% no comunican lo anteriormente señalado.

Figura 19: Grafico Cambio positivo al aplicar plan de seguridad

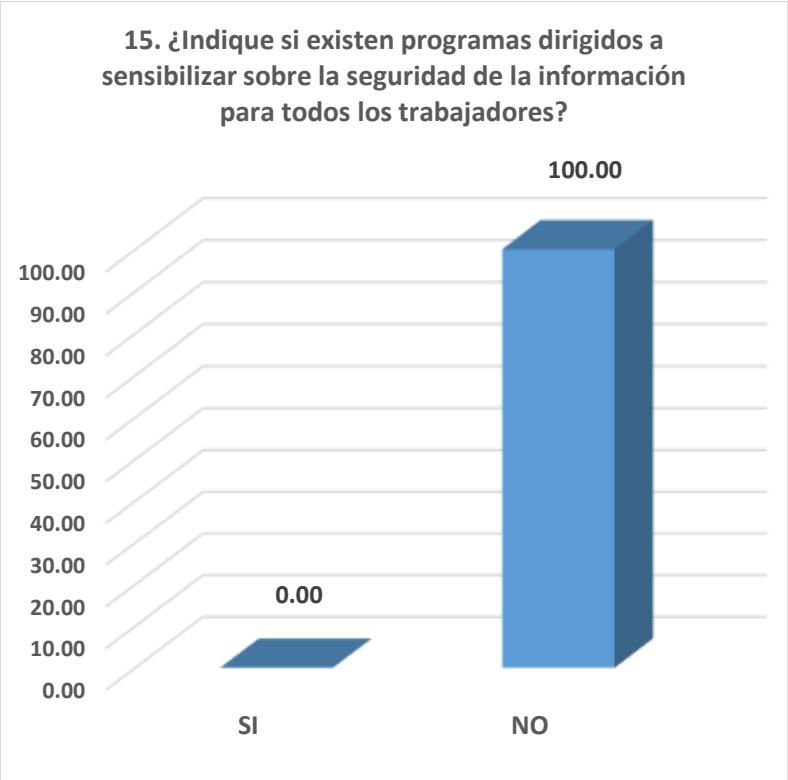
Fuente: Elaboración propia



Análisis: En el gráfico podemos apreciar que del 100% de la encuesta, el 58.33% de los trabajadores de la Municipalidad distrital de Bellavista – Sullana, indica que el manejo de la información está en manos del personal que tiene responsabilidad directa sobre ella, mientras un 41.67% señalo lo contrario.

Figura 20: Grafico Aprobaría usted la implementación del plan de Seguridad de la Información

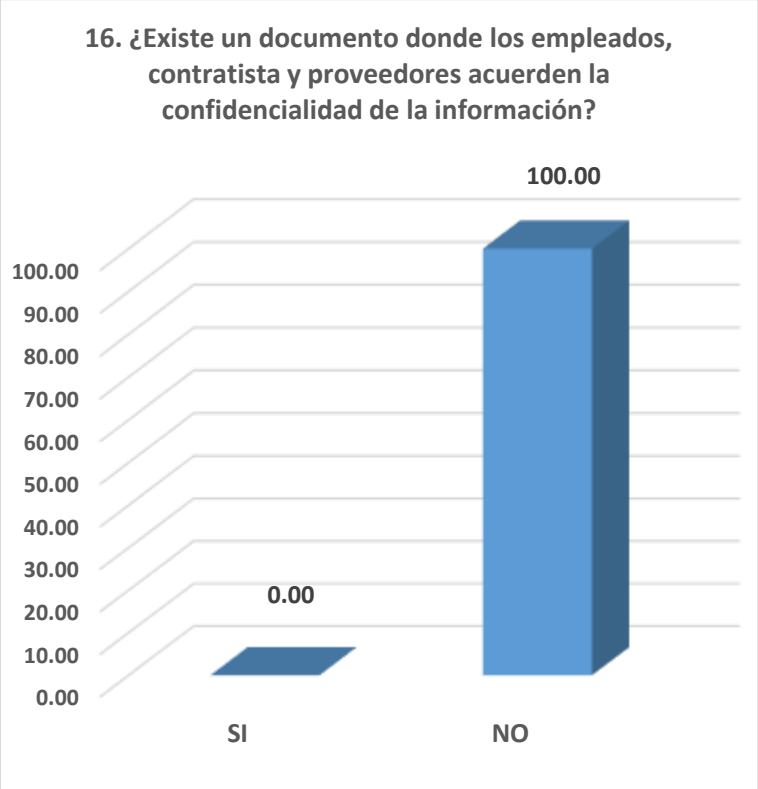
Fuente: Elaboración propia



Análisis: En el gráfico podemos apreciar que del 100% de la encuesta, el 0.0% de los trabajadores de la Municipalidad distrital de Bellavista – Sullana indica que si existe programas dirigidos a sensibilizar sobre la seguridad de la información le brinda capacitación acerca de seguridad de la información, mientras un 100.00% indica lo contrario.

Figura 21: Grafico se le brinda capacitación acerca de seguridad de la información

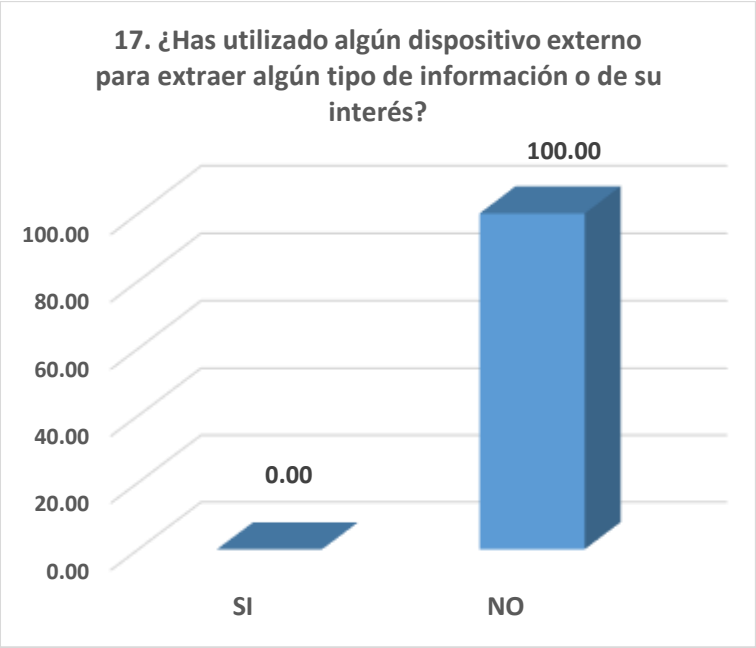
Fuente: Elaboración propia



Análisis: En el gráfico podemos apreciar que del 100% de la encuesta, el 0.0 % de los trabajadores de la Municipalidad distrital de Bellavista – Sullana indica que existe un documento donde los empleados, contratistas y proveedores acuerden la confidencialidad de la información, mientras un 100.00% señala que no existe dicho documento en mención.

Figura 221: Grafico Puede identificar a las personas que no trabajan en la Municipalidad distrital de Bellavista

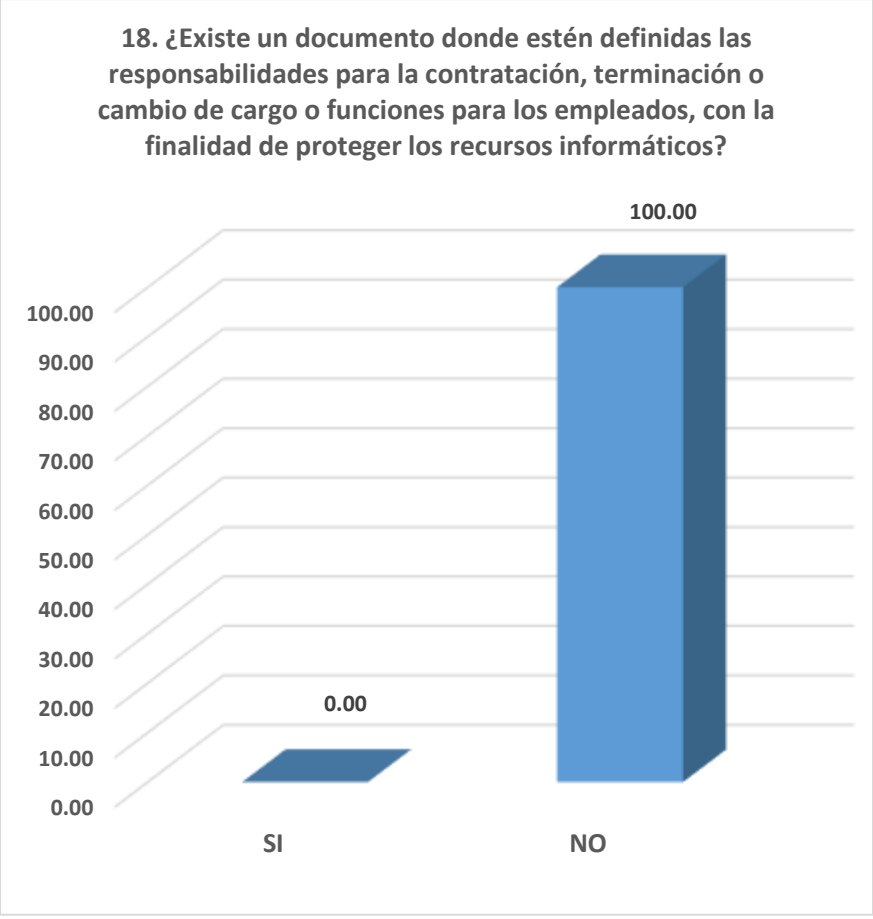
Fuente: Elaboración propia



Análisis: Podemos ver que del 100% de la encuesta, el 0.0 % de los trabajadores de la Municipalidad distrital de Bellavista – Sullana, han utilizado algún dispositivo externo para extraer algún tipo de información o de su interés, mientras un 100.00% señalo que no utilizo ningún dispositivo.

Figura 23: Grafico Sabe usted si existe un plan de recuperación ante desastres

Fuente: Elaboración propia



Análisis: Se observa que el 0.0 % de los trabajadores de la Municipalidad distrital de Bellavista – Sullana, indica que existe un documento donde se defina las responsabilidades para la contratación, terminación o cambio de cargo o funciones para los empleados, con la finalidad de proteger los recursos informáticos, mientras un 100.00% señalo lo contrario.

Figura 24: Sabe usted si se ha realizado evaluación de riesgos relacionados con la información

Fuente: Elaboración propia

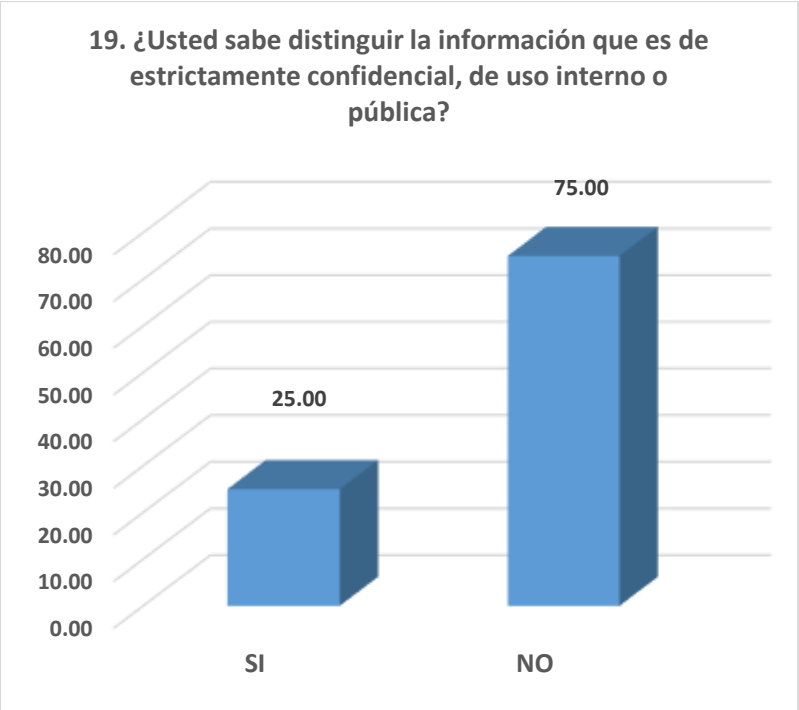


Figura 25: Tiene conocimiento lo que significa un plan de la seguridad de la información

Fuente: Elaboración propia

Análisis: En el gráfico podemos apreciar que del 100% de la encuesta, el 25.00 % de los trabajadores de la Municipalidad distrital de Bellavista – Sullana, sabe distinguir la información estrictamente confidencia, de uso interno o pública, mientras un 75.00% no distinguen.

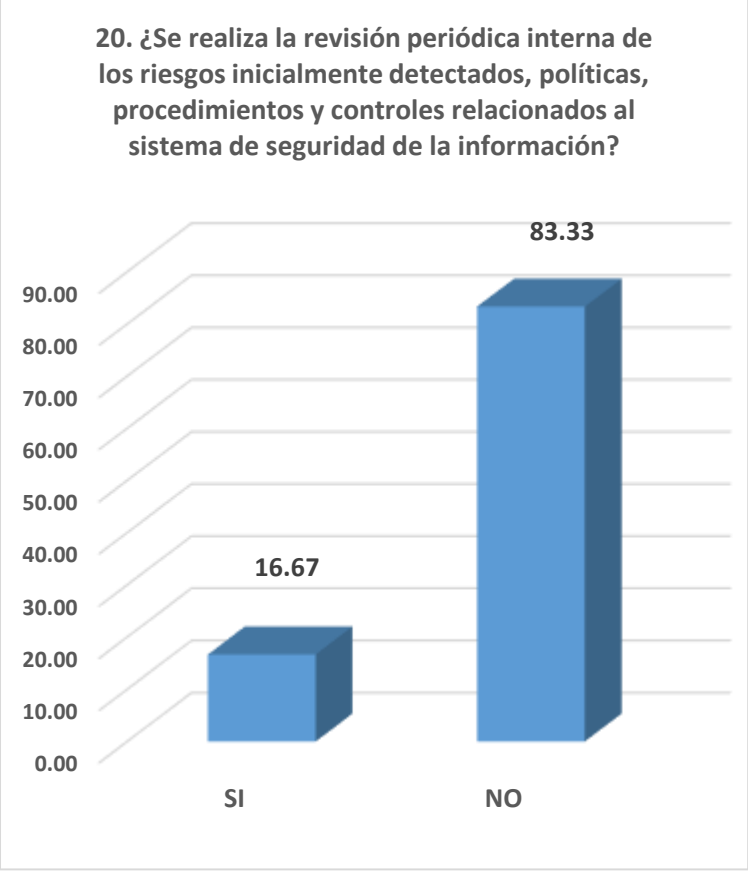


Figura 26: Sabe usted si se cuenta con software antivirus actualizado

Fuente: Elaboración propia

Análisis: En el gráfico podemos apreciar que del 100% de la encuesta, el 16.67% de los trabajadores de la Municipalidad distrital de Bellavista – Sullana, saben que se realiza una revisión periódica interna de los riesgos inicialmente detectados, políticas, procedimientos y controles relacionados al sistema de seguridad de la información, mientras un 100.00% no saben acerca de esta revisión.

ACTA DE CONSTITUCIÓN DEL PROYECTO CÓDIGO 001 versión 1					
PROYECTO	Sistema de Seguridad de la Información para el Centro de Operaciones, Emergencia y Monitoreo (COEM) de la Municipalidad Distrital de Bellavista - Sullana				
PATROCINADOR	Gerencia Municipal				
PREPARADO POR:	Joan Isaac Pulache Rosales	FECHA	17	10	2018
REVISADO POR:	Haiver Chinchay Navarro				
APROBADO POR:	Gerencia Municipal				

REVISIÓN (Correlativo)	DESCRIPCIÓN (REALIZADA POR) (Motivo de la revisión y entre paréntesis quien la realizó)	FECHA 22 10 2018
01		
02		
	BREVE DESCRIPCIÓN DEL PRODUCTO O SERVICIO DEL PROYECTO	
	El producto del proyecto “Sistema de Seguridad de la Información para el Centro de Operaciones, Emergencia y Monitoreo (COEM) de la Municipalidad Distrital de Bellavista - Sullana”, permitirá proteger los activos de información de la institución, permitiendo de esta forma la justificación del cumplimiento de los objetivos para la institución y la reducción de los riesgos de seguridad de la información mediante el empleo de controles. Se identifica en los siguientes entregables: • Política de Seguridad • Inventario de Activos • Análisis de Riesgo • Gestión de Riesgos • Plan de Tratamiento de Riesgo • Declaración de Aplicabilidad	

ALINEAMIENTO DEL PROYECTO

1. OBJETIVOS ESTRATÉGICOS DE LA ORGANIZACIÓN (A qué objetivo estratégico se alinea el proyecto)	2. PROPÓSITO DEL PROYECTO (Beneficios que tendrá la organización una vez que el producto del proyecto esté operativo o sea entregado)
El objetivo del área de la Municipalidad Distrital de Bellavista, es brindar una mayor seguridad a la ciudadanía del distrito mediante el registro de video y la disminuir el tiempo de respuesta antes un hecho delictivo, de servicio u apoyo.	Enfocar la organización hacia la generación creciente de valor, así como también el acceso controlado e integridad de la información; estableciendo los controles para identificar y mitigar los riegos operativos, informáticos, financieros y de los colaboradores basados en la norma ISO 27001:2013.

3. OBJETIVOS DEL PROYECTO
(Principalmente en términos de costo, tiempo, alcance, calidad)

- Alcance: El proyecto contempla la implementación de un SGSI en el Centro de Operaciones, Emergencia y Monitoreo (COEM) de la Municipalidad Distrital de Bellavista - Sullana.
- Tiempo: El proyecto debe culminar en un plazo máximo de 07 meses
- Costo: El presupuesto contempla un costo máximo S. 32,000.00 Soles, que incluye la consultoría.
- Calidad: Contar con personal capacitado y especializado en Seguridad de la información y Gestión de Proyectos.
- Elaborar un marco de referencia para asegurar que lo elementos del Sistema de Seguridad de la Información sean los apropiados y sirvan de apoyo como guía y control cuando el proyecto se ejecute.
- Establecer las expectativas de la gerencia con respecto al uso que el personal debe hacer de los activos de información de la Municipalidad Distrital de Bellavista – Sullana, así como las medidas que se deben adoptar para la protección de estos recursos.
- Infundir en todo el personal de la entidad la conciencia de la necesidad de la seguridad de la información y la comprensión de sus responsabilidades individuales.

4. FACTORES CRÍTICOS DE ÉXITO DEL PROYECTO
(Componentes o características que deben cumplirse en el proyecto para considerarlo exitoso)

- Asignación del recurso humano calificado y experimentado en proyectos similares a tiempo completo por parte la Municipalidad Distrital de Bellavista – Sullana.
- Adecuada comunicación de todas las partes involucradas en el proyecto.
- Aceptación de los resultados del proyecto por parte del personal de la empresa.
- Entrega de documentos en los plazos establecidos

5. REQUISITOS DE ALTO NIVEL
(Condiciones o características que deben cumplirse para satisfacer lo solicitado al proyecto)

- Aprobación del Acta de Constitución del Proyecto

- Elaboración del acta de constitución del proyecto (EDT/WBS)
- Cumplimiento con la Norma ISO 27001:2013, personal capacitado y con experiencia en el desarrollo o implementación de proyectos en Seguridad de la información.
- Documento del Inventario de Activos de Información del Centro de Operaciones, Emergencia y Monitoreo (COEM) de la Municipalidad Distrital de Bellavista - Sullana, contar con las herramientas necesarias para su desarrollo.
- Documento de la Política de seguridad de la Información.
- Documento entrevistas a Experto y usuarios.
- Documento de la Declaratoria de Aplicabilidad del proyecto.
- Personal con Experiencia.

EXTENSIÓN Y ALCANCE DEL PROYECTO	
6. FASES DEL PROYECTO (Agrupamiento lógico de actividades relacionadas que usualmente culminan elaborando un entregable principal)	**7. PRINCIPALES ENTREGABLES** (Un único y verificable producto, resultado o capacidad de realizar un servicio que debe ser elaborado para completar un proceso, una fase o un proyecto)
El Proyecto consta de las fases de que sigue las cuales se alinean en la metodología del ISO 27001. Inicio	• Acta de Constitución del Proyecto. • Introducción a la Norma ISO 27001:2013 • Objetivos del SGSI.
Planificación	• Desarrollar el plan de Gestión del proyecto • Crear EDT • Diccionario del EDT • Planificar la Gestión de Riesgos • Identificar los Riesgos • Realizar análisis • Cualitativos de Riesgos • Realizar el Análisis Cuantitativo de riesgos • Planificar la respuesta a los riesgos • Descripción de la Empresa. • Objetivos del Negocio • Situación Actual de La empresa ▪ Infraestructura de Seguridad de la Información

	▪ Alcance • Definición de la Política de Seguridad de la Información. ▪ Objetivos ▪ Alcance ▪ Dominios de la ISO 27001 :2013 o Política de seguridad de la Información. o Organización de la Seguridad de la Información. o Seguridad de los Recursos Humanos. o Gestión de Activos o Control de Accesos o Criptografía o Seguridad Física y del Entorno. o Seguridad de las Operaciones o Seguridad de la Comunicaciones o Adquisición, desarrollo y mantenimiento de sistemas. o Relación con los Proveedores. o Gestión de los Incidentes de Seguridad de la Información. o Aspectos de seguridad de la información de la gestión de continuidad de negocio o Cumplimiento
Ejecución	• Análisis de Riesgo ▪ Procesos del Negocio ▪ Inventario de Activos ▪ Valoración de Activos ▪ Identificación de Amenazas. ▪ Valoración de Riesgo por Activo. ▪ Tratamiento del Riesgo.
Seguimiento y Control	• Declaratoria de Aplicabilidad.
Cierre	• Informe Final.

INTERESADOS CLAVE

- Alcaldía
- Gerencia Municipal
- Unidad de Estadística y Tecnologías de la Información
- Gerencia de Seguridad Ciudadana
- Unidad de Imagen Institucional
- Gerencia de obras Públicas y Proyectos
- Gerencia de Servicios Comunales
- Sub Gerencia de Limpieza Pública, Parques y Jardines
- Sub Gerencia de Tránsito y Seguridad Vial

- Sub Gerencia de Comercialización
- Sub Gerencia de Limpieza Pública, Parques y Jardines
- Sub Gerencia de Tránsito y Seguridad Vial
- Sub Gerencia de Gestión Ambiental
- Sub Gerencia de Fiscalización y Policía Municipal
- Sub Gerencia de Defensa Civil
- Gerencia de Desarrollo Social
- Oficina de Administración y Finanzas
- Oficina de Asesoría Jurídica
- Personal de la entidad pública
- Población del distrito

RIESGOS

(Evento o condición incierta que, si ocurriese, tiene un efecto positivo o negativo sobre los objetivos del proyecto)

- Escaso compromiso con el personal involucrado en el proyecto
- Demora en las fases del proyecto
- Retraso en el financiamiento del proyecto
- Incumplimiento de plazos en la entrega de los resultados.
- No contar con personal calificado.

HITOS PRINCIPALES DEL PROYECTO

(Un evento significativo para el proyecto)

- Aprobación de proyecto por la Gerencia Municipal.
- Desarrollo de entrevistas con usuarios y expertos.
- La verificación de los procesos se desarrolle en el plazo pactado.
- Proceso de Inventarios de Activos.
- La entrega del producto debe ser menor o igual al tiempo estimado.

PRESUPUESTO DEL PROYECTO

(Áreas de la organización que tienen algo que aportar al proyecto o que se ven afectadas por su ejecución o su producto)

El costo del proyecto es asumido en un 100% por la Municipalidad Distrital de Bellavista - Sullana

REQUISITOS DE APROBACIÓN DEL PROYECTO

(Quién evalúa los FCE, decide el éxito del proyecto y quien cierra el proyecto)

FCE	Evaluador	Firma el Cierre del Proyecto
	Ing Jorge Luis Arroyo Tirado	Haiver Chinchay Navarro

• Asignación del recurso humano competente en el desarrollo de proyectos de automatización de ERP	Jefe de Recursos Humanos.	Gerencia Municipal
• Las áreas o personal involucrado deben de estar a disposición y responder con eficiencia para el desarrollo del proyecto	Responsables de áreas.	
• Aceptación del producto del proyecto por parte del área del Centro de Operaciones, Emergencia y Monitoreo (COEM).	Jefe del Centro de Operaciones, Emergencia y Monitoreo (COEM)	
• Entrega de documentos en los plazos establecidos	Gerente del Proyecto Pulache Rosales Joan Isaac	
GERENTE DE PROYECTO ASIGNADO AL PROYECTO Pulache Rosales Joan Isaac. / Gerente de Proyecto		
AUTORIDAD ASIGNADA Haiver Chinchay Navarro		
Jefe de Estadística y Tecnologías de la Información		

Tabla 3: ACTA DE CONSTITUCION DEL PROYECTO

Fuente: Elaboración propia

IV. DISEÑO METODOLOGICO DE LA NORMA ISO 27001:2013

La investigación se basa en el desarrollo de la Norma Internacional ISO 27001:2013, es por ello que se presenta los siguientes alcances.

Para la consideración del proyecto se realizará las siguientes fases:

Fases	Consideración
Norma ISO 27001: 2013	• Introducción a la Norma ISO 27001:2013 • Objetivos del SGSI.

IV.1 Análisis de la Empresa	• Descripción de la Empresa Descripción de los casos de uso
	• Objetivos del Negocio
	  o Infraestructura de Seguridad de la Información
	  o Alcance
	• Definición de la Política de Seguridad de la Información
	• Objetivos
	• Alcance
	• Dominios de la ISO 27001:2013
	  o Política de seguridad de la Información
	  o Organización de la Seguridad de la Información.
	  o Seguridad en los Recursos Humanos.
	  o Gestión de Activos
	  o Control de Accesos
	  o Criptografía
	  o Seguridad Física y del entorno
	  o Seguridad en las Operaciones
	  o Seguridad de las comunicaciones
	  o Adquisición, desarrollo, y mantenimiento de sistemas
	  o Relaciones con los Proveedores.
	  o Gestión de los Incidentes de Seguridad de la Información
	  o Aspectos de seguridad de la Información de la Gestión de la continuidad del Negocio.
	  o Cumplimiento

IV.2 Análisis de Riesgos	• Procesos del Negocio • Inventario de Activos • Valoración de Activos • Identificación de Amenazas • Valoración de Riesgo por Activo. • Tratamiento del Riesgo.
Declaración de Aplicabilidad	• Controles Aplicados

Tabla 4: FASES DE ISO

Fuente: elaboración propia

V. APLICACIÓN DE LA NORMA ISO 27001:2013

NORMA ISO 27001: 2013

Introducción a la norma ISO 27001:2013

Es un modelo de gestión de seguridad de la información, el cual se define como un conjunto de lineamientos el cual especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. Estos requisitos describen cual es el comportamiento esperado del sistema de Gestión una vez que esté en funcionamiento; por lo tanto, para el desarrollo del proyecto se tomó a la Norma ISO 27001:2013 como marco de referencia en la implementación del Sistema de Gestión de Seguridad de la información.

La ISO 27001:2013 cuenta con 114 controles, 14 Dominios de Seguridad y 130 Requisitos de Gestión.

Objetivos del sistema de gestión de seguridad de la información

- Llevar a cabo el análisis de riesgos, identificando amenazas, vulnerabilidades e impactos en la Entidad Pública en estudio con el objetivo de proporcionar una mejora en la adopción de la norma en cuanto a la forma de trabajo con respecto a la seguridad de la información.
- Una mejora continua en la gestión de la seguridad, en consideración al control de personas que interactúan en los procesos.
- Garantía de continuidad y disponibilidad del negocio.
- El incremento de los niveles de confianza tanto para sus trabajadores de la entidad pública, así como a toda la población del distrito de Bellavista - Sullana.

ANÁLISIS DE LA EMPRESA

DESCRIPCIÓN DE LA EMPRESA

La entidad pública es considerada para el desarrollo de aplicación de la Norma ISO 27001:2003 es la Municipalidad Distrital de Bellavista, siendo pionera en implantar un Centro de Operaciones, Emergencia y Monitoreo del norte del país con su propia red de fibra óptica con 30 cámaras de última tecnología instaladas en puntos críticos de la ciudad.

La sede del Centro de Operaciones, Emergencia y Monitoreo (COEM) de la Municipalidad Distrital de Bellavista – Sullana, está ubicada en la calle Madre de Dios esquina Transversal Canchaque S/N, actualmente trabajan unas 13 personas.

Visión: Satisfacer a la ciudadanía de Bellavista con los fundamentos primordiales y crear una participación uniforme basada en una administración rígida por los lineamientos que dicta la ley de nuestro país. En busca de una mejor calidad de vida para los habitantes de nuestro distrito, orientándola con una Gestión Municipal bajo la premisa de honestidad, servicio y atención al ciudadano del Distrito De Bellavista.

Misión: Ofrecer un sistema de Gestión participativa que garantice el desarrollo sostenible del Distrito de Bellavista, manteniendo niveles óptimos de servicios públicos, desarrollando una infraestructura moderna, Valores comunes e identidad colectiva, propia; bajo una administración correcta y planificada de los recursos originados y gestionados.

Objetivos del Negocio: Brindar una mayor seguridad a la ciudadanía del distrito mediante el registro de video y la disminuir el tiempo de respuesta antes un hecho delictivo, de servicio u apoyo.

ORGANIGRAMA DE LA MUNICIPALIDAD DISTRITAL BELLAVISTA – SULLANA

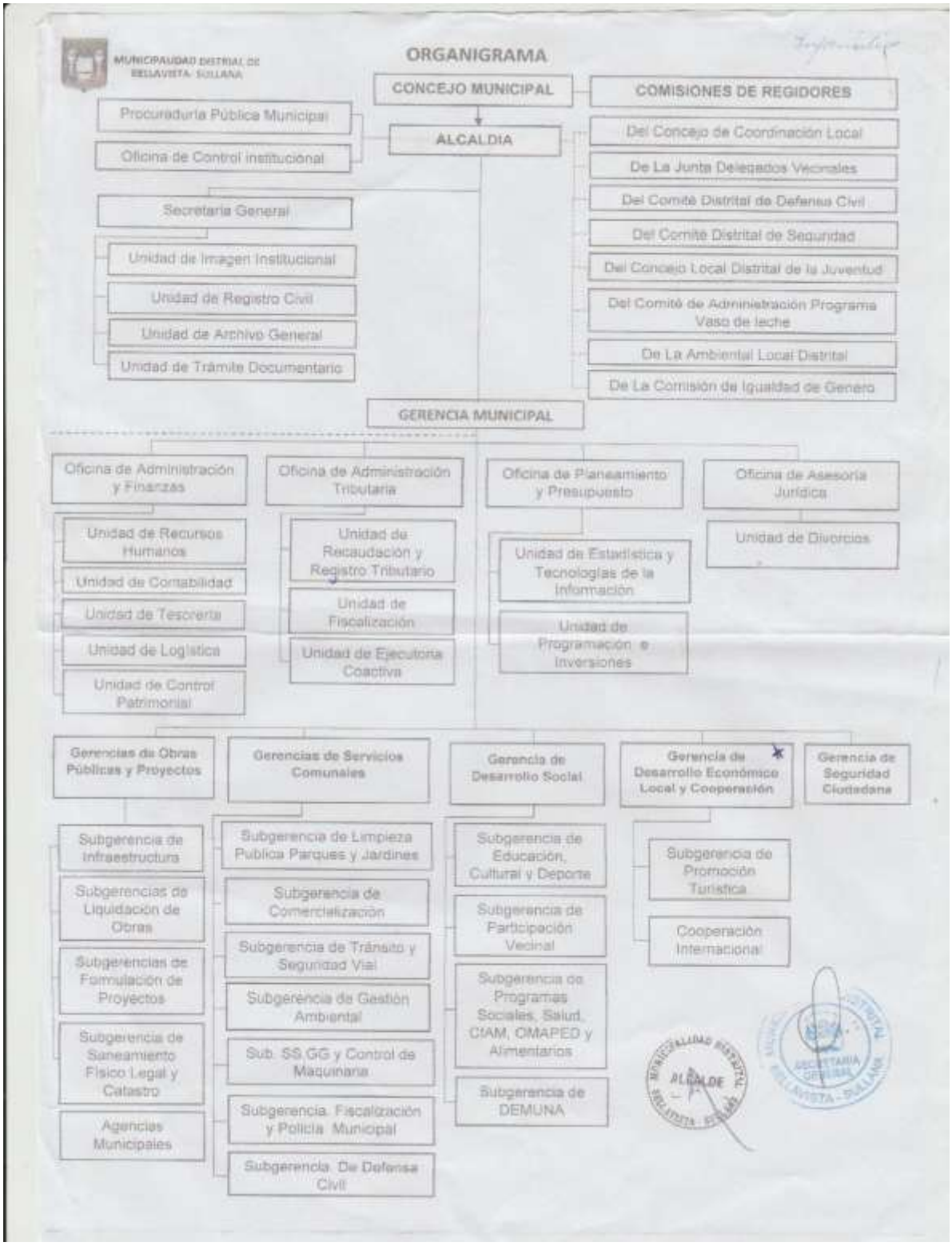


Figura 27: Organigrama de Municipalidad Distrital de Bellavista - Sullana

Fuente: Municipalidad Distrital de Bellavista – Sullana

ALCANCE

El Sistema de gestión de seguridad de la información se basa en la Norma ISO 27001:2013, el cual está limitado al área del Centro de Operaciones, Emergencia y Monitoreo (COEM) de la Municipalidad Distrital de Bellavista - Sullana, considerando esta área sensible ante una pérdida o fuga de información u activo, además se limita a la fase de desarrollo, ya que para una posible implementación sería necesario una inversión en recurso de tiempo, económico y humano por parte de la entidad pública.

DEFINICIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

La política de Seguridad es un conjunto de normas y procedimientos de obligado cumplimiento para el tratamiento de los riesgos de seguridad de la Entidad Pública.

OBJETIVOS DE ISO

Con la propuesta de la política se pretende conseguir lo siguiente:

- Elaborar un marco de referencia para asegurar que lo elementos del Sistema de Seguridad de la Información sean los apropiados y sirvan de apoyo como guía y control cuando el proyecto se ejecute.
- Establecer las expectativas de la gerencia con respecto al uso que el personal debe hacer de los activos de información de la Municipalidad Distrital de Bellavista - Sullana, así como las medidas que se deben adoptar para la protección de estos recursos.
- Infundir en todo el personal de la empresa la conciencia de la necesidad de la seguridad de la información y la comprensión de sus responsabilidades individuales.

ALCANCE

Dentro del alcance de la política de Seguridad de la información se encuentra involucrado todo el personal que forma parte del área del Centro de Operaciones, Emergencia y Monitoreo (COEM) los cuales interactúen con los activos de información del área en mención.

DOMINIOS DE LA ISO 27001:2013

Política de Seguridad de la Información

Normas y exigencias para los trabajadores para la protección de la confidencialidad integridad y disponibilidad en los activos de información en la compañía

Organización de la seguridad de la información

Identificación de roles dentro del sistema de gestión de seguridad de la información, para asignar responsabilidades y acuerdos de confidencialidad correspondientes

Seguridad en los recursos humanos.

Se encarga de asegurarse de que los empleados, contratistas y terceros entiendan y conozcan sus responsabilidades en cuanto a la protección de la información y estén capacitados adecuadamente para el rol que desempeñan dentro de la organización, para reducir el riesgo de robo, fuga de la información y fraude.

Gestión de activos

Identificación y clasificación de activos en la compañía asignando responsables y clasificando la información de acuerdo a su valor, Requerimientos legales, confidencialidad y grado crítico para la organización.

Control de accesos

Este control se encarga de vigilar el acceso adecuado a la información, asegurándose que la manipulación de los sistemas de información se encuentre autorizado y controlado por la organización, como permisos para modificar información, asignación de privilegios para utilizar aplicaciones entre otros.

Criptografía

Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

Seguridad física y del entorno

Se encarga de asegurarse de que la organización cumpla la seguridad adecuada, para evitar el acceso físico no autorizado daño e interferencia al local y la información de la compañía esto abarca al tema de cámaras de videovigilancia etc.

Seguridad en las operaciones

Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

Seguridad de las comunicaciones

Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

Adquisición, desarrollo, y mantenimiento de sistemas.

Se encarga de asegurarse que la seguridad sea una parte importante en los sistemas de información para evitar errores, pérdidas, modificación no autorizada o mal uso de la información por medio de las aplicaciones de la organización.

Relaciones con los proveedores.

Asegurar la protección de los activos de la entidad pública, ABZ Ingenieros se encarga de la garantía, soporte, configuración de todos los equipos e infraestructura (hasta Julio del 2019).

Gestión de los incidentes de seguridad de la información.

Se asegura que la información proveniente de eventos y vulnerabilidades en la seguridad de la información no se encuentran asociados a un sistema de información de la entidad pública, siendo comunicados y conocidos por otros medios por la gerencia de seguridad de ciudadana o partes interesadas de manera que no permiten tomar una decisión correctiva acertada y rápida.

Aspectos de seguridad de la información de la gestión de la continuidad del negocio.

Se encarga de implementar controles adecuados para contrarrestar las interrupciones de las actividades críticas para la entidad pública por efectos de fallas o desastres importantes en los sistemas de información, asegurándose que se reanude el proceso de manera correcta y segura.

Cumplimiento

Se encarga de que el sistema de gestión de seguridad de la información se acomode a la normatividad que exige la legislación del país como por ejemplo derechos de propiedad intelectual protección de data y privacidad de información persona.

PLAN DE GESTION DEL PROYECTOS

NOMBRE DEL PROYECTO	SIGLAS DEL PROYECTO
SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA EL CENTRO DE OPERACIONES, EMERGENCIA Y MONITOREO (COEM) DE LA MUNICIPALIDAD DISTRITAL DE BELLAVISTA - SULLANA	SIS_GEST_SEGU_INFOR_COEM_BESU

PROCESOS DE GESTIÓN DE PROYECTOS:

ENTRAGABLES	ENTRADAS	MODO DE TRABAJO	SALIDAS	HERRAMIENTAS Y TÉCNICAS
PROYECT CHARTER	Acuerdos, Enunciado del Trabajo	Mediante reunión entre el director de proyecto y el cliente	Contrato	Juicio de Expertos

CRONOGRAMA	Lista de Actividades	Reunión del equipo, estimación de la duración de las actividades	Calendario del Proyecto	Ruta critica
PLAN DE DIRECCIÓN DEL PROYECTO	Acta de Constitución del proyecto	Reuniones del equipo de proyecto	Plan de dirección del Proyecto Aprobado	Juicio de Expertos
ACTA DE COMITÉ DE SISTEMAS	Plan de Gestión de Comunicaciones		Actualización documentos	Reuniones
ACTA DE REUNIONES DE TRABAJO	Plan de Gestión de Comunicaciones	Reuniones formales e informales, distribución documentación	Actualización documentos	Reuniones
INFORMES DE DESEMPEÑO	Cronograma		Actualización documentos avance trabajo	Formato Excel
PLAN DE PRUEBAS	Plan de gestión de Calidad		Solicitudes de cambio	
INFORME DE CIERRE	Plan de Gestión de Comunicaciones		Actualización documentos	Formato Excel
ACTA DE CIERRE	Plan de Gestión de Comunicaciones		Actualización documentos	Reuniones

ENFOQUE DE TRABAJO:

- Inicialmente definió el alcance del proyecto
- Se establecen los documentos necesarios

- Se establecen los roles, responsabilidades y las fecha en que deberán estar listos
- Se realizan reuniones semanales para controlar el estado del proyecto
- Al término del proyecto se verifica la entrega de todos los entregables y se redactan los documentos de cierre del proyecto

CONTROL DE CAMBIOS:	
APROBADOR DE CAMBIOS A REQUERIMIENTOS	- Autoriza la presentación de una solicitud de cambio. Autoriza la solicitud de un cambio.
PROVEEDOR DE CAMBIOS A REQUERIMIENTOS	- Solicita cambios a los requerimientos acordados. - Solicita nuevos requerimientos sobre aquellos que están en curso. - Resuelve consultas acerca de los cambios en requerimientos que solicita.
COMUNICACIÓN ENTRE STAKEHOLDERS:	
NECESIDADES DE COMUNICACIÓN DE LOS STAKEHOLDERS	TÉCNICAS DE COMUNICACIÓN A UTILIZAR
ACTAS DE COMITÉ	Agenda de Reunión
AGENDA DE REUNIÓN	Agenda de Reunión
ACTAS DE REUNIÓN DE TRABAJO	Agenda de Reunión
CRONOGRAMA DE AVANCE DEL PROYECTO	Agenda de Reunión
CICLO DE VIDA DEL PROYECTO Y ENFOQUE MULTIFASE:	
CICLO DE VIDA DEL PROYECTO	ENFOQUES MULTIFASE

FASE DEL PROYECTO	ENTREGABLE RINCIPAL DE LA FASE	CONSIDERACIONES PARA LA INICIACIÓN DE ESTA FASE	CONSIDERACIONES PARA EL CIERRE DE ESTA FASE
INICIO	ProyectCharter	Proyect Charter aceptado	Proyect Charter aceptado
SEGUIMIENTO	Informes de Desempeño	Cronograma e indicadores de desempeño	Informe semanal de avance
EJECUCIÓN	Plan de Pruebas	Plan de gestión del proyecto	Pruebas aceptadas
CIERRE	Informe de Cierre	Entregable aceptado	Finiquito de cierre y lecciones aprendidas

REVISIONES DE GESTIÓN:

TIPO DE REVISIÓN DE GESTIÓN	CONTENIDO	EXTENSIÓN O ALCANCE	OPORTUNIDAD
DE AVANCE	Revisiones de avance y desarrollo del cronograma	Se finaliza con acta de reunión firmada por los asistentes	Quincenal Regular
DE CONTROL	Revisiones de indicadores y las mediciones de desempeño y calidad del producto	Se finaliza con informe interno para monitorear avance de las actividades y las acciones correctivas	Semanal Regular
EXTRAORDINARIA	Problemas generados por riesgos y nuevos requerimientos	Se desarrolla de manera exclusiva y se finaliza con un acta y una actualización del cronograma luego de analizar el impacto	En caso de alto riego o cuando se presente problemas

Tabla 5: Plan de Gestion del Proyecto

Fuente: elaboración propia

ESTRUCTURA DETALLADA DE TRABAJO (EDT)

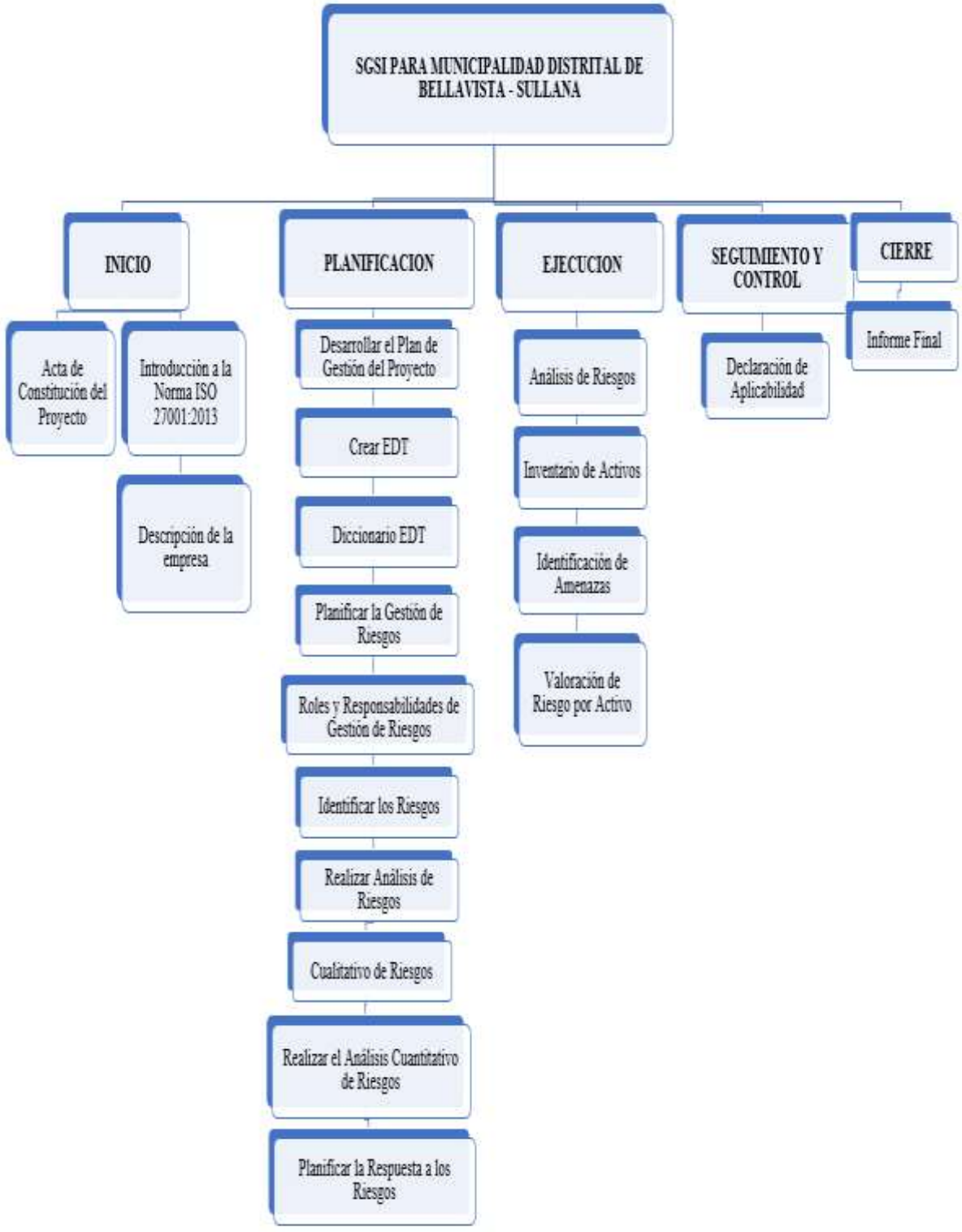


Figura 9: EDT

Fuente: Elaboración Propia

DICCIONARIO DEL EDT

Diccionario de la EDT					
Nombre del Proyecto:	Sistema de Seguridad de la Información para el Centro de Operaciones, Emergencia y Monitoreo (COEM) de la Municipalidad Distrital de Bellavista - Sullana				
Preparado por:	Joan Isaac Pulache Rosales		Fecha de Preparación:	18-10-18	
Revisado por:	Haiver Chinchay Navarro		Fecha Modificación:	24-10-17	
Autorizado por:	Gerencia Municipal				
Análisis de Riesgos					
Identificación del entregable	Encuestas				
Nombre del entregable	Resultados				
Alcance del Trabajo	Realizar análisis de los Riesgos existentes.				
Responsable	Gerencia Municipal				
Duración estimada 210 días	Fecha inicio	18 octubre	Fecha fin	23 mayo	
Requisitos de calidad	Realizar análisis de los Riesgos existentes. Descripción Categoría Proceso de negocio (Área del Centro de Operaciones, Emergencia y Monitoreo (COEM) de la Municipalidad Distrital de Bellavista - Sullana)				
Otras referencias					
Hitos del cronograma	Costos				

Tabla 6: Diccionario del EDT

Fuente: Elaboración Propia

PLANIFICAR LA GESTIÓN DE RIESGOS

Nombre del Proyecto	Siglas del Proyecto
Sistema de Seguridad de la Información para el Centro de Operaciones, Emergencia y Monitoreo (COEM) de la Municipalidad Distrital de Bellavista - Sullana	SIS_GEST_SEGU_INFOR_COEM_BESU

Tabla 7: Datos del Proyecto

Fuente: Elaboración Propia

En toda actividad que realicemos siempre existen riesgos, por eso es muy importante elaborar un Plan de Gestión de Riesgos cuyo contenido indica los diferentes tipos de riesgos que podemos encontrar y cuáles son las posibles causas, además de cómo prevenir y responder a estos posibles riesgos en caso de que sucedieran.

Equipo de gestión de riesgos:

El equipo de gestión de riesgos estará conformado por el director de proyecto (DP), analista de sistemas (AS) y los programadores.

Metodología

- **Realizar taller con el equipo para:**

  Identificar riesgos

  Planificar la respuesta a riesgos

Metodología de cálculo para análisis cualitativo de riesgos:

1. La probabilidad de ocurrencia de cada uno de los riesgos detectados se valorará según lo indicado.
2. se evaluará el impacto de los riesgos detectados, según el juicio de los participantes, sobre cada uno de los objetivos afectados (costo, calidad, tiempo y alcance).
3. Se definirá el tipo de riesgo según lo obtenido luego de efectuar la sumatoria de la multiplicación de la probabilidad e impacto, sobre cada uno de los objetivos afectados.

MATRIZ DE IMPACTO Y PROBABILIDADES		MUY BAJO	BAJO	MODERADO	ALTO	MUY ALTO
		0.1	0.2	0.4	0.6	0.9
MUY ALTO	9	0.9	1.8	3.6	5.4	8.1
ALTO	7	0.7	1.4	2.8	4.2	6.3
MODERADO	5	0.5	1	2	3	6.3
BAJO	3	0.3	0.6	1.2	1.8	2.7
MUY BAJO	1	0.1	0.2	0.4	0.6	0.9

UMBRALES	RANGO	CATEGORIA
	8.1 - 2.9.	ALTO
	2.8 - 1.4	MODERADO
	1.3 - 0.1	BAJO

Tabla 8: Matriz de Impactoy Probabilidades

Fuente: Elaboración Propia

Plantillas:

La identificación de riesgos y el análisis cualitativo de riesgos se llevará a cabo utilizando plantillas normalizadas de la organización.

Monitoreo y control:

Se efectuará monitoreo y control al plan de gestión de riegos, en cada una de las reuniones de seguimiento semanal del proyecto, procediendo según se indica a continuación:

a) Reevaluar y clasificar riesgos identificados.

b) Identificar y clasificar nuevos riesgos.

c) De acuerdo con la nueva clasificación de riesgos proceder como se indica a continuación:

- Riesgo muy alto o alto: si es interno, evitar el riesgo, no avanzar en el proyecto hasta no disminuir la clasificación. Si el riesgo es externo, transferir impactos al causante (cliente), de acuerdo con condiciones del contrato.
- Riesgo medio: tomar acciones para mitigar (disminuir probabilidad o el impacto).
- Riesgo bajo: dejar por escrito qué se hará cuando ocurra ese riesgo.
- Riesgo muy bajo: no se tomará ninguna acción al respecto.

d) Se dejará registro del monitoreo y control realizado, utilizando misma plantilla de identificación y evaluación de riesgos, agregando las acciones a emprender y el responsable.

PROCESO	ROLES	PERSONAS	RESPONSABILIDADES
11.1. PLANIFICAR LA GESTIÓN DE RIESGOS	1. Definir los planes a alto nivel para efectuar la gestión de riesgos 2. Desarrollar los elementos de costos de la gestión de riesgos para incluirlos en el presupuesto 3. Revisar las metodologías para la aplicación de las reservas para contingencias en materia de riesgos	Equipo de gestión.	1. Gerente de Proyecto 2. Equipo 3. Gerente de Proyecto
11.2. IDENTIFICAR LOS RIESGOS	1. Fomentar la identificación de riesgos por todo el personal del equipo de proyecto	Gerente de Proyecto	1. Gerente de Proyecto
11.3. REALIZAR EL ANÁLISIS CUALITATIVO DE RIESGOS	1. Evaluar la prioridad de los riesgos usando la probabilidad relativa de ocurrencia 2. Evaluar la prioridad de los riesgos identificados usando el impacto sobre los objetivos del proyecto, si los riesgos se presentan. 3. Evaluar la prioridad de los riesgos identificados usando el plazo de respuesta y la	Equipo de gestión.	1. Equipo 2. Equipo 3. Gerente de Proyecto

	tolerancia al riesgo por parte de la organización.		
11.5. PLANIFICAR LA RESPUESTA A LOS RIESGOS	1. Identificar y asignar a una persona para que asuma la responsabilidad de cada respuesta a los riesgos acordada y financiada 2. Introducir recursos y actividades en el presupuesto, el cronograma y el plan para la dirección del proyecto	Equipo de gestión.	1. Gerente de Proyecto 2. Equipo
11.6. MONITOREAR Y CONTROLAR LOS RIESGOS	1. Implementar planes de respuesta a los riesgos 2. Rastrear los riesgos identificados 3. Monitorear los riesgos residuales 4. Identificar nuevos riesgos 5. Evaluar la efectividad del proceso contra los riesgos a través del proyecto	Gerente de Proyecto Equipo de gestión Supervisor	1. Supervisores 2. Equipo 3. Equipo y supervisores 4. Gerente de Proyecto

PERIODICIDAD DE LA GESTIÓN DE RIESGOS			
PROCESO	**MOMENTO DE EJECUCIÓN**	**ENTREGABLE DEL EDT**	**PERIODICIDAD DE EJECUCIÓN**
Planificar la gestión de riesgos	Grupo de procesos de planificación		Mensual
Identificar los riesgos	Grupo de procesos de planificación		Semanal

Realizar el análisis cualitativo de riesgos	Grupo de procesos de planificación		Semanal
Planificar la respuesta a los riesgos	Grupo de procesos de planificación		Semanal
Monitorear y controlar los riesgos	Grupo de procesos de seguimiento y control		Diario

TABLA 9: Roles y Responsabilidades de Gestion de Riesgos

Fuente: Elaboración Propia

	RIESGO	DESCRIPCIÓN	CAUSA RAIZ	TRIGGER	ENTREG. AFECTADOS	TIPO DE RIESGO	ESTRATEGIA	RESPONSABLE
R01	Errores en la estimación del presupuesto	No se conocen bien los procesos o tareas a realizarse, lo que ocasiona que no se haya hecho una estimación adecuada	Mal gestión del conocimiento del equipo del proyecto.	Comunicación del cliente o detección de error.	Correspondiente a criterio modificado.	Muy Alta	Adecuado seguimiento y control a información de entrada.	DP, CP.
R02	Cambios en las políticas de gestión	Cambio en información de entrada.	Externo	Comunicación del cliente o detección de error.	Correspondiente a criterio modificado.	Alta	Adecuado seguimiento y control a información de entrada.	DP, EP.
R03	Seguridad del software	Cambio en información de entrada. Asignación de tareas a recurso inadecuado que	Interno	Consumo de tiempo mayor al programado.	Correspondiente a criterio modificado.	Alta	Adecuado seguimiento y control a criterios de diseño.	DP, CP,EP.

		requiere capacitación.						
R04	Cambios de alcance	Detección de errores en el proceso de revisión.	Externo	Nueva información de entrada, recibida del cliente.	Correspondiente a criterio modificado.	Muy Alta	Adecuado seguimiento y control a información de entrada.	DP, CP.
R05	Desconocimiento del flujo de procesos del cliente	Detección de errores en el proceso de revisión.		Comunicación del cliente o detección de error.	Correspondiente a criterio modificado.	Alta	Adecuado seguimiento y control a criterios de diseño.	DP
R06	Desconocimiento de la tecnología usada	Detección de errores en el proceso de revisión.	Externo	Consumo de tiempo mayor al programado.	Correspondiente a criterio modificado.	Alta	Adecuado seguimiento a consumo de recursos y llamado de atención oportuno al jefe de diseños.	DP, CP, EP
R07	Las pruebas de funcionamiento no resultan satisfactorias	Asignación de tareas a recurso inadecuado que requiere capacitación.	Interno	Consumo de tiempo mayor al programado.	Correspondiente a criterio modificado.	Alta	Adecuado seguimiento y control a criterios de diseño.	DP, EP.

Tabla 10: Identificacion, Evaluacion Plan de Respuesta a Riesgos

Fuente: Elaboración Propia

ANÁLISIS DE RIESGOS

Proceso del COEM	Descripción
Imágenes captadas por el operador	Ingreso de acceso al Sistema Operativo. Ingreso de acceso al jocstick. Ingreso de acceso al Sistema SSM Console Studio. Asignación de sectores con cámaras. Manejo de Cámaras por el operador.
Registro de datos C4I	Ingreso de acceso al Sistema Operativo. Ingreso de acceso al Sistema C4I. Ingreso de campos requeridos por el Sistema C4I.
Estación de Radio base	Se verifica ubicación del radio móviles y radios instaladas en las unidades vehiculares. Atender llamadas de radio móviles. Realizar llamadas para comunicar a radio móviles.
Central de llamadas	Realizar llamadas de emergencia. Atender llamadas de emergencia.
Solicitud de Copias de Video de Seguridad	Registrar datos del agraviado y realizar copia a denuncia. Realizar copias de video de seguridad formalmente previa solicitud de la comisaria del sector y con un efectivo policial a cargo. Asignar políticas de seguridad a copia de seguridad del video. Video entregado a mediante documento formal a comisaria del sector.
Solicitud de Video de Seguridad	Registrar datos al solicitante. Se procede si el solicitante del video es el agraviado y deberá ser acompañado por un efectivo policial además que el hecho delictivo se haya producido al menos una hora antes de esta solicitud.
Servicio Técnico (Coordinación con la empresa ABZ Ingenieros)	Se envía un correo electrónico para una Orden de Servicio Técnico (Apertura- Diagnostico y Cierre) Cambio de equipo por fallas técnicas, reincidencia de fallas.

Tabla 11: Procesos de negocio (Centro de Operaciones, Emergencia y Monitoreo (COEM) de la Municipalidad Distrital de Bellavista - Sullana)

Fuente: Elaboración Propia

INVENTARIO DE ACTIVOS

En este punto se procede a la identificación de los activos de información que forman parte de toda el área de Operaciones, tanto propietarios, personas o entidades encargadas del control del activo en todo su ciclo de vida y garantizar su seguridad, sin embargo, no se le atribuye derecho de autor sobre el mismo.

NOMBRE	DESCRIPCION	CATEGORIA	UBICACIÓN	PROPIETARIO
Equipo de Almacenamiento	Grabador de video NVR	Hardware	NVR	COEM
Equipo de comunicaciones	Torre Ventada	Ferretería	TORRE VENTADA TRIANGULAR	COEM
	Luz Baliza	Luminaria	TORRE VENTADA TRIANGULAR	
	Radio móvil para camionetas	Hardware	SISTEMA DE RADIOCOMUNICACIONES	
	Radio Repetidora	Hardware	SISTEMA DE RADIOCOMUNICACIONES	
	Radio Portátil	Hardware	SISTEMA DE RADIOCOMUNICACIONES	
	Duplexor	Dispositivo Electrónico	SISTEMA DE RADIOCOMUNICACIONES	
	Antena Base	Dispositivo Electrónico	SISTEMA DE RADIOCOMUNICACIONES	
	Central telefónica PBX OPENVOX	Hardware	CENTRAL TELEFONICA	
	Gateway digital DINSTAR MTG200	Hardware	CENTRAL TELEFONICA	
	Gateweay analógico DINSTAR DAG1000-8FXO	Hardware	CENTRAL TELEFONICA	
	Servidor de video Estándar	Hardware	Servidor	
	Switch administrable 24 Giga Puertos Multicapa (L2/L3)	Switch administrable 24 Giga Puertos Multicapa (L2/L3)	Switch	
	Switch administrable 24 Giga Puertos Capa	Switch administrable 24 Giga Puertos Capa	Switch	
	Switch Poe 24 Puertos 10/100 para Telefonía	Switch Poe 24 Puertos 10/100 para Telefonía	Switch	

	Equipo de Firewall Mikrotick	Equipo de Firewall	Firewall	
	Cámara domo, ptz, 32x ip opción onvif	Hardware	MONITOREO DE CAMARAS	
	Cámara Fija Tipo Domo	Hardware	MONITOREO DE CAMARAS	
Equipo de usuario	Impresora multifuncional	Hardware	SALA DE CRISIS	COEM
	Proyector Multimedia	Hardware	SALA DE CRISIS	
	Ecran Retráctil	Inmobiliario	SALA DE CRISIS	
	Mesa rectangular	Inmobiliario	SALA DE CRISIS	
	Teclado Digital con Joystick para Estación de trabajo, incluye fuente de	Hardware	MONITOREO DE CAMARAS	
	Monitor 21.5. para estaciones de trabajo de operadores	Hardware	MONITOREO DE CAMARAS	
	Monitor full HD 55", para Video Wall	Hardware	MONITOREO DE CAMARAS	
	UPS para estaciones de trabajo de CCTV	Dispositivo Electrónico	MONITOREO DE CAMARAS	
	Teléfono IP	Hardware	MONITOREO DE CAMARAS	
	Auricular HD ejecutivo	Hardware	MONITOREO DE CAMARAS	
	Monitor LCD de 21.5" para la estación de trabajo de incidencias	Hardware	MONITOREO DE CAMARAS	
	Servidor de emergencias (SAE)	Hardware	MONITOREO DE CAMARAS	
Equipo de Video	Equipo Sistema de Video Wall	Hardware	MONITOREO DE CAMARAS	COEM
Reportes de COEM	Reportes diarios y mensuales de las incidencias de video, oficios, informes, memorandos, requerimientos, copias de seguridad de video.	Documento.	Reporte del COEM	Trabajador asignado
Servicios	Internet	Subcontratación	Servicios	Movistar

	Energía Eléctrica Agua y desague Telefonía	Subcontratación Subcontratación Subcontratación	Servicios Servicios Servicios	ENOSA EPS Grau Movistar
Software comercial	Sistema de Video Wall	Software	MONITOREO DE CAMARAS	COEM
	Software de gestión de incidencias, geolocalización, APP Mobile, rastreo por GPS	Software	MONITOREO DE CAMARAS	
	Windows 10.1	Software	MONITOREO DE CAMARAS	
	Paquete completo SSM	Software	MONITOREO DE CAMARAS	
	SISTEMA DE ATENCION DE EMERGENCIAS - C4I	software	MONITOREO DE CAMARAS	
Trabajador	Personal propio de la entidad	Personal	Personal	Recursos Humanos

Tabla 12: Inventario de Activos

Fuente: Elaboración Propia

IDENTIFICACION DE AMENAZAS

Se procede a identificar las amenazas que pueden afectar a los activos. Una amenaza es cualquier acción o acontecimiento que pueda atentar contra nuestra seguridad.

- Amenazas Naturales (Tormentas, Terremotos, Inundaciones)
- Amenazas a Instalaciones (fuego, daños por agua, explosión, caída de energía, perdida de acceso, fallas eléctricas, fallas mecánicas)
- Amenazas Humanas (Huelgas, Epidemias, materiales peligrosos, problemas de transporte, perdida del personal clave)
- Amenazas Tecnológicas (virus, pérdida de datos, hacking, fallas de Software y de Hardware, fallas en las líneas de comunicación)
- Amenazas Operacionales (Crisis Financieras, fallas en equipos, errores de usuario)
- Amenazas Sociales (protestas, vandalismo, terrorismo, bombas, sabotaje, violencia laboral, extorsión)

DIAGRAMA DE ISHIKAWA DESASTRES NATURALES

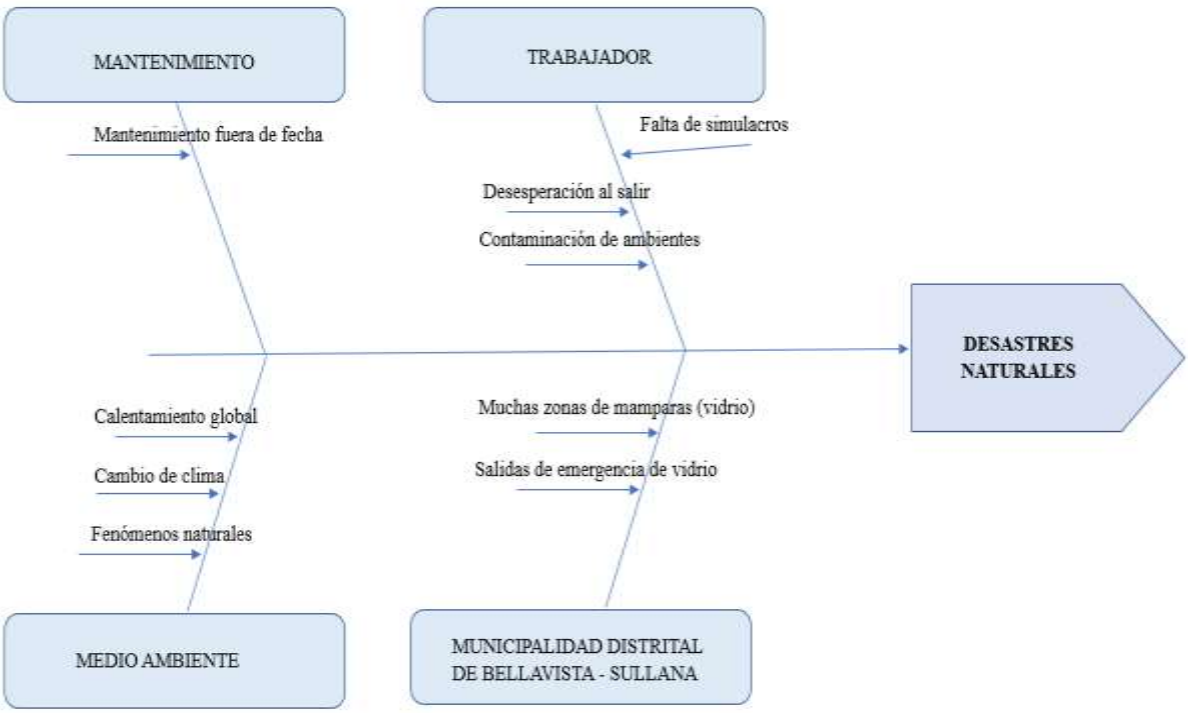


Figura 28: Ishikawa Desastres Naturales
Fuente: Elaboración Propia

DIAGRAMA DE ISHIKAWA AMENAZAS TECNOLOGICAS

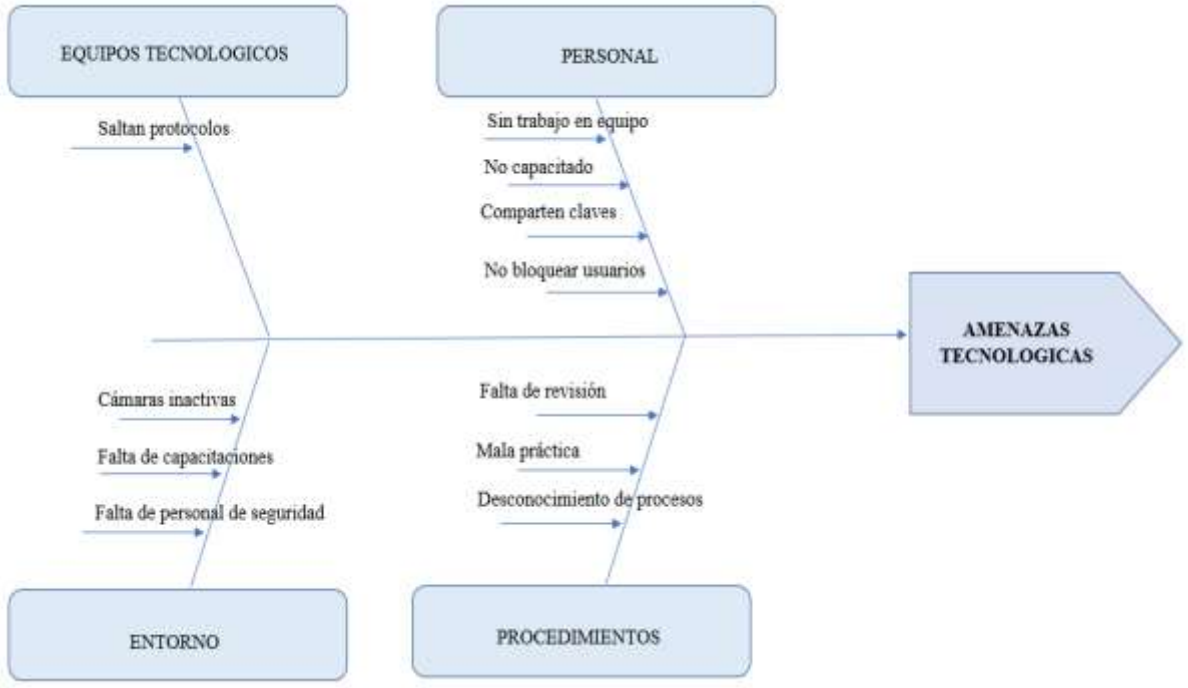


Figura 29: Ishikawa Amenazas Tecnológicas

Fuente: Elaboración Propia

DIAGRAMA DE ISHIKAWA PERDIDA DE PERSONAL

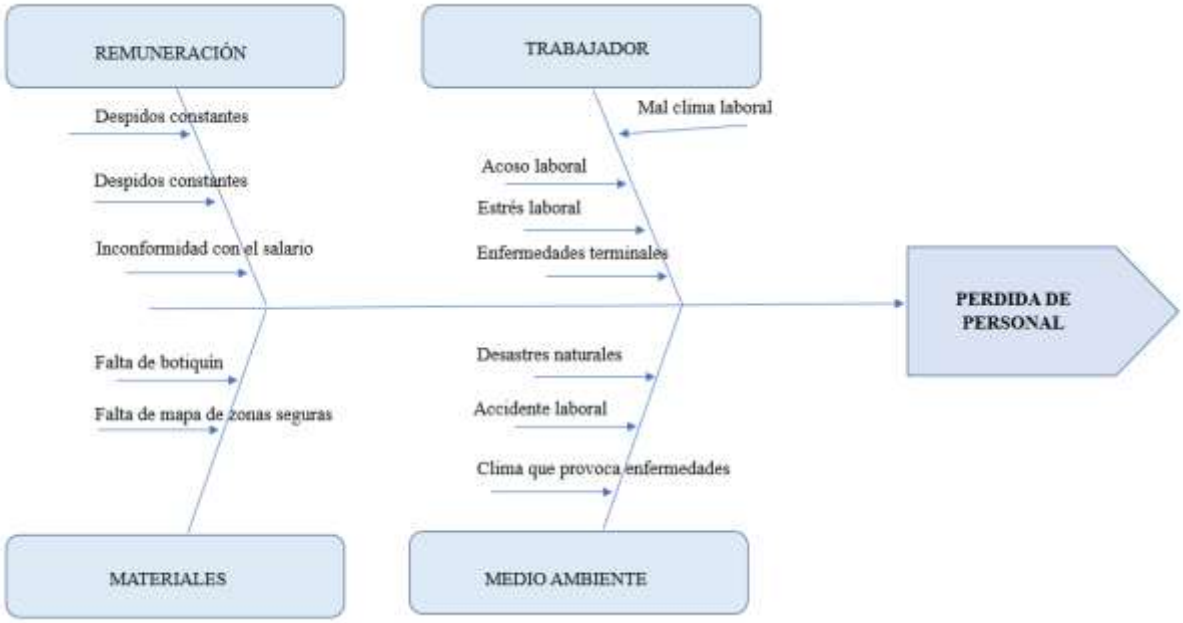


Figura 30: Ishikawa Perdida de Personal

Fuente: Elaboración Propia

VALORIZACIÓN DE ACTIVOS

Se valorizará los activos según las escalas de puntuación de 0 (no aplicable /sin valor) a 4 (mucho valor). La suma aritmética de los 4 valores. Valorización total.

Activos	Confidencial	Integridad	Disponibilidad	Total
Equipo de Almacenamiento	4	4	4	12
Equipo de comunicaciones	4	4	4	12
Equipo de usuario	3	3	3	9
Equipo de Video	3	4	3	10
Reportes de COEM	4	4	3	11
Servicios	3	3	3	9
Software comercial	2	4	3	9
Trabajador	3	4	3	10

Tabla 13: Valoracion de Activos

Fuente: Elaboración Propia

VALORACIÓN DE RIESGO POR ACTIVO

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Inundaciones, sismos, incendios)	6	1	1	6
Humanas (Robo, renuncias, huelgas, accidentes)	6	1	1	6
Instalaciones (energía, explosión, fuego, fallas)	6	2	2	24
Tecnológicas (Software, Hardware, Red, Virus, Hacking)	6	3	2	36
Operacionales (errores usuario)	6	2	1	12

Tabla 14: Aplicaciones Comerciales

Fuente: Elaboración Propia

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Tormentas, Terremotos, Inundaciones)	12	1	0	0
Humanas (Huelgas, Epidemias, materiales peligrosos, problemas de transporte, perdida del personal clave)	12	1	1	12
Instalaciones (fuego, daños por agua, explosión, caída de energía, perdida de acceso, fallas eléctricas, fallas mecánicas)	12	1	1	12
Tecnológicas (virus, pérdida de datos, hacking, fallas de Software y de Hardware, fallas en las líneas de comunicación)	12	2	3	72

Operacionales (Crisis Financieras, fallas en equipos, errores usuarios)	12	2	2	48

Tabla 15: Equipo de Almacenamiento
Fuente: Elaboración Propia

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Tormentas, Terremotos, Inundaciones)	12	1	0	0
Humanas (Huelgas, Epidemias, materiales peligrosos, problemas de transporte, perdida del personal clave)	12	1	1	12
Instalaciones (fuego, daños por agua, explosión, caída de energía, perdida de acceso, fallas eléctricas, fallas mecánicas)	12	1	1	12
Tecnológicas (virus, pérdida de datos, hacking, fallas de Software y de Hardware, fallas en las líneas de comunicación)	12	2	3	72
Operacionales (Crisis Financieras, fallas en equipos, errores usuarios)	12	2	2	48

Tabla 16: EQUIPO DE COMUNICACIONES

Fuente: Elaboración Propia

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Tormentas, Terremotos, Inundaciones)	9	2	2	36
Humanas (Huelgas, Epidemias, materiales peligrosos, problemas de transporte, perdida del personal clave)	9	2	2	36

Instalaciones (fuego, daños por agua, explosión, caída de energía, perdida de acceso, fallas eléctricas, fallas mecánicas)	9	3	2	54
Tecnológicas (virus, pérdida de datos, hacking, fallas de Software y de Hardware, fallas en las líneas de comunicación)	9	2	3	54
Operacionales (Crisis Financieras, fallas en equipos, errores usuarios)	9	2	2	36

TABLA 17: Equipo de Usuario

Fuente: Elaboración Propia

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Tormentas, Terremotos, Inundaciones)	10	1	0	0
Humanas (Huelgas, Epidemias, materiales peligrosos, problemas de transporte, perdida del personal clave)	10	1	1	10
Instalaciones (fuego, daños por agua, explosión, caída de energía, perdida de acceso, fallas eléctricas, fallas mecánicas)	10	1	1	10
Tecnológicas (virus, pérdida de datos, hacking, fallas de Software y de Hardware, fallas en las líneas de comunicación)	10	2	3	60
Operacionales (Crisis Financieras, fallas en equipos, errores usuarios)	10	2	2	40

TABLA 18: Equipo de Video

Fuente: Elaboración Propia

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Tormentas, Terremotos, Inundaciones)	11	3	2	66
Humanas (Huelgas, Epidemias, materiales peligrosos, problemas de transporte, perdida del personal clave)	11	3	2	66
Instalaciones (fuego, daños por agua, explosión, caída de energía, perdida de acceso, fallas eléctricas, fallas mecánicas)	11	2	1	22
Tecnológicas (virus, pérdida de datos, hacking, fallas de Software y de Hardware, fallas en las líneas de comunicación)	11	1	1	11
Operacionales (Crisis Financieras, fallas en equipos, errores usuarios)	11	3	3	99

TABLA 19: Reportes COEM

Fuente: Elaboración Propia

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Tormentas, Terremotos, Inundaciones)	9	2	1	18
Humanas (Huelgas, Epidemias, materiales peligrosos, problemas de transporte, perdida del personal clave)	9	1	1	9
Instalaciones (fuego, daños por agua, explosión, caída de energía, perdida de acceso, fallas eléctricas, fallas mecánicas)	9	2	2	36
Tecnológicas (virus, pérdida de datos, hacking, fallas de Software y de Hardware, fallas en las líneas de comunicación)	9	1	1	9

Operacionales (Crisis Financieras, fallas en equipos, errores usuarios)	9	1	1	9

TABLA 20: Servicios

Fuente: Elaboración Propia

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Tormentas, Terremotos, Inundaciones)	9	2	1	18
Humanas (Huelgas, Epidemias, materiales peligrosos, problemas de transporte, perdida del personal clave)	9	1	1	9
Instalaciones (fuego, daños por agua, explosión, caída de energía, perdida de acceso, fallas eléctricas, fallas mecánicas)	9	2	2	36
Tecnológicas (virus, pérdida de datos, hacking, fallas de Software y de Hardware, fallas en las líneas de comunicación)	9	3	3	81
Operacionales (Crisis Financieras, fallas en equipos, errores usuarios)	9	2	2	36

TABLA 21: Software Comercial

Fuente: Elaboración Propia

Amenaza	Impacto	Nivel de Amenazas	Vulnerabilidades	Nivel de Riesgo
Naturales (Tormentas, Terremotos, Inundaciones)	10	2	1	20
Humanas (Huelgas, Epidemias, materiales peligrosos, problemas de transporte, perdida del personal clave)	10	2	2	40
Instalaciones (fuego, daños por agua, explosión, caída de energía, perdida de acceso, fallas eléctricas, fallas mecánicas)	10	1	0	0
Tecnológicas (virus, pérdida de datos, hacking, fallas de Software y de Hardware, fallas en las líneas de comunicación)	10	0	0	0

Operacionales (Crisis Financieras, fallas en equipos, errores usuarios)	10	3	3	90

TABLA 22: Trabajador

Fuente: Elaboración Propia

TRATAMIENTO DEL RIESGO

El valor de riesgo aceptable en este caso se establecerá en 50, por los que se tratarían los que igualan o superan esta cifra y se asumirían los que estuvieran por debajo, De todas formas, se aplicarían los controles mínimos establecidos por la norma.

ACTIVOS	RIESGO	TRATAMIENTO
Equipo de Almacenamiento	72	Se asume el riesgo
Equipo de comunicaciones	72	Se asume el riesgo
Equipo de usuario	54	Se asume el riesgo
Equipo de Video	60	Se asume el riesgo
Reportes de COEM	99	Se asume el riesgo
Servicios	36	Se asume el riesgo
Software comercial	81	Se asume el riesgo
Trabajador	90	Se asume el riesgo

TABLA 23: Tratamiento del Riesgo

Fuente: Elaboración Propia

DECLARACIÓN DE APLICABILIDAD

Se considera:

Controles Aplicados

En este punto escogeremos los controles que nos ayudarán a salvaguardas los activos de la empresa según el análisis

OBJETIVOS DE CONTROL	CONTROLES		APLICABILIDAD	JUSTIFICACIÓN
POLITICAS DE SEGURIDAD DE LA INFORMACIÓN				
ORIENTACIÓN DE LA DIRECCIÓN PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	POLÍTICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	1	APLICAR	Se ha identificado los riesgos de información y de sus activos, por lo que es necesario establecer un Política de Seguridad de la información, estas políticas deberán definir exactamente a los responsables del desarrollo e implementación. Los Gerentes deberán brindar el apoyo necesario en consideración de los requisitos del área y de acuerdo a las políticas, leyes y reglamentos pertinentes. Una vez definido las Políticas de seguridad de la información se deberá publicar y poner a disposición a todas las partes interesadas. Trimestralmente se deberá hacer una revisión para asegurar su idoneidad con respecto a los riesgos de información.
	REVISIÓN DE LAS POLITICAS PARA LA SEGURIDAD DE LA INFORMACIÓN	2	APLICAR	
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN				
ORGANIZACIÓN INTERNA	ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN	3	APLICAR	La Institución mediante la política de seguridad de la información debe definir y asignar las responsabilidades en la Seguridad de la Información y separar las responsabilidades y asignar los deberes de los activos de información de la Institución y así minimizar las posibles modificaciones no autorizadas. Además de mantener los contactos apropiados con las autoridades pertinentes; en
	SEPARACIÓN DE DEBERES	4	APLICAR	

	CONTACTO CON LAS AUTORIDADES	5	APLICADO	consideración con los grupos de interés se debe mantener como contactos a especialistas y profesiones especializados en Seguridad de la Información. Todo el proceso de implementación o mejora deben de considerarse mediante el proceso de gestión de Proyectos.
	CONTACTO CON GRUPOS DE INTERÉS ESPECIAL	6	APLICADO	
	SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE PROYECTOS.	7	APLICAR	
DISPOSITIVOS MÓVILES Y TELETRABAJO	POLÍTICA PARA DISPOSITIVOS MÓVILES	8	APLICAR	La institución mediante la presente política restringe la conexión a las redes inalámbricas de internet por parte de los dispositivos móviles y equipos de terceros.
	TELETRABAJO	9	NO APLICAR	De acuerdo con lo establecido en la ley N 300036 del año 2013, la Institución si cuenta con teletrabajo, la cual es una forma de organización laboral. Se caracteriza por el desempeño de labores remuneradas sin la presencia física del trabajador a través de medios informáticos de telecomunicaciones y análogos. Sin embargo, para el área no es necesario este tipo de labores a desempeñar.
SEGURIDAD DE LOS RECURSOS HUMANOS				
ANTES DE ASUMIR EL EMPLEO	SELECCIÓN	10	APLICAR	Para el desarrollo del proceso y actividades de selección de personal el área de Recursos Humanos son los responsables de llevar a cabo las etapas para el reclutamiento del personal, en consideración de los reglamentos, códigos de ética y las leyes pertinentes que aseguran la calidad del proceso bajo las consideraciones de la gerencia. El personal en inducción interactúa permanentemente con los activos de información de la institución por tal
	TÉRMINOS Y CONDICIONES DEL EMPLEO	11	APLICAR	
DURANTE LA EJECUCIÓN DEL EMPLEO	RESPONSABILIDADES DE LA DIRECCIÓN	12	APLICAR	

	TOMA DE CONCIENCIA, EDUCACIÓN, Y FORMACIÓN EN S.I.	13	APLICAR	motivo se lleva a cabo la firma de aceptación de documentos tales como: Acta de fiel cumplimiento de manual de prevención de lavado de activos, Código de Ética y de Conducta, Reglamento de seguridad y salud en el trabajo, Política de uso de correo electrónico. La institución junto otras áreas de interés se comprometen en el fiel cumplimiento de capacitación y actualización del personal. El cumplimiento del proceso disciplinario debe ser responsabilidad hasta cierto punto del superior del área, esta consideración es basado a las políticas y procedimientos que se le anteponen para la ejecución de sus labores. Lo mencionado anteriormente recae en la ejecución por parte del área de Recursos humanos.
	PROCESO DISCIPLINARIO	14	APLICAR	
TERMINACIÓN Y CAMBIO DE EMPLEO	TERMINACIÓN O CAMBIO DE RESPONSABILIDADES DE EMPLEO	15	APLICAR	
GESTION DE ACTIVOS				
RESPONSABILIDAD POR LOS ACTIVOS	INVENTARIO DE ACTIVOS	16	APLICAR	Se debe identificar los activos de Información del área y las instalaciones de procesamiento de información, además de documentar y mantener un inventario actualizados de estos activos.
	PROPIEDAD DE LOS ACTIVOS	17	APLICAR	Se debe identificar los propietarios de los activos de información obtenidos en los inventarios. Además del seguimiento de la regularización de los activos de información faltantes por parte de sus propietarios o interesados y de la verificación de su autenticidad.

	USO ACEPTABLE DE LOS ACTIVOS	18	APLICAR	Se debe implementar las políticas y procedimientos en la identificación, documentación e implementación de las reglas para el uso aceptable de la información y de activos asociados con la información e instalaciones de procesamiento de información.
	DEVOLUCIÓN DE LOS ACTIVOS	19	APLICAR	Los activos de la institución deberán ser devueltos por los colaboradores al finalizar su relación contractual o uso del mismo bajo un documento de entrega al superior o área responsable. El superior o área responsable debe asegurar la devolución de los activos cuando se presentan renuncias, rotaciones, terminaciones o cambios de la contratación del personal que conforman los diferentes proyectos o áreas transversales de la institución.
CLASIFICACIÓN DE LA INFORMACIÓN	CLASIFICACIÓN DE LA INFORMACIÓN	20	APLICAR	La institución debe asegurar que la información reciba un nivel apropiado de protección, de acuerdo con su importancia para la institución, así mismo todos los usuarios deben de estar comprometidos en respetar la clasificación de la información propuesta o definida.
	ETIQUETADO DE LA INFORMACIÓN	21	APLICAR	Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la institución. Toda información que se clasifica como "confidencial" debe de poseer una etiqueta de seguridad que provea todos los datos correspondientes a esta categoría.
	MANEJO DE ACTIVOS	22	APLICAR	Se debe desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la institución.
MANEJO DE MEDIOS	A 8.3.1. GESTIÓN DE MEDIOS REMOVIBLES	23	APLICAR	Se debe implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la institución en tal sentido establecer un formato de asignación de propietario de medios removibles tales como, correo electrónico laboral, servicios de mensajería, USB, CD, entre otros

				además de un formato para la entrega o custodia y destrucción de tales medios o dispositivos.
	DISPOSICIÓN DE LOS MEDIOS	24	APLICAR	Se debe llevar un control de la disposición de los medios cuando ya no se requieran, mediante procedimiento y formato establecido que dispongan el área de Seguridad de la Información, así como la información contenida en dichos medios conforme a políticas correspondientes.
	TRANSFERENCIA DE MEDIOS FÍSICOS.	25	APLICAR	Se debe llevar a cabo un procedimiento para el manejo y almacenamiento de la información, para asegurar la que se eviten eventos como divulgación, modificación, retiro o destrucción de información no autorizada cuando se traslade un medio físico de un punto a otro.
CONTROL DE ACCESO				
REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	POLÍTICA DE CONTROL DE ACCESO	26	APLICAR	La institución día a día genera y desarrolla activos de información lo cuales deben estar salvaguardados o custodiados de acuerdo a su importancia o clasificación por lo que se debe controlan el acceso a la información.
	ACCESO A REDES Y A SERVICIOS EN RED	27	APLICAR	Se debe asegurar que los usuarios de la red o los que usan el sistema de la institución sólo acceden a los servicios para los que están autorizados y que sus accesos solo se establezcan de acuerdo a un perfil definido o mediante la autorización del área de Seguridad de la Información.
GESTIÓN DE ACCESO DE USUARIOS	REGISTRO Y CANCELACIÓN DEL REGISTRO DE USUARIOS	28	APLICAR	Se debe implementar un procedimiento para llevar a cabo el Registro y Cancelación de los Registro de cada usuario de la Institución, además de evitar el acceso no autorizado a los sistemas y servicios de información.
	SUMINSITRO DE ACCESO DE USUARIOS	29	APLICAR	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios de la Institución.

	GESTIÓN DE DERECHOS DE ACCESO PRIVILEGIADO	30	APLICAR	Se debe llevar el control y un registro formal mediante un formato de la asignación y uso del acceso privilegiado a la información de los sistemas y servicios.
	GESTIÓN DE LA INF. DE AUTENTICACIÓN SECRETA DE USUARIOS	31	APLICAR	La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal a través de un gestor de identidad.
	REVISIÓN DE LOS DERECHOS DE ACCESO DE USUARIOS	32	APLICAR	Se debe llevar a cabo una revisión periódica de cada 2 meses y así asegurar que cada usuario solamente tenga acceso a la información que requiere para sus funciones.
	RETIRO O AJUSTE DE LOS DERECHOS DE ACCESO.	33	APLICAR	Se debe llevar a cabo un registro por parte del área de los trabajadores que culminan vínculos laborales, por lo que se debe proceder a retirar los derechos de los accesos a los sistemas u activos de información de la institución.
RESPONSABILIDADES DE LOS USUARIOS	USO DE INFORMACIÓN DE AUTENTICACIÓN SECRETA	34	APLICAR	Se debería exigir y promover a los usuarios que cumplan las buenas prácticas de la institución para el uso de información de autenticación secreta de su contraseña.
CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	RESTRICCIÓN DE ACCESO A LA INFORMACIÓN	35	APLICAR	Evitar que usuarios no autorizados tengan acceso a los sistemas de información, además que cada 30 días se cambien las claves.
	PROCEDIMIENTO DE INGRESO SEGURO.	36	APLICAR	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
	SISTEMA DE GESTIÓN DE CONTRASEÑAS.	37	NO APLICAR	Se debe hacer una evaluación a los sistemas de gestión de contraseñas, ya que estas deberían ser interactivos y deberían asegurar la calidad de las contraseñas. Se debe promover el protocolo de las buenas prácticas de la creación de una contraseña por parte de los usuarios; además de establecer el cambio de clave cada treinta días (30) para cada portal, por consiguiente, la existencia de un formato como Política del buen uso de las contraseñas,

				y que su prestación o mal uso se considere falta grave. No aplica, por no contar con un sistema de gestión de contraseñas.
	USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS.	38	APLICAR	Restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
	CONTROL DE ACCESO A CODIGOS FUENTE DE PROGRAMAS.	39	APLICAR	Es necesario aplicar dicho control, porque los responsables de su administración es el área del COEM y la unidad de estadística y tecnologías de la información.
CRIPTOGRAFIA				
CONTROLES CRIPTOGRAFICOS	POLÍTICA SOBRE USO DE CONTROLES CRIPTOGRÁFICOS	40	APLICAR	Los sistemas de información que se manejan en los diferentes proyectos deben establecer controles criptográficos con el objetivo de garantizar la confidencialidad e integridad de la información, además de asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
	GESTIÓN DE LLAVES	41	APLICAR	Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
SEGURIDAD FISICA Y DEL ENTORNO				
ÁREAS SEGURAS	PERÍMETRO DE SEGURIDAD FÍSICA	42	APLICADO	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización. Limitar la posibilidad de pérdida de activos de información definiendo perímetros de seguridad física.

	CONTROLES DE ACCESO FÍSICOS	43	APLICADO	Evitar el acceso no autorizado a áreas seguras como área de servidores, área de comunicaciones, archivo con información confidencial. El personal que deba ingresar será con la Aprobación autorización del área de COEM y de la unidad de estadística y tecnologías de la información.
	SEGURIDAD DE OFICINAS, RECINTOS E INSTALACIONES	44	APLICAR	Se mantiene la información bajo llave, (estrictas medidas de seguridad) y se restringe el acceso sin autorización, o se permite bajo un documento de autorización con avisos impresos.
	PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES	45	APLICADO	Se cuenta con sistema de aire acondicionado en todos los ambientes y en data center, protegido con extintores especiales para data center y sistema contra incendios.
	TRABAJO EN ÁREAS SEGURAS	46	APLICAR	Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras, además de la implementación de las políticas y procedimientos del área de Seguridad Física y Medio Ambiente.
	ÁREAS DE DESPACHO Y CARGA	47	APLICAR	Se controla los puntos de acceso tales como sala de operadores, data center y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
EQUIPOS	UBICACIÓN Y PROTECCION DE LOS EQUIPOS	48	APLICAR	Todos los equipos de la institución se encuentran ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado. La institución realiza anualmente inventarios de todos los equipos tales como: servidores, computadores de escritorio, teléfonos entre otros por tal razón es necesario establecer controles que permitan evitar la ocurrencia de eventos como pérdida, daño, robo o interrupción de los equipos tanto dentro como fuera de la organización. Así como el registro de los bienes o activos robados.
	SERVICIOS DE SUMINSITRO	49	APLICADO	
	SEGURIDAD EN EL CABLEADO	50	APLICADO	
	MANTENIMIENTO DE EQUIPOS	51	APLICADO	

	RETIRO DE ACTIVOS	52	APLICAR	Los equipos, información o software no se deberían retirar de su sitio sin autorización previa, para ello se necesita la aprobación de las áreas de COEM, unidad de estadística y tecnologías de la información, además del visto del Gerente de seguridad ciudadana y/o del Gerente Municipal.
	SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DE LAS INSTALACIONES	53	APLICAR	Para evitar daños o pérdidas a los equipos cuando se encuentran fuera de las instalaciones se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
	DISPOSICIÓN SEGURA O REUTILIZACIÓN DE EQUIPOS	54	APLICAR	Se deberían verificar que todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
	EQUIPOS DE USUARIO DESATENDIDO	55	APLICADO	El personal de la institución es responsable de los activos de información que se encuentran a su cargo, así como de la protección de estos activos en cuanto confidencialidad, integridad y disponibilidad, de tal forma que se han definido responsabilidades claras en cuanto a seguridad de la información, en tal sentido es necesario establecer controles de seguridad para asegurar que se evita el acceso de usuarios no autorizados y el robo de información de equipos en desuso. La institución cuenta con una política de escritorio limpio y una política de pantalla limpia en las instalaciones de procesamiento de información.
	POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA.	56	APLICAR	
SEGURIDAD DE LAS OPERACIONES				

PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	PROCEDIMIENTOS DE OPERACIÓN DOCUMENTADOS	57	APLICAR	Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten segmentados por áreas y por perfiles de usuarios con especificaciones del nivel de activo con el que interactué o genere, estos procedimientos deberían estar a disposición mediante un documento físico, además se debería de entregar un manual básico de operaciones que sirva como guía de operaciones al personal nuevo o en inducción.
	GESTIÓN DE CAMBIOS	58	APLICAR	Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información. Estos cambios deben llevar un registro histórico en consideración al área de COEM por parte del área de Seguridad de la Información y de las áreas interesadas.
	GESTIÓN DE CAPACIDAD	59	APLICAR	Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura en consideración con los procesos de cada área y su giro de negocio.
	SEPARACION DE LOS AMBIENTES DE DESARROLLO, PRUEBAS Y OPERACIÓN.	60	APLICAR	La institución mantiene los ambientes de cada área separados ya sea de desarrollo, prueba y operación, para así reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
PROTECCION CONTRA CODIGOS MALICIOSOS	CONTROLES CONTRA CÓDIGOS MALICIOSOS	61	APLICAR	Para el desarrollo de las actividades de la Institución se utilizan servicios como Internet, medios extraíbles, los cuales pueden afectar el correcto funcionamiento de activos de información como equipos, software entre otros, por lo tanto, es importante establecer controles de seguridad que permitan la detección y prevención de la acción de códigos maliciosos, así como también procedimientos de concientización de los usuarios. Se debería llevar a cabo el manteniendo de cada uno de los equipos y actualización de antivirus en horarios que no

				afecten el desarrollo de las funciones de los usuarios y la atención a los clientes.
COPIAS DE RESPALDO	RESPALDO DE LA INFORMACIÓN	62	APLICAR	La información de la Institución, como memorandos, reportes de incidencias, copias de seguridad de video, documentos del COEM así como en el servidor de video, en tal sentido es importante establecer controles de seguridad que aseguren la ejecución de procedimientos de backup y recuperación que permitan restaurar en el menor tiempo la información ante la materialización de un riesgo, y así permitir que la Institución continué con sus actividades habituales sin ningún inconveniente y la atención a población en general.
REGISTRO Y SEGUIMIENTO	REGISTRO DE EVENTOS	63	APLICAR	El COEM para el desarrollo de sus actividades cuenta con trabajadores que tienen acceso a los diferentes activos de información ya sea a nivel de base de datos, o parte operativa de sus labores, por lo que, para la ejecución de sus actividades, en tal sentido es importante establecer controles de seguridad que permitan la detección oportuna de actividades de procesamiento de información no autorizadas y herramientas para investigaciones futuras de incidentes de seguridad de la información. Además, se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información. Registro de eventos en los sistemas operativos de acceso de errores, de aplicación y se revisan periódicamente.
	PROTECCIÓN DE LA INFORMACIÓN DE REGISTRO	64	APLICADO	La Institución mantiene y protege el historial de logs, por lo que solo los Administradores de los equipos tienen acceso a la información de registro.
	REGISTROS DEL ADMINSITRADOR Y DEL OPERADOR	65	APLICAR	La entidad pública mantiene el histórico de las actividades del jefe del área, supervisor de operador y operador del sistema de incidencias mediante reportes físicos diarios o mensuales. Tales registros se deberían

				almacenar como histórico ya sea como archivos o escanear los físicos, proteger y custodiar. Se debería desarrollar un procedimiento de autenticidad o calidad bajo un muestreo aleatorio de los activos de información correspondientes a las copias de seguridad de video, además de la implementación de un ambiente donde se custodie cada activo de información.
	SINCRONIZACIÓN DE RELOJES	66	APLICADO	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro del COEM se encuentran sincronizados con una única fuente de referencia de tiempo.
CONTROL DE SOFTWARE OPERACIONAL	INSTALACIÓN DE SOFTWARE EN SISTEMAS OPERATIVOS	67	APLICAR	La Institución ha establecido controles de seguridad para garantizar la protección, control y correcta operación de los sistemas operativos. De igual forma para los equipos asignados a los Usuarios se restringe la posibilidad de instalación de programas y/o aplicativos; y así asegurar la integración de los sistemas operativos.
GESTION DE LA VULNERABILIDAD TÉCNICA	GESTIÓN DE LAS VULNERABILIDADES TÉCNICAS	68	APLICAR	La Institución mantiene activos de información tecnológicos los cuales están expuestos a vulnerabilidades de tipo técnico, por lo tanto, se establecía controles de seguridad para garantizar la reducción de los riesgos derivados de las vulnerabilidades técnicas, así como un histórico de sus eventos.
	RESTRICCIÓN SOBRE LA INSTALACION DE SOFTWARE	69	APLICAR	Para garantizar la protección, control y correcto uso de los sistemas operativos, debe contar con controles para la Restricción sobre la Instalación de cualquier Software.
CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	CONTROLES DE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	70	APLICAR	La Institución cuenta con sistemas operativos o procesos que pueden ser objeto de auditoria de seguridad de la información, por lo tanto, es importante establecer controles de seguridad que garanticen un adecuado uso de las herramientas de auditoria y minimizar la interrupción de los sistemas.

SEGURIDAD DE LAS COMUNICACIONES				
GESTIÓN DE LA SEGURIDAD DE LAS REDES	CONTROLES DE REDES	71	APLICADO	La institución mantiene asegurada la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte. Se ha desarrollado mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red.
	SEGURIDAD DE LOS SERVICIOS DE RED	72	APLICAR	
	SEPARACIÓN EN LAS REDES	73	APLICADO	Los grupos de servicios de información, usuarios y sistemas de información se mantienen separados en las redes para así evitar que el tráfico de una subred afecte a las demás.
TRANSFERENCIA DE INFORMACIÓN	POLÍTICAS Y PROCEDIMIENTOS DE TRASNFERENCIA DE INFORMACIÓN	74	APLICAR	Dentro del desarrollo normal de las actividades de la entidad se presentan actividades de intercambio de información con clientes (población en general), lo cual es importante establecer controles de seguridad para asegurar que se cumplen las políticas y procedimientos de la institución para el intercambio de información y para garantizar que no se presente el uso inadecuado, violación o corrupción cuando la información sale de las instalaciones de la organización. Información Parte de los controles es la identificación de la clasificación de la, ya sea del tipo; confidencial, uso interno y pública.
	ACUERDOS SOBRE TRASNFERENCIA DE INFORMACIÓN	75	APLICAR	
	MENSAJERIA ELECTRÓNICA	76	APLICAR	

	ACUERDOS DE CONFIDENCIALIDAD O DE NO DIVULGACIÓN	77	APLICAR	Se debería considerar el promover los acuerdos de Confidencialidad en cada uno de los trabajadores del COEM, sobre todo quienes interactúan con el público a diario, es decir: No divulgar información de la entidad que haya sido clasificada como confidencial. Está prohibido que los trabajadores saquen información de la entidad.
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS				
REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	ÁNALISIS Y ESPECIFICACIÓN DE REQUISITOS DE SI	78	APLICAR	El jefe del COEM es el encargado de estas funciones y en coordinación con la unidad de estadística y tecnologías de la información. Por lo que se deberán establecer políticas. Con visto de Gerencia Municipal.
	SEGURIDAD DE SERVICIOS DE LAS APLICACIONES EN REDES PÚBLICAS	79	NO APLICAR	No es necesario aplicar dicho control, porque no se administra ninguna aplicación en redes públicas.
	PROTECCIÓN DE TRANSACCIONES DE LOS SERVICIOS DE LAS APLICACIONES	80	NO APLICAR	No es necesario aplicar dicho control, porque no se administra ninguna transacción de los servicios en aplicaciones.
CONTROL DE ACCESO AL SISTEMA OPERATIVO	POLÍTICA DE DESARROLLO SEGURO	81	APLICAR	El jefe del COEM es el encargado de estas funciones y en coordinación con la unidad de estadística y tecnologías de la información. Por lo que se deberán establecer políticas. Con visto de Gerencia Municipal.
	PROCEDIMIENTO DE CONTROL DE CAMBIOS EN SISTEMAS	82	APLICAR	El jefe del COEM es el encargado de estas funciones y en coordinación con la unidad de estadística y tecnologías de la información. Por lo que se deberán establecer políticas. Con visto de Gerencia Municipal.
	REVISIÓN TÉCNICAS DE LAS APLICACIONES DESPUES DE CAMBIOS EN LA	83	APLICAR	El jefe del COEM es el encargado de estas funciones y en coordinación con la unidad de estadística y tecnologías de la información. Por lo que se deberán establecer políticas. Con visto de Gerencia Municipal.

	PLATAFORMA DE OPERACIÓN			
	RESTRICCIONES EN LOS CAMBIOS A LOS PAQUETES DE SOFTWARE	84	APLICAR	El jefe del COEM es el encargado de estas funciones y en coordinación con la unidad de estadística y tecnologías de la información. Por lo que se deberán establecer políticas. Con visto de Gerencia Municipal.
	PRINCIPIOS DE CONSTRUCCIÓN DE LOS SISTEMAS SEGUROS	85	APLICAR	El jefe del COEM es el encargado de estas funciones y en coordinación con la unidad de estadística y tecnologías de la información. Por lo que se deberán establecer políticas. Con visto de Gerencia Municipal.
	AMBIENTE DE DESARROLLO SEGURO	86	APLICAR	Se deberá implementar una oficina con los ambientes y herramientas para asegurar un desarrollo seguro. El jefe del COEM es el encargado de estas funciones y en coordinación con la unidad de estadística y tecnologías de la información. Por lo que se deberán establecer políticas. Con visto de Gerencia Municipal.
	DESARROLLO CONTRATADO EXTERNAMENTE	87	APLICAR	El jefe del COEM es el encargado de estas funciones y en coordinación con la unidad de estadística y tecnologías de la información. Por lo que se deberán establecer políticas. Con la aprobación de Gerencia Municipal.
	PRUEBAS DE SEGURIDAD DE SISTEMAS	88	APLICAR	El jefe del COEM es el encargado de estas funciones y en coordinación con la unidad de estadística y tecnologías de la información. Por lo que se deberán establecer el tipo de prueba a realizar buscando alguna vulnerabilidad o error en la seguridad de los sistemas de seguridad. Con aprobación de Gerencia Municipal.
	PRUEBAS DE ACEPTACIÓN DE SISTEMAS	89	APLICAR	El jefe del COEM es el encargado de estas funciones y en coordinación con la unidad de estadística y tecnologías de la información. Por lo que se deberán establecer un cronograma para las pruebas de aceptación al sistema. Con aprobación de Gerencia Municipal.
DATOS DE PRUEBA	PROTECCIÓN DE DATOS DE PRUEBA	90	APLICAR	El jefe del COEM es el encargado de estas funciones y en coordinación con la unidad de estadística y tecnologías de la información. Por lo que se deberán establecer

				políticas de seguridad a la protección de datos según su clasificación. Con aprobación de Gerencia Municipal.
RELACIONES CON LOS PROVEEDORES				
RELACIONES CON LOS PROVEEDORES	SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES	91	APLICAR	La institución desarrolla actividades para las cuales requiere realizar diferentes tipos de servicios, en tal sentido no existen controles que garantizan la seguridad del negocio; antes de gestionar un servicio que afecten la seguridad de la información de la organización y la infraestructura que sobre la cual esta soportada.
	TRATAMIENTO DE LA SEGURIDAD DENTRO DE LOS ACUERDOS CON PROVEEDORES	92	APLICAR	La institución debe establecer y mantener acuerdos de requisitos de seguridad de la información con el proveedor. Estos requisitos de seguridad se definen en los conceptos técnicos y en los pliegos de condiciones.
	CADENA DE SUMINISTRO DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN	93	APLICAR	Los acuerdos con terceros deben incluir requisitos para tratar los riesgos de seguridad de la información. Acuerdo de Confidencialidad con terceros.
GESTIÓN DE LA PRESENTACIÓN DE SERVICIOS DE PROVEEDORES	SEGUIMIENTO Y REVISIÓN DE LOS SERVICIOS DE LOS PROVEEDORES	94	APLICAR	La institución debe determinar el grado de cumplimiento de terceras partes conforme contrato y/o acuerdos establecidos.
	GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE LOS PROVEEDORES	95	NO APLICAR	No se considera que este control ayude a reducir el riesgo de los activos identificados.
GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION				
GESTION DE INCIDENTES Y MEJORAS EN LA SEGURIDAD DE LA INFORMACIÓN	RESPONSABILIDADES Y PROCEDIMIENTOS	96	APLICAR	La institución debe asegurar una respuesta oportuna, efectiva y organizada de los incidentes de seguridad de la información ocurrido en el Centro de Operaciones, emergencias y operaciones (COEM) ya sea en sala de operadores o sala del data center, por lo que mediante su política de seguridad de la información establezca su

				compromiso, organización y asignación de para su cumplimiento, de igual forma velar por mantener protegido sus activos de información mediante la revisión del sistema de gestión de seguridad de la información, la firma de los acuerdos de confidencialidad, manteniendo contacto con las autoridades y con grupos de interés especiales, y la revisión independiente de sus activos, por lo que la programación periódica de auditorías, y muestreos aleatorios de la autenticidad de activos físicos le permitirán a reducir el riesgo de los mencionados.
	REPORTE DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	97	APLICAR	Se debe de asegurar que los eventos e incidentes de seguridad de información sean reportados oportunamente y que las áreas involucradas deberán emitir el Reporte de Eventos vinculados a la Seguridad de la Información, dichos reporte deben de ser documentos por los involucrados o participantes en el menor tiempo posible.
	REPORTE DE DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	98	APLICAR	Se debería exigir a todos los trabajadores que usan los servicios y sistemas de información de la institución, que observen e informen cualquier debilidad, falta en seguridad de la información observada o sospechosa en los sistemas o servicios.
	EVALUACIÓN DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN Y DECISIONES SOBRE ELLOS	99	APLICAR	Cada uno de los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información considerando el activo de información y tipo afectado. Estos incidentes de seguridad de la información deben ser analizados por el personal designado por la jefatura del COEM con el apoyo de la unidad de estadística y tecnologías de la información, con la aprobación de las Gerencia Municipal para identificar acciones de mejora, en tal sentido es necesario establecer controles de seguridad para garantizar un manejo eficaz y consistente de los incidentes de seguridad de la información.

	RESPUESTA A INCIDENTES DE SEGUIRIDAD DE LA INFORMACIÓN	100	APLICAR	Se debería tener un Procedimiento para atender en el menor tiempo posible a los incidentes de seguridad de la información y así dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
	APRENDIZAJE OBTENIDO DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	101	APLICAR	Todo conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para prever, reducir y mitigar la posibilidad o el impacto de incidentes futuros.
	RECOLECCIÓN DE EVIDENCIA	102	APLICAR	La institución debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia ante los eventos en contra de la seguridad de la Información del Centro de Operaciones, Emergencia y Monitoreo (COEM).
ASPECTOS DE SEGURIDAD DE LA INFORMACION DE LA GESTION DE CONTINUIDAD DE NEGOCIO				
CONTINUIDAD EN SEGURIDAD DE LA INFORMACIÓN	PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	103	APLICAR	La institución mantiene un gran vinculo y responsabilidad con la atención de sus clientes (población en general), por lo que debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre naturales; lo que permita seguir con la atención a sus clientes (población en general), minimizando los riesgos vinculados ante tales. Tanto los procedimientos como los formatos deben estar aprobados por la Gerencia Municipal.

	IMPLEMENTACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	104	APLICAR	La institución debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa. Se debe nombrar a representantes los cuales dirigirán dichos eventos cuando se presenten; ellos informarán y serán quienes reporten y documenten dichos eventos. El área del Centro de Operaciones, Emergencia y Monitoreo (COEM), Gerencia de Seguridad de Ciudadana, Unidad de Estadística y Tecnologías de la información, Gerencia Municipal, se harán responsables de la toma de decisiones según lo amerite ante dicho evento.
	VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SI	105	APLICAR	La institución debe verificar a intervalos regulares y mantener actualizados los controles de continuidad de la seguridad de la información establecidos e implementados acordes a la realidad, con el fin de asegurar su eficiencia durante situaciones adversas.
REDUNDANCIAS	DISPONIBILIDAD DE INSTALACIONES DE PROCESAMIENTO DE INFORMACIÓN	106	NO APLICAR	No se considera que este control ayude a reducir el riesgo de los activos identificados.
CUMPLIMIENTO				
CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	IDENTIFICACIÓN DE LA LEGISLACIÓN APLICABLE Y DE LOS REQUISITOS CONTRACTUALES.	107	APLICAR	La institución debe evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito orientado a la seguridad.
	DERECHOS DE PROPIEDAD INTELECTUAL	108	APLICADO	La institución asegura el cumplimiento de los requisitos legislativos de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados o adquiridos.

	PROTECCIÓN DE REGISTROS	109	APLICAR	La institución deberá proteger los registros contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada.
	PRIVACIDAD Y PROTECCIÓN DE INFORMACIÓN DE DATOS PERSONALES	110	APLICAR	La institución deberá cuidar las bases de datos y expedientes con datos personales tanto como de sus clientes (población en general), como parte de las buenas prácticas de seguridad para evitar violar los derechos de seguridad en la información y ocasionar daños al personal o a los clientes (población en general).
	REGLAMENTACIÓN DE CONTROLES CRIPTOGRÁFICOS	111	APLICAR	La institución para los sistemas de información deberá establecer el uso de controles criptográficos con el objetivo de garantizar la confidencialidad e integridad de la información.
REVISIONES DE SEGURIDAD DE LA INFORMACIÓN	REVISIÓN INDEPENDIENTE DE LA SEGURIDAD DE LA INFORMACIÓN	112	APLICAR	La institución mediante su política de seguridad de la información debe establecer su compromiso, organización y asignación para su cumplimiento, de igual forma vela por mantener protegido sus activos de información; así mismo establece la revisión del sistema de gestión de seguridad de la información por lo que deberá actualizar en consideración a la última versión de la norma estándar ISO 27001: 2013. La revisión y actualización de los controles y objetivos de control debe de estar bajo el Área del Centro de Operaciones, Emergencia y Monitoreo (COEM) y la Unidad de Estadística y Tecnologías de la información bajo el apoyo de las áreas pertinentes con el visto de Gerencia Municipal.
	CUMPLIMIENTO CON LAS POLÍTICAS Y NORMAS DE SEGURIDAD	113	APLICAR	El personal de la institución interactúa permanentemente con los activos de información para los cuales se han diseñado políticas y controles en materia de seguridad de la información, en tal sentido es importante establecer

	REVISIÓN DEL CUMPLIMIENTO TÉCNICO	114	APLICAR	controles de seguridad que garanticen que todo el personal de la institución conozca y aplique las políticas de seguridad de la información y los respectivos controles. Además es necesaria la inclusión de la Alta Dirección en este proceso, como requisito de la norma y condición de éxito del Sistema de Gestión de Seguridad de la Información por lo tanto se debería considerar desarrollar un historial de Actas de comité de calidad del proceso gestión de recursos informáticos y considerar la revisión de los controles y consideraciones de los requisitos mínimos de seguridad.

TABLA 24: APLICABILIDAD

Fuente: Elaboración Propia

ANÁLISIS Y DISCUSIÓN

La presente investigación, permitió analizar y diagnosticar la situación actual del Centro de Operaciones, Emergencia y Monitoreo (COEM) de la Municipalidad Distrital de Bellavista - Sullana, Aplicando la misma metodología por Camargo (2017), consistente en ISO 27000 e ISO 27001; dando como resultado que existen muchos controles que no se encuentran aplicados a la entidad, identificándose que se encuentra en riesgo alto, por falta de controles, los mismos que al ser aplicados por el autor de la presente investigación, determinaron la urgencia de proteger los activos de información manejados en la empresa.

Por otra parte, en forma concordante con López (2016), en la presente tesis propone herramientas metodológicas tanto para la prevención como para la detección de riesgo relacionados con el aumento de vulnerabilidades de equipo informáticos utilizando norma ISO/IEC 27001.

Asimismo, debido a que la investigación desarrolla un sistema de Gestión de Seguridad de la Información aplicada por Villena (2006) se tomó en cuenta con el soporte en relación a los 3 pilares de la seguridad de la información como son la; confidencialidad, integridad y disponibilidad de sus activos de información, en forma concordante con el autor de la presente tesis.

Finalmente, se logró elaborar las políticas de seguridad o recomendaciones que deben establecerse en la Municipalidad Distrital de Bellavista - Sullana; al igual que Barragán, Góngora y Martínez (2013) quienes lograron establecer también políticas de seguridad para la municipalidad de Guayaquil, indicando la importancia y la valoración que deben tener la seguridad de la información para una empresa minimizando el impacto en caso de producirse incidentes y resaltando que la seguridad no es responsabilidad únicamente de la tecnología sino que debe existir responsabilidades desde la gerencia hasta todos los procesos.

CONCLUSIONES

Para el desarrollo de la presente investigación fue fundamental realizar una serie de actividades lo cual nos permitió plasmar el objetivo de la presente investigación.

Terminado el desarrollo de la investigación se tuvo las siguientes conclusiones:

- Se llevó a cabo encuestas al jefe y a los trabajadores del área de Centro de Operaciones, Emergencia y Monitoreo (COEM) y al jefe de la Unidad de Estadística y Tecnologías de la Información lo que su resultado nos permitió identificar el nivel del conocimiento de la los Políticas de seguridad de la información de la institución, además de su nivel de compromiso con el mismo.
- Se desarrolló la guía de las buenas prácticas para la Gestión de proyectos PMBOK, donde se consideró los procesos de dirección del proyecto de Inicio y Planificación, bajo el área de conocimiento de la Gestión de la Integración del Proyecto y la Gestión del Alcance del Proyecto; además del desarrollo de la EDT/WBS (Estructura Desagregada de Trabajo) el cual permitió subdividir el trabajo del proyecto en componentes más pequeños y manejables enfocados al objetivo del proyecto.
- Se desarrolló un inventario de los activos de información pertenecientes o vinculados al área, lo que nos permitió la identificación de los activos más importantes del área, se documentó el modelo del Sistema de Gestión de Seguridad de la información basado en el estándar ISO 27001:2013, la documentación del Análisis de riesgo y de su Gestión de riesgo; además se desarrolló la Declaración de Aplicabilidad la cual nos permitió presentar las consideraciones de la mejoras de los procesos del área que fueron vulnerados y que se considera que cuentan con cierto nivel de riesgo en sus procesos operativos.

RECOMENDACIONES

Se plantea la verificación, corrección y actualización de los procesos de las operaciones donde se presenta vulnerabilidad de acuerdo a la investigación desarrollada, además de la verificación y actualización de los controles del área del Centro de Operaciones, Emergencia y Monitoreo (COEM).

RECOMENDACIONES FINALES A TOMAR EN CUENTA

PERFILES Y ACCESOS

- Se recomienda llevar las medidas correctivas en la verificación de los perfiles de cada trabajador del Centro de Operaciones, Emergencia y Monitoreo (COEM), considerando mayor énfasis en la verificación de accesos no autorizados.

CLAVES

- El uso de las claves de acceso para los sistemas por parte de los trabajadores del COEM se debe cumplir con los protocoles de seguridad, además de la verificación y seguimiento del mal uso de las claves de accesos entre los trabajadores.
- Implementar que el uso de cada clave de acceso para cualquier sistema o aplicación sea no mayor a 30 días calendarios sin excepción, lo cual obligue al jefe del Centro de Operaciones, Emergencia y Monitoreo (COEM) a cambiar su clave de acceso.

EQUIPOS DE ALMACENAMIENTO, COMUNICACIONES, VIDEO Y DE USUARIO

- Se recomienda la auditoria y revisión historia de cada equipo del Centro de Operaciones, Emergencia y Monitoreo (COEM).

- Llevar a cabo la identificación, autenticación y ubicación de los equipos, además de la custodia o verificación a través de un documento que garantice este proceso.

DOCUMENTOS

- Los documentos físicos como, informes, oficios, denuncias que represente un activo de información que procede del cliente (población en general) o alguna institución gubernamental, se debe escanear y guardar en archivo digital y físico, clasificado por tipo de activo de información y fechas correspondientes.
- Además de desarrollar procedimiento de un muestreo aleatorio para verificación de estos documentos de esta manera reducir la pérdida o errores cometidos por los trabajadores del Centro de Operaciones, Emergencia y Monitoreo (COEM).
- Se recomienda ejecutar encuestas a todo el personal del Centro de Operaciones, Emergencia y Monitoreo (COEM) de la Municipalidad Distrital de Bellavista - Sullana y evaluar su desempeño, actitud y la mejora del mismo, basado en las políticas y normativas de seguridad de la información y así perfeccionar y minimizar el riesgo de los activos de información ya observados.
- Se recomienda mantener una constante revisión de la política del SGSI y verificar el cumplimiento de la misma parte de los trabajadores de la institución, además de la existencia de cambios en los requisitos legales que impacten en el SGSI.
- Se recomienda establecer los mecanismos que permitan la identificación de nuevos activos de información para tomar acciones correctivas frente a nuevas vulnerabilidades, amenazas o riesgos detectados y con base a esa información y tomar acciones preventivas.
- Se recomienda seguir con el uso de la metodología en consideración a la identificación de nuevos riesgos que aparezcan.
- Y finalmente se recomienda; formar, capacitar y promover el compromiso periódicamente al personal en temas de seguridad de la información

REFERENCIAS BIBLIOGRAFICAS

Agramonte Albán, A. M. (2016). *Auditoría del sistema de seguridad de información en el hospital III José Cayetano Heredia – Castilla; 2016.* (Tesis de título) Universidad Católica Los Ángeles de Chimbote del Perú. Recuperado de: http://repositorio.uladech.edu.pe/bitstream/handle/123456789/918/SEGURIDAD_AUDITORIA%20_AGRAMONTE%20_ALBAN_ANA%20_MARIA.pdf?sequence=1

Aguirre Mollehuanca, D. A. (2014). *Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A.* (Tesis de título) Pontificia Universidad Católica del Perú. Recuperado de: http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/5677/AGUIRRE_DAVID_SISTEMA_GESTION_SEGURIDAD_INFORMACION_SERVICIOS_POSTALES.pdf?sequence=1&isAllowed=y

Arroyo Alarcón, F., Inseguridad Informática (Revista TEC)
Recuperado de: http://www.itsteziutlan.edu.mx/site2010/index.php?option=com_content&view=article&id=763:inseguridad-informatica&catid=27:artlos&Itemid=288

Barragán I., Góngora I. & Martínez, E. (2013). *Implementación de políticas de seguridad informática para la M.I. municipalidad de Guayaquil aplicando la norma iso/iec 27002.* (Tesis de título) Escuela Superior Politécnica del Litoral) Guayaquil, Ecuador.
Recuperado de: http://www.dspace.espol.edu.ec/bitstream/123456789/21546/2/ManualTopico.pf

Benavides, G.P., Seguridad informática (Servicios - Consultoría en riesgo de negocios)

Recuperado de:
https://www.grantthornton.com.co/servicios/consultoria-en-riesgo-de-negocios/seguridad-informatica/

Berrío López, J. P. (2016). *Metodología para la evaluación del desempeño de controles en sistemas de gestión de seguridad de la información sobre la norma ISO/IEC 27001*. (Tesis de Investigación) Universidad Nacional de Colombia de Colombia. Recuperado de:
http://bdigital.unal.edu.co/56173/1/1128401087.2017.pdf

Camargo Ramírez, J. D. (2017). *Diseño de un Sistemas de Gestión de la Seguridad de la Información (SGSI) en el Área Tecnológica de la Comisión Nacional del Servicio Civil – CNSC basado en la Norma ISO 27000 e ISO 27001*. (Trabajo de Grado) Universidad Nacional Abierta y a Distancia de Colombia. Recuperado de:
https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/11992/1/75104100.pdf

De La Cruz Vargas, R. E. (2016). *Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la municipalidad provincial de Paita; 2016.* (Tesis de título) Universidad Católica Los Ángeles de Chimbote del Perú. Recuperado de:
http://repositorio.uladech.edu.pe/bitstream/handle/123456789/255/DE_LA_CRUZ_VARGAS_RONALD_EDUARDO_BUENAS_PRACTICAS_SEGURIDAD_INFORMACION.pdf?sequence=1

García López, P., Principales Novedades de la ISO 27001/ISO 27002 (Jornadas Técnicas 2013 - Dibujando el nuevo escenario normativo en el siglo XXI)
Recuperado de:

http://www.isaca.org/chapters7/Madrid/Events/Documents/Principales%20Novedades%20de%20la%20ISO27001ISO%2027002%20-%20Paloma%20Garcia.pdf

ISO 27000.es, Ciclo Deming (2005)- mejora continua (El portal de ISO 27001 en español).
Recuperado de:
http://www.iso27000.es/sgsi.html

ISO 27000.es, ¿Qué es un SGSI? (El portal de ISO 27001 en español)
Recuperado de:
http://www.iso27000.es/sgsi.html

Olivos Guerra, F. O. & Guevara Saldaña, E. W. (2017). *Formulación de políticas de control de accesos y seguridad física y del entorno basado en la norma técnica peruana NTP-ISO/IEC 17799 para la mejora de la gestión en la oficina central de cómputo – Universidad de Lambayeque* (Tesis de título) Universidad de Lambayeque, Perú. Recuperado de:
http://repositorio.udl.edu.pe/bitstream/UDL/110/1/olivos%20guevara%20_%20guevara%20saldaña.pdf

Villamizar, C., Elementos del Riesgo (Identificación y Administración del Riesgo)
Recuperado de:
https://pt.slideshare.net/clauditasuvi/exposicion-7288461/7

Villena Aguilar, M. A. (2006). *Sistema de gestión de seguridad de información para una institución financiera.* (Tesis de título) Pontificia Universidad Católica del Perú. Recuperado de:
http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/362/VILLENA_MOISÉS_SISTEMA_DE%20GESTIÓN_DE_SEGURIDAD_DE_INFOR

MACIÓN_PARA_UNA_INSTITUCIÓN_FINANCIERA.pdf?sequence=1&isAllowed=y

ANEXOS

UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERIA INFORMATICA Y DE SISTEMAS

ENCUESTA AL PERSONAL DEL AREA ESTADISTICA Y TECNOLOGIAS DE LA INFORMACION Y DEL CENTRO DE OPERACIONES DE EMERGENCIA Y MONITOREO

PROYECTO: SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA EL CENTRO DE OPERACIONES, EMERGENCIA Y MONITOREO (COEM) DE LA MUNICIPALIDAD DISTRITAL DE BELLAVISTA - SULLANA

OBJETIVO: Recolectar información confiable y confidencial del personal del Centro de operaciones de emergencia y monitoreo (COEM), que permita el desarrollo de un Sistema de Seguridad de la Información, Según ISO 27001:2013 en la Municipalidad Bellavista-Sullana - Piura.

CUESTIONARIO N° 01

DIAGNÓSTICO DEL ESTADO ACTUAL DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN EL CENTRO DE OPERACIONES, EMERGENCIA Y MONITOREO DE LA MUNICIPALIDAD DE BELLAVISTA.

Instrucción: Sírvase por favor responder con sinceridad a cada pregunta formulada para el estudio, marcando con una (X) la alternativa de la pregunta que Usted considere conveniente. En tal sentido, agradecemos su colaboración y le invocamos ser objetivo y honesto en sus apreciaciones, la encuesta es anónima.

Preguntas	SI	NO
1. ¿La municipalidad distrital de Bellavista - Sullana cuenta con un comité de seguridad de la información?		
2. ¿Cree usted que el diseño de un plan de la seguridad de la información permitirá mejorar la calidad tecnológica?		

3. ¿Cree usted que se logrará un cambio positivo con la aplicación del plan de la seguridad de la información en la política de la seguridad de la información?		
4. ¿Aprobaría usted la implementación del plan de seguridad de la Información para la política de seguridad de la información?		
5. ¿A usted se le brinda capacitación acerca de seguridad de la información?		
6. ¿Puede identificar a las personas que no trabajan en la Municipalidad distrital de Bellavista - Sullana?		
7. ¿Sabe usted si existe un plan de recuperación ante desastres?		
8. ¿Sabe usted si se ha realizado evaluación de riesgos relacionados con la información?		
9. ¿Tiene usted conocimiento sobre lo que significa un plan de la seguridad de la información?		
10. ¿Sabe usted si se cuenta con software antivirus actualizado?		

UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERIA INFORMATICA Y DE SISTEMAS

ENCUESTA AL PERSONAL DEL AREA ESTADISTICA Y TECNOLOGIAS DE LA INFORMACION Y DEL CENTRO DE OPERACIONES DE EMERGENCIA Y MONITOREO

PROYECTO: SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA EL CENTRO DE OPERACIONES, EMERGENCIA Y MONITOREO (COEM) DE LA MUNICIPALIDAD DISTRITAL DE BELLAVISTA - SULLANA

OBJETIVO: Recolectar información confiable y confidencial del personal del Centro de operaciones de emergencia y monitoreo (COEM), que permita el desarrollo de un Sistema de Seguridad de la Información, Según ISO 27001:2013 en la Municipalidad Bellavista-Sullana - Piura.

CUESTIONARIO N° 02

NECESIDAD DE POLÍTICAS BASADAS EN BUENAS PRÁCTICAS PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL CENTRO DE OPERACIONES, EMERGENCIA Y MONITOREO DE LA MUNICIPALIDAD DE BELLAVISTA.

Instrucción: Sírvase por favor responder con sinceridad a cada pregunta formulada para el estudio, marcando con una (X) la alternativa de la pregunta que Usted considere conveniente. En tal sentido, agradecemos su colaboración y le invocamos ser objetivo y honesto en sus apreciaciones, la encuesta es anónima.

Preguntas	SI	NO
1. ¿Considera usted que deben existir políticas de la seguridad de la información para la gestión del Sistema de seguridad de la información?		
2. ¿Existe un documento donde se especifiquen las políticas de la seguridad de la información?		

3. ¿Usted comunica oportunamente alguna incidencia sobre seguridad detectada?		
4. ¿El manejo de la información de la organización está en manos del personal que tiene responsabilidad directa sobre ella?		
5. ¿Indique si existen programas dirigidos a sensibilizar sobre la seguridad de la información para todos los trabajadores?		
6. ¿Existe un documento donde los empleados, contratista y proveedores acuerden la confidencialidad de la información?		
7. ¿Has utilizado algún dispositivo externo para extraer algún tipo de información o de su interés?		
8. ¿Existe un documento donde estén definidas las responsabilidades para la contratación, terminación o cambio de cargo o funciones para los empleados, con la finalidad de proteger los recursos informáticos?		
9. ¿Usted sabe distinguir la información que es de estrictamente confidencial, de uso interno o pública?		
10. ¿Se realiza la revisión periódica interna de los riesgos inicialmente detectados, políticas, procedimientos y controles relacionados al sistema de seguridad de la información?		

CENTRO DE OPERACIONES, EMERGENCIA Y MONITOREO (COEM)
MUNICIPALIDAD DISTRITAL DE BELLAVISTA – SULLANA

Figura 01: COEM - Bellavista
Fuente: Elaboración Propia

Figura 02: SALA DE OPERADORES DEL COEM - BELLAVISTA
Fuente: Elaboración Propia

Figura 03: DATA CENTER DEL COEM - BELLAVISTA
Fuente: Elaboración Propia

Figura 04: TABLERO DE COMUNICACIONES ENTRE CAMARA Y DATA CENTER
Fuente: Elaboración Propia

Figura 05: CAMARA PTZ
Fuente: Elaboración Propia

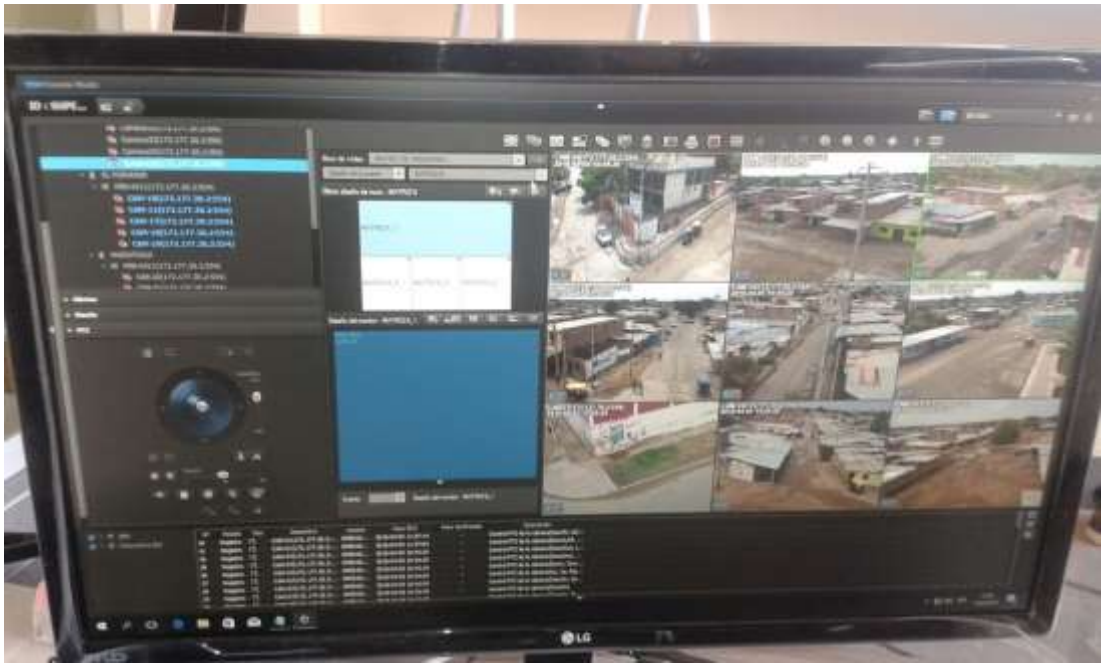


Figura 06: SSM CONSOLE STUDIO
Fuente: Elaboración Propia

Figura 07: TURBO NET (Monitor izquierdo) – SISTEMA DE EMERGENCIA C4I (MONITOR DERECHO)
Fuente: Elaboración Propia

Figura 08: TRABAJADORES DEL COEM BELLAVISTA
Fuente: Elaboración Propia

Figura 09: OPERADORES DE VIDEOCAMARAS DEL COEM BELLAVISTA
Fuente: Elaboración Propia

Figura 10: SALA DE CRISIS
Fuente: Elaboración Propia

Figura 11: REUNIONES CODISEC
Fuente: Elaboración Propia