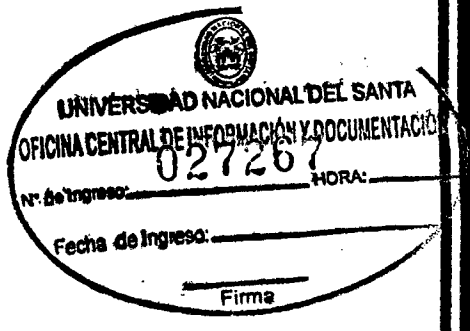
UNIVERSIDAD NACIONAL DEL SANTA

UNIVERSIDAD NACIONAL DEL SANTA

FACULTAD DE INGENIERÍA

E.A.P. DE INGENIERÍA DE SISTEMAS E INFORMÁTICA



"SISTEMA DE GESTIÓN PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN LA INSTITUCIÓN SERVICIOS INDUSTRIALES DE LA MARINA"

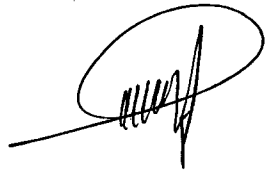
TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

INVESTIGADOR:

BACH. JEINER MARTÍNEZ RAMOS

ASESOR :

ING. LUIS RAMÍREZ MILLA



NVO. CHIMBOTE - PERÚ

2014

UNIVERSIDAD NACIONAL DEL SANTA

FACULTAD DE INGENIERÍA

E.A.P. DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

"SISTEMA DE GESTIÓN PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN EN LA INSTITUCIÓN SERVICIOS INDUSTRIALES DE LA MARINA"

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

APROBADO POR EL SIGUIENTE JURADO EVALUADOR

Mg. Hugo Caselli Gismondi
Presidente

Mg. Carlos Vega Moreno
Integrante

Ing. Pedro Manco Pulido
Integrante

NVO. CHIMBOTE –PERU
2014

INDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

DEDICATORIA

A Dios por haberme dado la dicha
de la vida y permitirme concluir con
éxito mi carrera profesional.

A mis padres, Luis Martínez Aramburú
y Carmen Ramos Torres, por haberme
brindado día a día su apoyo incondicional
durante mi formación profesional.

A mis hermanos Luis y Elías;
y hermanas Jeily y Magdalena,
por apoyarme en todo momento
y brindarme su confianza.

A todos mis profesores, por haberme
transmitido sus conocimientos y
experiencias a lo largo de mi formación
profesional.

A todas aquellas personas que
estuvieron a mi lado siempre y
compartieron conmigo muchos
momentos.

AGRADECIMIENTO

Para el logro del presente trabajo recibí el apoyo de muchas personas que contribuyeron con su ayuda a la realización y finalización del informe de tesis, a quienes expreso mis sinceros agradecimientos:

A Dios por haberme dado la vida y el apoyo constante día tras día

A mis padres, que gracias a sus esfuerzos permitieron que pueda finalizar con éxito mi carrera profesional

A mis hermanos, que siempre me brindaron su apoyo y consejos en los momentos que necesite de ellos.

A Joanna Rodríguez, por sus consejos y apoyo para la finalización del presente trabajo.

A la Universidad Nacional del Santa y a los docentes, por la enseñanza recibida durante el transcurso de mi formación profesional.

A mi asesor Luis Ramírez Milla, que con su conocimiento y experiencia me guió durante el transcurso del presente informe de tesis.

Al Ing. Santos Blas, por su apoyo durante mi permanencia en los Servicios Industriales de la Marina.

Al personal de la División de Tecnologías de la Información, por su colaboración y apoyo para el éxito del presente trabajo de tesis.

PRESENTACIÓN

SEÑORES MIEMBROS DEL JURADO EVALUADOR:

UNIVERSIDAD NACIONAL DEL SANTA

De mi mayor consideración:

En cumplimiento a lo dispuesto en el Reglamento General de Grados y Títulos de la Universidad Nacional del Santa y en conformidad a la Ley Universitaria N° 23733 y al D.L. N° 739 para optar el Título de INGENIERO en la Escuela Académico Profesional de Ingeniería de Sistemas e Informática, pongo a vuestra disposición el presente proyecto de tesis titulado: "**Sistema de Gestión para mejorar la Seguridad de la Información en la Institución Servicios Industriales de la Marina**", para su valiosa revisión y aprobación.

La presente tesis tiene como lugar de aplicación la Institución Servicios Industriales de la Marina (SIMA) de la ciudad de Chimbote, cuyo propósito consiste en implementar los procesos del Sistema de Gestión para mejorar la Seguridad de la Información.

Atentamente,

Bach. Jeiner Martínez Ramos

RESUMEN

La presente tesis se realizó en la Institución Servicios Industriales de la Marina (SIMA) de la ciudad de Chimbote, cuyo propósito fue implementar los procesos del Sistema de Gestión de Seguridad de la Información con la finalidad de mejorar los procesos informáticos de la División de Tecnologías de la Información y de esa manera garantizar la confidencialidad, disponibilidad e integridad de la información.

Se implementaron los procesos de clasificación y control de activos, seguridad ligada al personal, seguridad física y del entorno, gestión de comunicaciones y operaciones, adquisición, desarrollo y mantenimiento de sistemas, control de accesos y gestión de continuidad del negocio; los cuales permitieron clasificar adecuadamente los activos de la Institución, mejorar el control de acceso a los servicios informáticos e implementar una cultura de seguridad de información a todos los usuarios de la Institución.

Logrando así gestionar la seguridad de la información de todos los procesos de la División de Tecnologías de la Información, y de esta manera lograr reducir el número de observaciones por parte de la Oficina de Gestión de Control en las auditorías de seguridad de la información que se realizan periódicamente.

Autor: Bach. Jeiner Martínez Ramos

Asesor: Ing. Luis Ramírez Milla

ABSTRACT

This thesis was performed at the Institute of Marine Industrial Services (SIMA) of the city of Chimbote, whose purpose was to implement processes Management System Information Security in order to improve computer processes Technology Division Information and thereby ensure the confidentiality, availability and integrity of information.

Processes of asset classification and control, security linked to personal, physical and environmental security, communications and operations management, acquisition, development and maintenance of systems, access control and business continuity management were implemented, which allowed to classify properly assets of the Institution, improve the control of access to computer services and implement a culture of safety information to all users of the Institution.

Achieving and managing information security in all processes of the Division of Information Technology and thus to reduce the number of observations by the Office of Management Control in security audits of the information place regularly.

Author: Bach. Jeiner Martínez Ramos

Adviser: Ing. Luis Ramírez Milla

INTRODUCCIÓN

En la actualidad las tecnologías de información han ido evolucionando a razón de progresión geométrica, permitiendo reducir el tiempo de procesamiento de los procesos tecnológicos de las Empresas. Los sistemas de información cada vez se diseñan con mayores propósitos estratégicos que operacionales, ayudando a la toma de decisiones a través de la información que se obtiene y permitiendo su almacenamiento en diferentes dispositivos de seguridad.

Situación que ha implicado que las Empresas brinden una mayor importancia a la seguridad de la información, ya que así como evoluciona la tecnología también se ha evidenciado el crecimiento de ataques informáticos, que a través del uso de software tratan de alterar o sustraer información clasificada como confidencial para uso indebido. Es por ello que el presente trabajo de tesis titulado **"Sistema de Gestión para mejorar la Seguridad de la Información e la Institución Servicios Industriales de la Marina"** tiene por finalidad implementar los procesos de un Sistema de Gestión de Seguridad a los procesos informáticos de la División de Tecnologías de la Información. Consiguiendo así garantizar la confidencialidad, disponibilidad e integridad de la información distribuida y almacenada en los equipos informáticos de la Institución. El trabajo de tesis de encuentra dividido en siete capítulos, los cuales se detallan a continuación:

EL CAPÍTULO I: describe los datos de la Institución (nombre, dirección, misión, visión, valores, estructura organizativa, etc.)

EL CAPÍTULO II: describe el plan de investigación, indicando la realidad problemática, análisis, formulación y antecedentes del problema, hipótesis, objetivos generales y específicos, etc.

EL CAPÍTULO III: describe el marco referencial a emplearse en el presente trabajo, indicando los conceptos e información necesaria para facilitar su realización.

EL CAPÍTULO IV: describe los resultados, indicando el desarrollo de los procesos del sistema de gestión de seguridad y los resultados de su aplicación en la División de Tecnologías de la Información.

EL CAPÍTULO V: describe la discusión a través de la comprobación de las hipótesis formuladas y las conclusiones por cada indicador.

EL CAPÍTULO VI: describe las conclusiones generales y específicas luego de haber finalizado el trabajo de tesis.

EL CAPÍTULO VII: describe las recomendaciones que debe tomar en cuenta la Institución para continuar mejorando la seguridad de la información.

Finalmente se detallan las conclusiones y recomendaciones obtenidas de la presente tesis.

CAPITULO I

DATOS GENERALES DE LA INSTITUCIÓN

1.1 Nombre

Servicios Industriales de la Marina Chimbote (Sima Chimbote)

1.2 Domicilio legal

El Centro de Operaciones de Sima Chimbote se encuentra ubicado en Avenida Los Pescadores N° 151, Zona Industrial 27 de Octubre, Distrito de Chimbote, Provincia del Santa, Departamento de Ancash.

1.3 Misión

La misión de Sima Chimbote es efectuar el mantenimiento, modernización, diseño y construcción de las unidades de la Marina de Guerra del Perú y complementariamente ejecutar proyectos relacionados con la industria naval y metal mecánica para el sector estatal y privado, dentro de los más exigentes estándares de calidad, con el fin de contribuir a la Defensa Nacional y al desarrollo socio-económico y tecnológico del país.

1.4 Visión

La visión de Sima Chimbote es ser reconocido como el mejor Astillero Naval en Latinoamérica, orgullo de la industria nacional.

1.5 Valores

Los valores que tiene cada trabajador de Sima Chimbote son:

- Entrega de personal
- Identificación y orgullo de ser trabajador de Sima Chimbote
- Destreza y calidad del trabajo
- Integridad
- Competencia
- Compromiso con la mejora continua

1.6 Centros de operaciones

Sima Chimbote cuenta con 03 centros de operaciones en el país, los cuales se encuentran distribuidos en lugares estratégicos al entorno de la construcción y reparación de buques industriales, pesqueros y militares.

Los centros de operaciones son:

- Sima Chimbote (astillero y metal mecánica)
- Sima Callao
- Sima Iquitos

1.7 Certificaciones

Sima Chimbote cuenta con las siguientes certificaciones:

- ISO 9001:2008 – Gestión de calidad
- ISO 14001:2004 – Gestión ambiental
- OHSAS 18001:2007 – Gestión de seguridad y salud en el trabajo

1.8 Organigrama Estructural

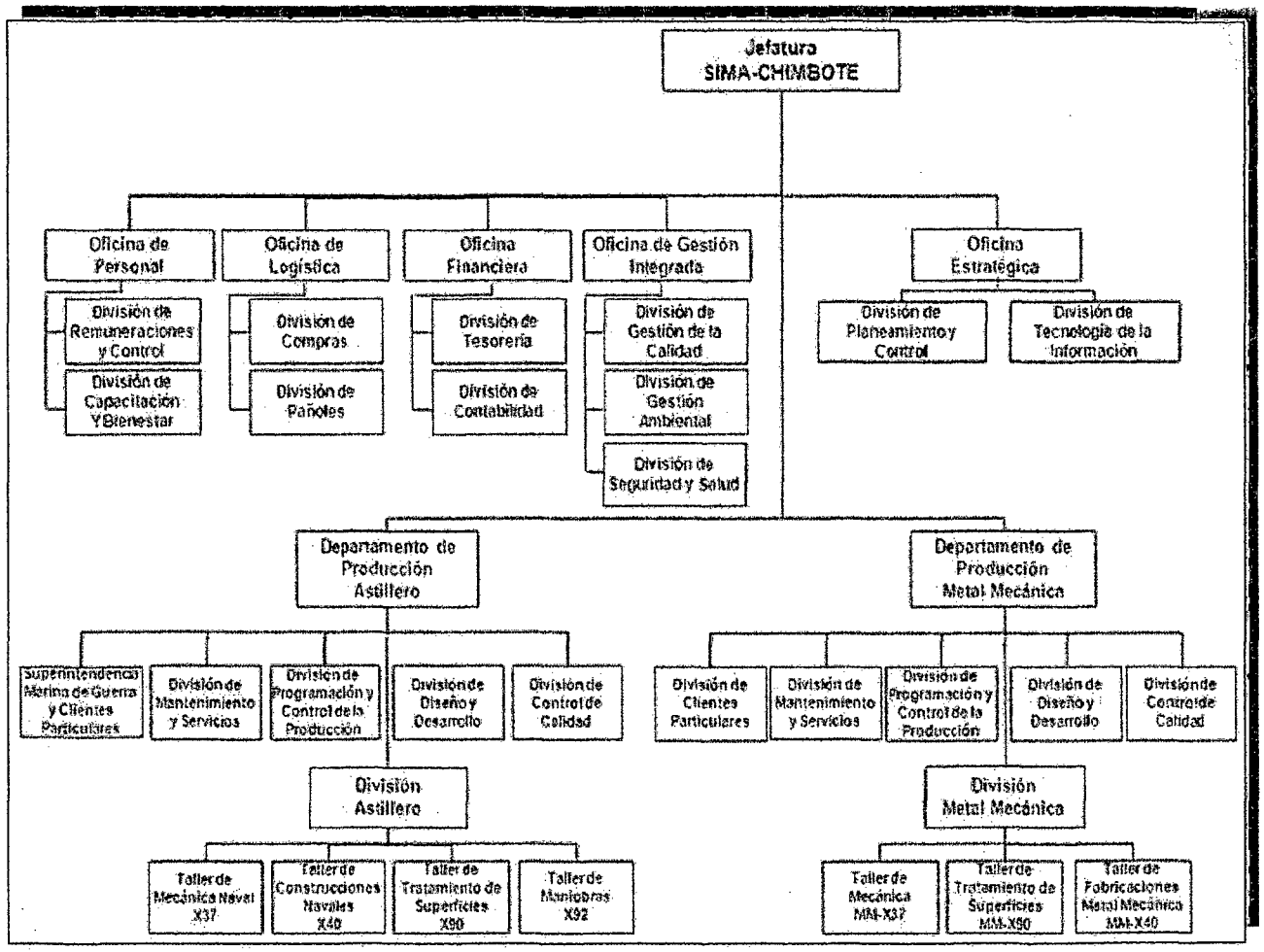


Figura Nº 01: Organigrama Estructural de Sima Chimbote

1.9 Área de Estudio

El área donde se realizó la investigación es la División de Tecnologías de la Información (DTI), quien es la encargada de llevar a cabo todas las funciones relacionadas a tecnologías de la información (sistemas, redes, informática, etc.).

La DTI está conformada por las áreas de Desarrollo de Sistemas, Soporte Informático y Seguridad de la Información.

CAPITULO II

PLAN DE INVESTIGACIÓN

2.1 El Problema

2.1.1 Realidad Problemática

Los Servicios Industriales de la Marina Chimbote (Sima Chimbote) es el mayor astillero nacional para embarcaciones de bajo bordo y uno de los principales centros de producción de metal mecánica en el país. Brinda en todo momento servicios de calidad a sus clientes, contribuye con la conservación del medio ambiente y brinda una seguridad y salud adecuada a todos sus trabajadores.

Cuenta actualmente con oficinas y divisiones, dentro de las cuales se encuentra la División de Tecnologías de la Información (DTI), quién se encarga de brindar a las diferentes áreas la información estratégica requerida para la toma de decisiones en los diferentes niveles organizacionales, a través de la aplicación de las tecnologías de información. La DTI está conformada por las áreas de Desarrollo de Sistemas, Soporte Informático y Seguridad de la Información; de esta manera la DTI se encarga de dar cumplimiento a las funciones establecidas en el Manual de Organización y Funciones vigente. Los problemas relacionados a la seguridad de la información son los siguientes:

El personal de desarrollo de sistemas desconoce las nociones de seguridad de la información, ya que ningún sistema de información tiene implementado controles de seguridad que garanticen un procesamiento adecuado de la información (controles de entrada, procesamiento y salida). Lo que ha venido originando que el 50% de los sistemas registren datos incompletos, incoherentes y por lo tanto el resultado no sea el correcto y adecuado. Provocando que se emplee tiempo adicional en solucionar estos problemas.

El 80% de los usuarios de los servicios informáticos proporcionan información confidencial (contraseñas), lo que ha originado que en 02

ocasiones, desde áreas como contabilidad y tesorería se operen los sistemas asignados exclusivamente al área de personal (control de asistencia, cálculo de las planillas, etc.) provocando problemas internos y manipulación de información no autorizada.

El 90% de contraseñas de los usuarios no cumplen con niveles de seguridad adecuados ya que se realizó una verificación y se pudo comprobar que usan datos como su primer nombre, nombre del área, números del 1 al 6, nombre del sistema, nombre de alguna familiar, etc. Información que es sencilla de obtener por cualquier usuario, lo que ha ocasionado que en mas de 07 ocasiones se manipulen sistemas e información por parte de usuarios que desconocen la correcta operación de dichos sistemas, teniendo que intervenir en estos casos el personal de desarrollo de sistemas para corregir dicha manipulación.

La DTI alberga activos informáticos de gran importancia para la Empresa (servidores, equipos de comunicaciones, base de datos, sistemas de información, documentación, software, etc.). Pero frente a un simulacro de tsunami realizado en la Institución el personal de la DTI no supo que activos salvaguardar en primera instancia; ya que no existe una clasificación de los activos de acuerdo al nivel de importancia para la continuidad de los servicios informáticos frente a algún desastre.

La DTI por ser un área que aloja equipos e información de gran importancia para la Empresa debe implementar cámaras que permita monitorear y supervisar en todo momento el ingreso de personal interno y externo (contratistas, técnicos de telefónica, visitas, etc.); ya que diariamente ingresan un promedio de 45 personas al área, y en una ocasión ingresó personal técnico a la sala de servidores y por alguna mala manipulación dejó sin servicios informáticos a los usuarios; y en este caso nadie supo quien provocó el incidente, ya que no se realizó dicho registro.

En 04 oportunidades se pudo verificar que usuarios de diferentes áreas tenían más niveles de accesos sobre los sistemas (eliminar y modificar). Lo que ocasionó que se elimine información del sistema de producción,

relacionado a operaciones realizadas durante la semana. Para ello fue necesario ingresar y procesar nuevamente la información. Todo ello debido a que no se realiza un control periódico de los niveles de accesibilidad de los usuarios sobre el uso de los sistemas en relación al tipo de usuario y área donde se encuentran.

La baja de los usuarios sobre los servicios informáticos (sistemas, computadora, correo electrónico) se realiza hasta con 02 semanas de retraso, debido a que el Jefe de dicha área no comunica a la DTI dicha situación y ni el encargado de seguridad de la información se comunica con el área de personal para obtener información de los usuarios que renuncian, son despedidos o no son renovados (con acceso a los servicios informáticos). Se pudo comprobar en 03 ocasiones que usuarios de la misma área (logística, contabilidad, personal) usaron los servicios informáticos del personal que ya no forma parte de la Institución, provocando el uso incorrecto de los sistemas correspondientes.

No se realiza un control del acceso que realiza el personal de desarrollo (analistas de sistemas y programador) a las librerías y código fuente de los sistemas en producción, dando la posibilidad a que el personal de desarrollo acceda al código fuente de sistemas a los que no se encuentra asignado y debido a su desconocimiento realice alteraciones que pueden afectar con el funcionamiento normal de los sistemas, ya que estos se encuentran en producción y son utilizados por los diferentes usuarios para el procesamiento de la información.

En la codificación de los sistemas de información no se implementan reglas de integridad y validación, lo que originó en mas de 04 ocasiones, desbordamiento de la información en los sistemas de comercial y producción, generándose así un conflicto en el sistema por lo cual no estuvo disponible por un lapso de 01 hora, dejando sin servicio informático a los usuarios.

La Institución se encuentra ubicada cerca del mar, por lo cual después de un sismo se podría originar un tsunami o maremoto; u otro desastre

(incendio, sismo, etc.). Razón por la cual debe existir un plan de contingencias debidamente actualizado y realizado dentro de la Institución como simulacro frente a los desastres mencionados anteriormente. Pero se pudo comprobar que más del 50% del personal de la DTI desconoce que actividades realizar en estas situaciones, a la vez el plan de contingencias se encuentra desactualizado y no contempla toda la información necesaria para poder actuar y recuperarse frente algún desastre.

2.1.2 Análisis del Problema

La presencia de estos problemas relacionados con la seguridad de la información en la DTI, se debe a los siguientes factores:

- ✓ No se cumplen adecuadamente las funciones de seguridad de la información, tales como coordinación de las acciones sobre mejoramiento de los sistemas respecto a medidas de seguridad, mantener políticas y estándares vigentes de seguridad, identificar objetivos de seguridad, realizar evaluaciones periódicas sobre las vulnerabilidades en los sistemas, capacitaciones a los usuarios de los servicios informáticos en temas de seguridad de la información, etc.

- ✓ Falta de interés por parte del personal de desarrollo de sistemas, en investigar y aplicar los estándares de seguridad de la información; para garantizar que los sistemas de información estén disponibles en todo momento, estén permitidos solo a usuarios autorizados y conserven la información en los diferentes procesos.

- ✓ Falta de interés por parte del personal de soporte técnico, en implementar medidas de seguridad en los equipos informáticos y la red.

- ✓ El 95% del tiempo se emplea para actividades de desarrollo de sistemas y soporte técnico, dejando de lado las actividades de seguridad de la información.

Para poder solucionar los problemas detallados anteriormente es necesario implementar un conjunto de políticas, procedimientos y estándares; que permitan garantizar en todo momento una confidencialidad, disponibilidad e integridad de la información; a la vez debe existir el compromiso por parte del personal de seguridad de la información en cumplir adecuadamente sus funciones; y la capacitación permanente al personal (desarrollo de sistemas y soporte técnico).

2.1.3 Formulación del Problema

¿En qué medida el Sistema de Gestión permitirá mejorar la Seguridad de la Información en la Institución Servicios Industriales de la Marina?

2.1.4 Antecedentes del Problema

Los siguientes Proyectos de Investigación realizados por egresados de la Universidad Nacional del Santa permitieron resolver problemas parecidos de los cuales afronta el presente Proyecto, para lo cual se detallan a continuación:

- Sistema de Gestión de Seguridad de la Información para la financiera Edyficar - oficina de Nuevo Chimbote
Autores: María Flores Coronel y Jessica Ruiz Cortez
Año: 2011
Resumen: La presente Tesis tiene por objeto investigar las normas y estándares que van difundiéndose con mayor énfasis en el mercado peruano, en especial en el sector financiero. Para lo cual se pretende rescatar los aspectos más saltantes de cada norma y estándar, a partir de los cuales se va a plantear un esquema de gestión de seguridad de información que puede ser empleado por una Financiera en el Perú, en este caso su aplicabilidad será en la Financiera Edyficar.

Conclusión: Se planteó un esquema de seguridad lo cual permitió implementar normas y estándares sobre cada proceso de la Institución; mejorando de esta manera la seguridad de los diferentes procesos financieros y de la información con la que se trabaja. Esta investigación

ayudó a establecer un esquema basado en normas y estándares de seguridad de la información, para su posterior aplicación.

Información utilizada: Se utilizó información relacionada a normas y estándares de seguridad de la información, con la cual se permitió facilitar la investigación.

- Auditoría de las comunicaciones y seguridad informática para optimizar los controles y procedimientos informáticos de la Empresa Pesquera Tecnológica de Alimentos S.A - sede Malabrigo.
Autores: Bonye Villarreal Sánchez y Glirio Sarzo Miranda
Año: 2010
Resumen: El presente informe de tesis desarrolla una auditoría a las comunicaciones y seguridad informática en la Sede Malabrigo de la Pesquera Tecnológica de Alimentos S.A., con el fin de revelar la consistencia de las políticas y procedimientos prescriptos, y el cumplimiento de los mismos. Como resultado se detallan las debilidades encontradas y se emiten las recomendaciones que contribuyan a mejorar su nivel de seguridad. Finalmente se concluye con la contrastación de la hipótesis de cada uno de los segmentos establecidos, como resultado del desarrollo de la Auditoría a las Comunicaciones y Seguridad Informática.

Conclusión: Se realizó una auditoría de seguridad informática y se pudo obtener las debilidades que tiene la Empresa respecto a seguridad de la información; realizándose las recomendaciones necesarias para su mejoramiento. Esta investigación ayudó en la elaboración de procedimientos y políticas de seguridad; previos a una auditoría realizada.

Información utilizada: Se utilizó información relacionada al proceso de auditoría de seguridad informática, con lo cual se facilitó realizar dicho proceso en la Empresa.

- Auditoría orientado a los sistemas de información, comunicaciones y seguridad informática en corporación pesquera San Antonio S.A oficina Samanco.

Autor: Edward Romero Bustamante

Año: 2001

Resumen: El presente informe de tesis realiza una auditoria a los sistemas de información, comunicaciones y seguridad informática en la corporación pesquera San Antonio, con el fin de verificar las políticas y procedimientos, junto al cumplimiento de los mismos. Como resultado se detallan las debilidades encontradas y se emiten las recomendaciones que contribuyan a mejorar el nivel de seguridad en los procesos auditados.

Conclusión: Se realizó la auditoría a la seguridad informática, comunicaciones y sistemas de la información, detallándose las debilidades y recomendaciones a la Empresa. Esta investigación ayudó a verificar de manera adecuada las políticas y procedimientos de seguridad de la información.

Información utilizada: Se utilizó información relacionada a políticas y procedimientos para garantizar una adecuada implementación de la seguridad de la información.

2.1.5 Justificación

Justificación Social

La realización del presente Proyecto de Investigación en la DTI permitirá lo siguiente:

- ✓ Controlar y clasificar adecuadamente los activos de gran importancia.
- ✓ Controlar adecuadamente el acceso a los servicios informáticos.
- ✓ Promover una cultura de seguridad entre los usuarios de los diferentes servicios informáticos.
- ✓ Brindar a los usuarios servicios adecuados.

- ✓ Garantizar una adecuada recuperación ante posibles contingencias.

Justificación Económica

Sima Chimbote es una Institución que cuenta con recursos económicos necesarios para invertir en la realización de proyectos que mejoren los servicios que actualmente brinda, y debido a que el presupuesto del proyecto no es demasiado alto entonces no existen inconvenientes para su ejecución.

Justificación Operativa

Para la ejecución del Sistema de Gestión, Sima Chimbote cuenta actualmente con todos los recursos necesarios (personal, software, hardware, etc.) para lograr una adecuada gestión de la seguridad de la información.

2.1.5 Importancia de la Investigación

La realización del presente Proyecto denominado "Sistema de Gestión para mejorar la Seguridad de la Información en la Institución Servicios Industriales de la Marina", es de gran importancia ya que permitirá lo siguiente:

- ✓ Gestionar adecuadamente la seguridad de la información sobre los activos de gran importancia.
- ✓ Controlar de manera adecuada el acceso a la información sensible por parte de los usuarios.
- ✓ Proteger la información sensible de robos o ataques de agentes externos.
- ✓ Clasificar los activos de acuerdo a su nivel de importancia para la continuidad de las actividades de la Empresa.
- ✓ Incentivar una cultura de seguridad de la información entre los usuarios.

2.2 Objetivos

2.2.1 Objetivo General

- ✓ Mejorar la Seguridad de la Información en la Institución Servicios Industriales de la Marina.

2.2.2 Objetivos Específicos

- ✓ Utilizar la metodología PDCA, para una adecuada implementación del sistema de gestión de seguridad.
- ✓ Capacitar periódicamente a los usuarios de los servicios informáticos sobre temas relacionados a la Seguridad de la Información. (C)
- ✓ Establecer y supervisar los niveles de accesibilidad a los sistemas de información. (C)
- ✓ Actualizar y ejecutar el Plan de Contingencias, con la finalidad de preparar y capacitar al personal frente a algún desastre que pueda interrumpir la continuidad de los servicios informáticos. (D)
- ✓ Establecer controles de seguridad (entrada, proceso y salida) en todos los sistemas de información operativos. (I)
- ✓ Implementar niveles adecuados de seguridad en el uso y creación de las contraseñas de acceso a los diferentes servicios informáticos. (I)
- ✓ Clasificar los activos informáticos (servidores, backup, software, documentación, etc.) de acuerdo al nivel de importancia para la Empresa. (I)
- ✓ Establecer un procedimiento para dar de baja a los usuarios de los servicios informáticos. (I)
- ✓ Emplear normas nacionales relacionadas a seguridad de la información, para una adecuada implementación del sistema de gestión de seguridad.

2.3 Hipótesis

El Sistema de Gestión mejora la Seguridad de la Información en la Institución Servicios Industriales de la Marina.

2.4 Variables

2.4.1 Variable independiente

X: Sistema de Gestión

Definición: Sistema de gestión compuesto por un conjunto de políticas, procedimientos y estándares, para mejorar un proceso específico.

2.4.2 Variable dependiente

Y: Seguridad de la Información

Definición: Conjunto de procesos para establecer un nivel de seguridad adecuado a la información.

Indicadores:

***y1:* Confidencialidad de la información**

- Número de accesos garantizados
- Nivel de seguridad de las contraseñas
- Número de niveles de accesibilidad

***y2: D*isponibilidad de la información**

- Número de sistemas de información operativos
- Tiempo de continuidad de los sistemas
- Número de activos clasificados

***y3: I*ntegridad de la información**

- Número de modificaciones no autorizadas
- Numero de permisos establecidos
- Número de controles establecidos

2.5 Metodología

2.5.1 Tipo de investigación

El tipo de investigación es ***aplicada***, porque se hace uso de las teorías y las leyes de la investigación básica y sobre gestión de seguridad de la información. A la vez se utilizará información obtenida en diferentes investigaciones relacionadas con el tema, las cuales servirán de ayuda para poder resolver el problema identificado.

2.5.2 Nivel de investigación

El nivel de investigación es ***descriptivo***, porque se señala como se manifiesta un fenómeno o evento; cuando se busca especificar las propiedades importantes para medir y evaluar aspectos, dimensiones o componentes del fenómeno a estudiar.

2.6 Diseño de Investigación

El Diseño de la Investigación que aplicaremos será: ***Series cronológicas de un solo grupo***, donde a un único grupo se le administran varias pre-pruebas, después se le aplica el tratamiento experimental y finalmente varias post-pruebas. El diagrama del diseño sería:

$$G: O_1 O_2 O_3 \ X \ O_4 O_5 O_6$$

Donde:

G:	grupo único
O1, O2, O3:	pre pruebas
X:	variable independiente
O4, O5, O6:	post pruebas

El número de mediciones está sujeto a las necesidades específicas de la investigación.

$$\mathbf{X \rightarrow Y\ (y1, y2, y3)}$$

2.7 Cobertura de Investigación

2.7.1 Población

La población está conformada por todas las oficinas, divisiones, departamentos y talleres que utilizan los servicios informáticos; áreas en las cuales la seguridad de la información pueda ser vulnerada.

Oficina/Departamento	División/Taller	Total
Gestión Integrada	Gestión ambiental	01
	Gestión de la calidad	01
	Seguridad y salud	01
Logística	Contrataciones	01
	Almacenes	01
Estratégica	Evaluación y desarrollo	01
	Tecnologías de la información	01
Producción	Clientes particulares	02
	Mantenimiento y servicios	02
	Control de calidad	02
	Diseño y desarrollo	02
	Planeamiento y control	02
	Construcciones navales	01
	Mecánica naval	01
	Mecánica	01
	Tratamiento de superficies	02
	Maniobras	01
	Fabricaciones	01
TOTAL		24

Tabla N° 01: Áreas que utilizan servicios informáticos

2.7.2 Muestra

La muestra será la ***División de Tecnologías de la Información,*** ya que es el área donde se encuentran los servidores (correo, base de datos, archivos, etc.), sistemas de información, documentación y diferentes activos de gran importancia para la realización de las actividades de la Institución; la cual representa a la vez la división más vulnerable a sufrir algún ataque relacionado con la seguridad de la información.

2.7.3 Tipo de muestreo

Se va a utilizar un muestreo no probabilístico intencionado, con la finalidad de seleccionar como muestra a la DTI para la investigación.

2.8 Técnicas e Instrumentos de recolección de datos

2.8.1 Técnicas

Las técnicas que utilizaremos para la recoleccionar, conservar, analizar y transmitir los datos de los fenómenos sobre los cuales realizamos la investigación son las siguientes:

- **La observación:** Consiste en la percepción sistemática y dirigida a captar los aspectos más significativos de los objetos, hechos, realidades sociales y personas en el contexto donde se desarrollan normalmente.

- **La encuesta:** Es una técnica que al igual que la observación está destinada para recopilar los datos necesarios para realizar la investigación.

- **La entrevista:** Consiste en una conversación personal que el entrevistador establece con los sujetos investigados, con el propósito de obtener los datos necesarios para realizar la investigación.

2.8.2 Instrumentos

Los instrumentos facilitan a las técnicas el proceso de recolección de los datos. Los instrumentos a emplear en la investigación son los siguientes:

- Fichas
- Fotografía
- Cuaderno de notas
- Cuestionarios
- Checklist

2.9 Técnicas de procesamiento y análisis de datos

Para el procesamiento, análisis contrastación e interpretación de resultados de la investigación se aplicarán las técnicas estadísticas.

- ✓ **Medidas de tendencia central**
  Media aritmética

- ✓ **Medidas de dispersión**
  Desviación estándar

- ✓ **Presentación de los datos**
  Elaboración de cuadros estadísticos y gráficos

- ✓ **Pruebas de hipótesis**
  Prueba de normalidad: Para probar el supuesto de normalidad.

2.10 Limitaciones

En la presente investigación encontramos las siguientes limitaciones:

- ✓ El personal de la DTI disponen de un tiempo reducido para colaborar con la investigación, ya que tienen tareas asignadas diariamente.
- ✓ La DTI dispone solo del 10% de información relacionado a seguridad de la información, haciendo complicado la investigación.
- ✓ El acceso a los recursos y servicios informáticos se encuentran restringidos.

CAPITULO III

MARCO REFERENCIAL

3.1 Marco Teórico

3.1.1 Seguridad de la Información

La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. Esto es muy importante en el creciente ambiente interconectado de negocios. Como resultado de esta creciente interconectividad, la información expuesta a un mayor rango de amenazas y vulnerabilidades. La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene. La seguridad de la información se consigue implantando un conjunto adecuado de controles, que puedes ser políticas, prácticas, procedimiento, estructuras organizativas y funciones de software y hardware. Estos controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados donde sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y negocios de la organización [1].

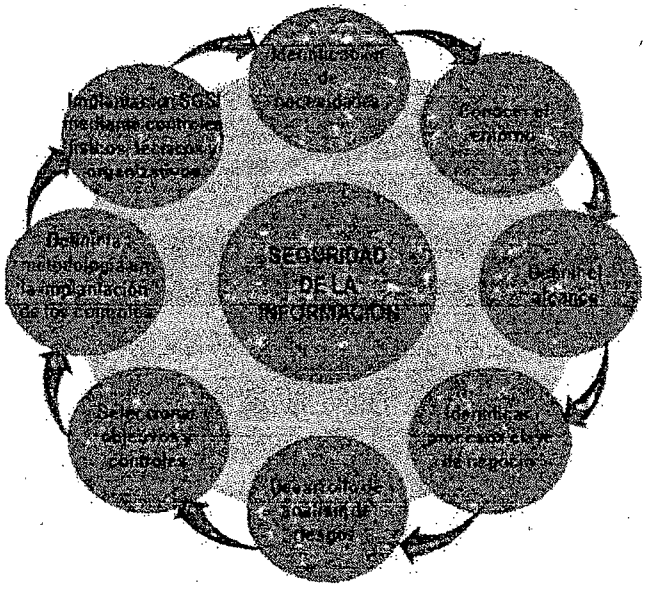


Figura N° 02: Proceso de Seguridad de la Información

La necesidad de mantener la integridad de la información y de proteger los activos de T.I, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de T.I. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de T.I para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad [2].

Definir la seguridad de la información es complejo, debido a la gran cantidad de factores que intervienen. Sin embargo es posible dar una aproximación a la definición y se puede decir que la seguridad es el conjunto de recursos (metodologías, documentos, programas y dispositivos físicos) encaminados a lograr que los recursos de cómputo disponibles en un ambiente dado, tengan acceso única y exclusivamente quienes tengan la autorización para hacerlo. La complejidad creciente y el alcance del uso de las computadoras en una organización ha propiciado que los sistemas de almacenamiento y divulgación de información se encuentren en manos de unas cuantas personas, las cuales al efectuar su trabajo y concentrarse mas que de nada en ello, no realizan controles adecuados en el uso de los mismos, es decir, en estos sistemas [3].

Para lograr un gobierno efectivo de seguridad de información, la gerencia debe establecer y mantener un marco para guiar el desarrollo y administración de un programa completo de seguridad de información que soporte los objetivos del negocio [4].

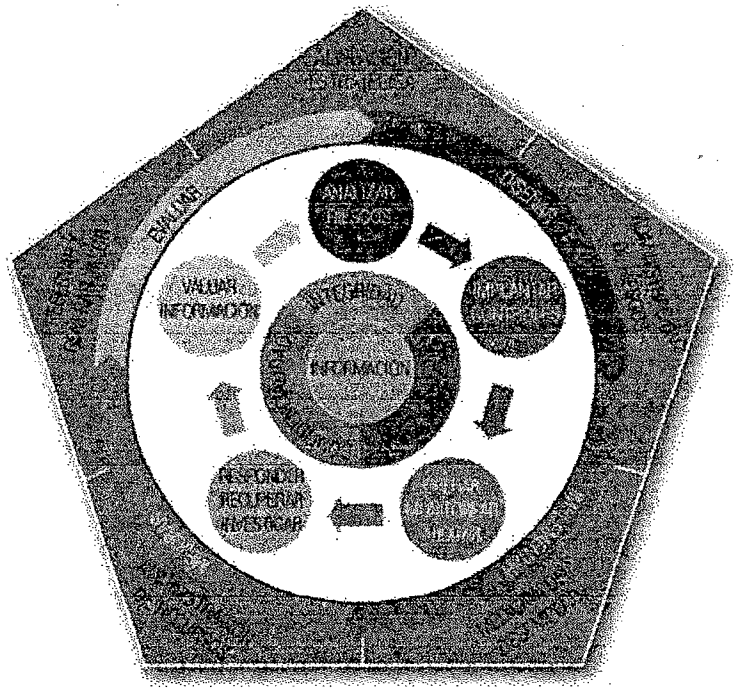


Figura Nº 03: Gobierno Corporativo de Seguridad de la Información

3.1.2 Seguridad y Acceso de la Información

En los procedimientos administrativos es recomendable la identificación previa del personal que va a ingresar a las áreas de cómputo, verificando si cuenta con la autorización correspondiente y registrándose el ingreso y salida al área. Las rutinas de control, permiten que los usuarios ingresen al sistema, previa identificación, mediante una palabra clave (password), la cual será única para cada uno de ellos; negando el acceso a las personas que no han sido definidos como usuarios del sistema. Las rutinas de control de acceso identificarán a los usuarios autorizados a usar determinados sistemas con su correspondiente nivel de acceso, el cual incluye la lectura o modificación en sus diferentes formas [5].

Toda información almacenada en medios magnéticos u ópticos debe contar con un documento donde se registre:

- Intensificación del archivo, especificándose si se trata de un archivo maestro, base de datos, archivo primario o archivo temporal.

- Identificación del sistema o aplicación que lo usa.
- Frecuencia del proceso.
- La longitud del registro del archivo (numero total de caracteres por registro).
- Los campos contenidos, cada uno con su nombre mnemotécnico, una explicación descriptiva, longitud y tipo de campo (alfanumérico, numérico, fecha, etc.).

3.1.3 Respaldo de Seguridad

La información almacenada en medios magnéticos u ópticos tendrán al menos una copia de respaldo en (diskettes o en otro medio de que disponga la Institución), debido a que el costo de recuperación de la información puede ser demasiado alto. La información almacenada debe ser verificada íntegramente, tanto el original como las copias (en caso de encontrarse empaquetada, desempaquetarla como verificación). Asimismo, debe verificarse que la información no esté contaminada con virus informático. Debe existir una copia de los archivos importantes que están concluidos, tanto en el órgano central como en uno de sus locales, como respaldo preventivo. Los archivos que son textos, hojas de cálculo, gráficos, etc.; mientras no se concluyan, será guardado en una sola copia por cada actualización para facilitar su almacenamiento. [6]

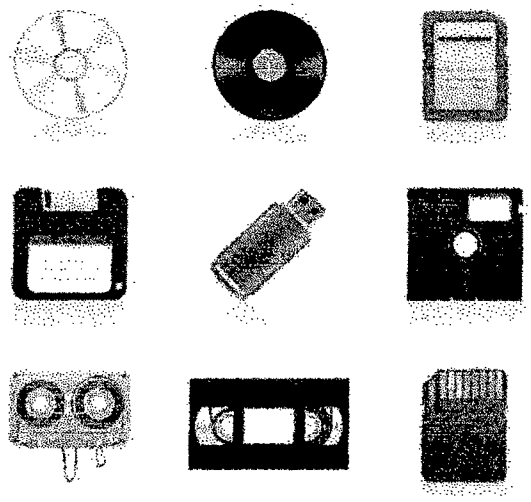


Figura N° 04: Medios de respaldo de información

3.1.4 Acciones de Prevención

Con relación a las áreas de trabajo y a las aplicaciones utilizadas:

- El área de cómputo, donde operan los servicios de información y sistemas interactivos orientados a internet, deben ser de acceso restringido, solo para personal autorizado.
- La información, servicios y procedimientos administrativos a proveer a la ciudadanía, deben administrarse por medios electrónicos con aplicaciones seguras.
- Debe incorporarse un sistema de seguridad antivirus, a los servidores que gestionan las bases de datos y las aplicaciones de los servicios a la ciudadanía.
- Se recomienda incluir una herramienta de detección de intrusos y control de accesos para proteger la información de carácter confidencial de la Institución.
- Disponer de copias completas de seguridad (backup) de la información base de datos y aplicativos, con herramientas de respaldo en línea que evite interrumpir los servicios de los servidores.
- Disponer de dispositivos de backup SCSI de tecnología actual, para un respaldo adecuado de los servidores.
- Resolver el problema de administración de cuentas y grupos para tener el absoluto control de quienes son las personas autorizadas y con derechos en los recursos de almacenamiento.
- Tener una adecuada alimentación eléctrica, que involucra el estado de los pozos a tierra, UPS, estabilizador, grupo electrógeno y redes de alimentación eléctrica independientes [7].

3.2 Marco Conceptual

3.2.1 Sistema de Gestión de Seguridad de la Información: El SGSI, es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información. Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.[1]

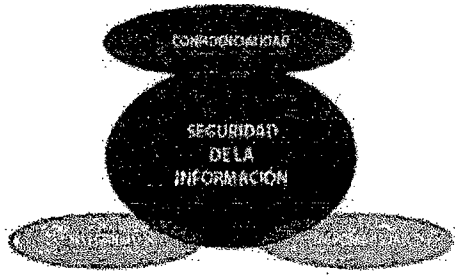


Figura N° 05: Características de la Seguridad de la Información

3.2.2 Confidencialidad: La confidencialidad se entiende en el ámbito de la seguridad informática, como la protección de datos y de información intercambiada entre un emisor y uno o más destinatarios frente a terceros. Esto debe hacerse independientemente de la seguridad del sistema de comunicación utilizado: de hecho, un asunto de gran interés es el problema de garantizar la confidencialidad de la comunicación utilizada cuando el sistema es inherentemente insegura (como Internet). En un sistema que garantice la confidencialidad, un tercero que entra en posesión de la información intercambiada entre el remitente y el destinatario no es capaz de extraer cualquier contenido inteligible.

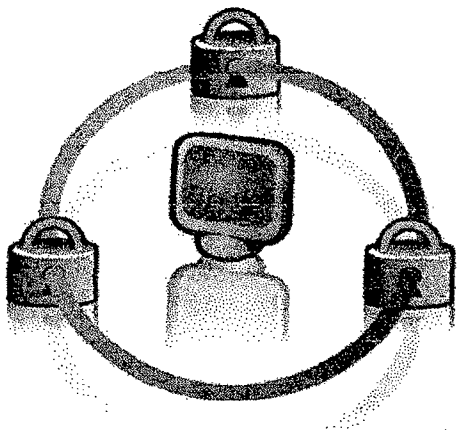


Figura N° 06: Confidencialidad de la Información

3.2.3 Disponibilidad: Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran. Este principio es particularmente importante en sistemas informáticos cuyo compromiso con el usuario es prestar servicio permanente.

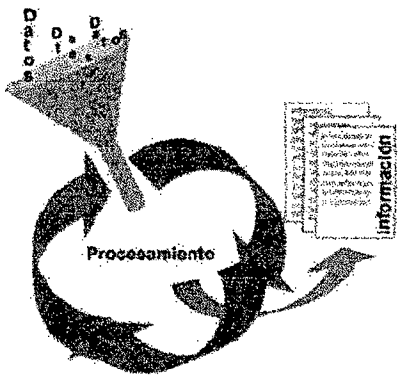


Figura N° 07: Disponibilidad de la Información

3.2.4 Integridad: Se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio es particularmente

importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios, computadoras y procesos comparten la misma información.

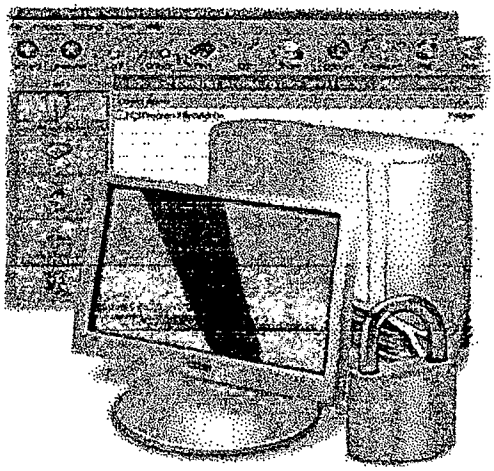


Figura N° 08: Integridad de la Información

3.2.5 Política de Seguridad Informática: Una política de seguridad informática es una forma de comunicarse con los usuarios y los gerentes. Establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización. No se trata de una descripción técnica de mecanismo de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es mas bien una descripción de lo que deseamos proteger y el porque de ello. Es a la vez un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general de los sistemas.

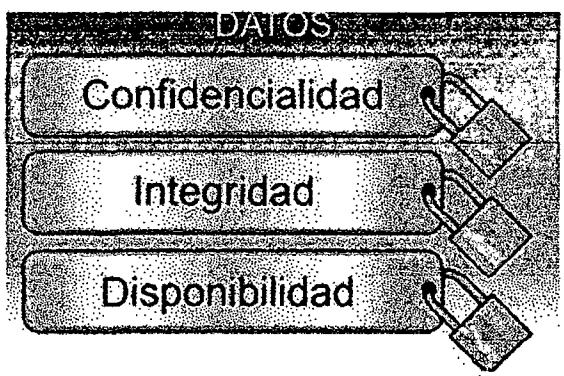


Figura N° 09: Política de Seguridad Informática

3.2.6 Plan de Contingencias: Es un procedimiento alternativo al orden normal de una Empresa, cuyo fin es permitir el normal funcionamiento de esta, aun cuando alguna de sus funciones se viese dañada por un accidente interno o externo. El plan de contingencia supone un avance a la hora de superar cualquier eventualidad que puedan ocasionar pérdidas y llegado el caso no solo materiales sino personales.

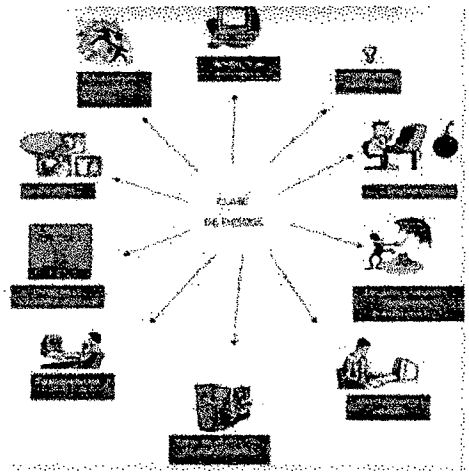


Figura N° 10: Plan de Contingencias

3.2.7 Procedimiento de Seguridad: Determina las acciones o tareas a realizar en el desempeño de un proceso relacionado con la seguridad y las personas o grupos responsables de su ejecución. Son, por tanto, la especificación de una serie de pasos en relación a la ejecución de un proceso o actividad que trata de cumplir con una norma o garantizar que en la ejecución de actividades se considerarán determinados aspectos de seguridad.

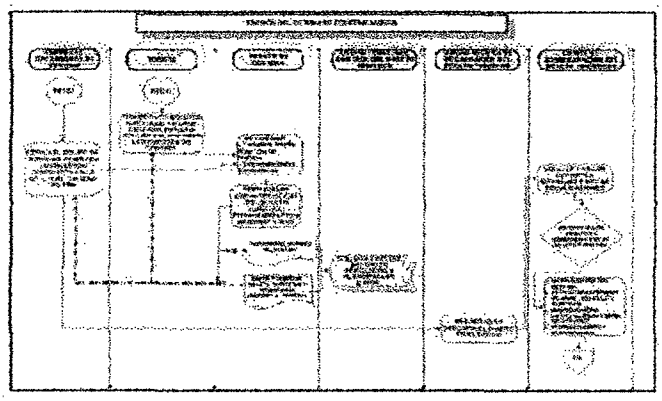


Figura N° 11: Procedimiento de Seguridad

3.2.8 ISO/IEC 27001: Es el estándar para la seguridad de la información, fue aprobado y publicado como estándar internacional en octubre de 2005 por la Organización Internacional de Estandarización y por la Comisión Electrotécnica Internacional. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido ciclo de Deming. Es consistente con las mejores prácticas descritas en ISO/IEC 17799 y tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica British Standars Institution (BSI).

Figura N° 12: ISO/IEC 27001

3.2.9 Activo Informático: Recurso del sistema de información o relacionado con éste, necesario para que la Organización funcione correctamente y alcance los objetivos propuestos.

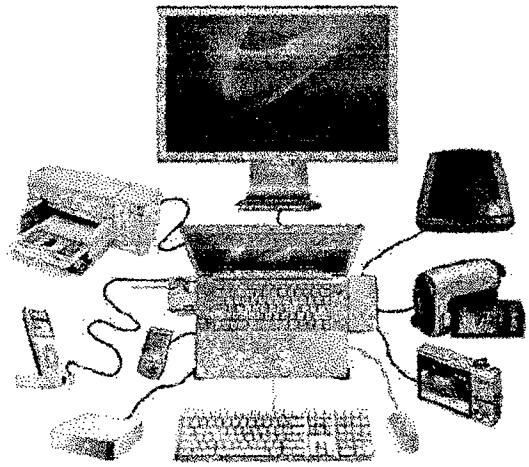


Figura N° 13: Activos Informáticos

3.2.10 NTP ISO/IEC 17799: Es la Norma Técnica Peruana publicada por la Oficina Nacional de Gobierno Electrónico, encargada de proporcionar el código de buenas prácticas para la gestión de la seguridad de la información en las Entidades del Estado.

Figura N° 14: Modelo de Seguridad de ISO/IEC 17799

3.2.11 Auditoría de Seguridad Informática: Abarca los conceptos de seguridad física y lógica. La seguridad física se refiere a la protección del hardware y los soportes de datos, así como la seguridad de los edificios e instalaciones que los albergan. El auditor informático debe contemplar situaciones de incendios, inundaciones, sabotajes, robos, catástrofes naturales, etc. Por su parte, la seguridad lógica se refiere a la seguridad en el uso de software, la protección de los datos, procesos y programas; así como la del acceso ordenado y autorizado de los usuarios a la información.

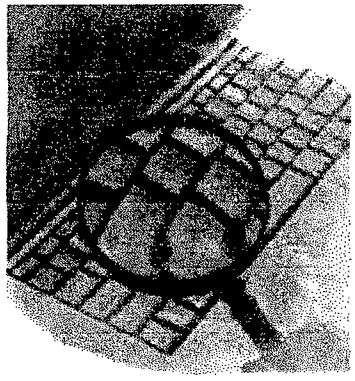


Figura N° 15: Auditoría de Seguridad Informática

3.2.12 Metodología PDCA: Es la metodología empleada para la implementación de un sistema gestión de seguridad de la información. Está compuesto por las siguientes etapas: planificar, hacer, verificar y actuar, donde cada etapa comprende una serie de actividades correspondientes.

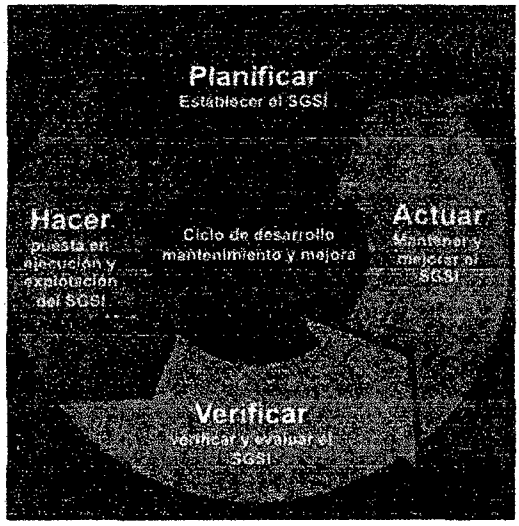


Figura N° 16: Fases de la Metodología PDCA

CAPITULO IV

RESULTADOS

4.1 Desarrollo del Sistema de Gestión de Seguridad

Para el desarrollo del SGSI es necesario tomar como base la norma ISO 27001 e ISO/IEC 17799. Estos estándares fueron elaborados para proveer un modelo para el establecimiento, implementación, operación, monitoreo, mantenimiento y mejora de un SGSI. La decisión por parte de la Institución de adoptar un SGSI es una decisión estratégica, ya que el SGSI está fuertemente ligado a las necesidades y objetivos de la misma.

Para el desarrollo del SGSI adoptaremos el modelo "Plan – Do – Check – Act", también conocido como **PDCA**, el cual es aplicado a toda la estructura de procesos del SGSI.

- **Plan (Establecer el SGSI):** Implica establecer la política del SGSI, sus objetivos, procesos y procedimientos relevantes para la administración de riesgos y mejoras para la seguridad de la información, con resultados acordes a las políticas y objetivos de toda la Organización.

- **Do (Implementar y operar el SGSI):** Representa la forma en que se debe operar e implementar las políticas, controles, procesos y procedimientos que se vayan a definir en la planificación del SGSI.

- **Check (Monitorizar y revisar el SGSI):** Analizar y medir donde sea aplicable, los procesos ejecutados con relación a la política del SGSI, evaluar objetivos, experiencias e informar los resultados a la administración para su revisión.

- **Act (Mantener y mejorar el SGSI):** Realizar las acciones preventivas y correctivas, basados en las auditorías internas y/o externas, revisiones del SGSI o cualquier otra información relevante para permitir la continua mejorar del sistema.

4.1.1 Plan (Establecer el SGSI)

El Sistema de Gestión de Seguridad de la Información a implementar estará conformado por 07 procesos: clasificación y control de activos, seguridad ligada al personal, seguridad física y del entorno, gestión de comunicaciones y operaciones, control de accesos, desarrollo y mantenimiento de sistemas, y gestión de continuidad del negocio.

Para conocer la actual situación en la que se encuentran estos procesos en la DTI se realizó una auditoría a cada proceso identificado, obteniendo los siguientes resultados:

a) Clasificación y Control de Activos

Para este proceso aplicamos la ***Guía de Observación N° 01 – Clasificación y Control de Activos (Anexo 01)***

- Los activos informáticos con los que cuenta la DTI son los siguientes:

N°	Activo	Descripción
01	Software	Se cuenta con software de ofimática, desarrollo, diseño, etc.
02	Hardware	Se cuenta con equipos de cómputo, impresión, fotocopiado, etc.
03	Servidores	Se cuenta con los servidores de correo, base de datos, archivos, impresión, etc.
04	Backup	Se cuenta con backup de todas las áreas almacenados en DVDs.
05	Documentación	Se cuenta con documentación de los procesos de desarrollo, soporte y seguridad.

Tabla N° 02: Activos informáticos de la DTI

- El software con que cuenta la DTI no se encuentra clasificado de acuerdo a su uso y al nivel de importancia para el área, teniendo en cuenta que todo el software es licenciado y original.

- El hardware con que cuenta la DTI se encuentra inventariado hasta el año 2009, en adelante no se ha realizado una actualización de los nuevos equipos informáticos adquiridos.

- Los servidores con que cuenta la DTI no se encuentran clasificados de acuerdo a su importancia para la Institución en una situación de contingencia.

- El backup con que cuenta la DTI se encuentra almacenada en un estante de madera por fecha de respaldo, pero no se encuentra clasificado de acuerdo a su importancia, ya que en este backup se encuentra información de los sistemas, correo, base de datos, etc. Información que es de gran importancia para la Institución.

- La documentación con que cuenta la DTI se encuentra archivada en estantes de madera pero no clasificada adecuadamente por ejemplo en documentación de usuarios (solicitudes, formatos, trámites, etc.) y sistemas (manuales, diagramas, formatos, listas de accesos, etc.).

- El control de los activos informáticos no se realiza como parte de las funciones del área, obviándose información de cómo se encuentran actualmente y cuales son las acciones a tomar para garantizarles una seguridad de la información adecuada.

b) Seguridad Ligada al Personal

Para este proceso aplicamos la ***Guía de Observación N° 02 – Seguridad Ligada al Personal (Anexo 02)***

- Cuando un personal ingresa a laborar a la DTI no se le hace firmar ningún acuerdo de confidencialidad, ya que por su

naturaleza el área procesa y almacena información confidencial y de gran importancia para la Institución.

- Cuando un personal ingresa a laborar al Sima Chimbote y según sus funciones hará uso de los servicios informáticos (correo, internet, sistemas, etc.), actualmente no se le brinda a nadie una pequeña capacitación relacionada a seguridad informática, concerniente al uso y cambio de las contraseñas de los sistemas, accesos a páginas web y acceso a información confidencial. Lo que implica que los usuarios de los servicios informáticos no cuentan con nociones de seguridad en la realización de sus funciones.

- Cuando se contrata personal externo (outsorcing) para realizar trabajos dentro de la DTI, no se le hace firmar ningún compromiso para proteger la confidencialidad e integridad de la información y a la vez en los contratos no existe ningún cláusula el cual garantice que la seguridad de la información de la Institución no se verá comprometida ni afectada con el cumplimiento de sus actividades.

c) Seguridad Física y del Entorno

Para este proceso aplicamos la ***Guía de Observación N° 03 – Seguridad Física y del Entorno (Anexo 03)***

- El acceso principal a la DTI es utilizado tanto para personal interno como externo (terceros), en los casos donde personal externo ingresan al área a realizar trabajos de mantenimiento de servidores o verificación de algún servicio informático. Actualmente hay dos 02 puertas de ingresos al área pero solamente su utiliza la principal, razón por la cual se puede visualizar fácilmente los trabajos que realizan los analistas de sistemas y documentación propia del área.

- Las puertas de ingreso a la DTI son de madera y no tienen ninguna protección adicional. Una vez que se retira todo el personal del área el último es el encargado de ponerle seguro, pero mensualmente 03 veces no se realiza esto por olvido. Quedando el área libre para el acceso de cualquier personal.

- El perímetro de la DTI no cuenta con dispositivos de seguridad como sensores o cámaras, los cuales se encarguen de alertar al personal de seguridad sobre posibles incidentes que puedan vulnerar la seguridad física del área.

- El control del ingreso a las instalaciones del Sima Chimbote es realizado por personal de seguridad (interna y externa), desde la garita de ingreso. En todo momento el personal de seguridad se encuentra distribuido en las diferentes zonas (almacén, talleres, muelle y oficinas de producción), pero actualmente no se realiza verificaciones en el transcurso de la noche de la DTI; con la finalidad de evitar que personal no autorizado intente ingresar con algún fin. Todo esto debido a que en meses de producción (Febrero – Abril y Agosto - Octubre), tanto personal interno como externo se quedan a laborar en turnos de noche y amanecida.

d) Gestión de Comunicaciones y Operaciones

Para este proceso aplicamos la ***Guía de Observación N° 04 – Gestión de Comunicaciones y Operaciones (Anexo 04)***

- En la DTI no existen procedimientos documentados para actividades del sistema asociados con el procesamiento de información y los recursos de comunicación, tales como procedimientos de encendido y apagado de la computadora, Backup, correo corporativo y seguridad. Los cuales se encarguen de brindar los conocimientos necesarios a los

usuarios de los diferentes servicios informáticos, relacionados con la manipulación de información.

- La DTI actualmente tiene en operación 16 sistemas informáticos:

    - Sistema Comercial (visual)
    - Sistema de Producción (visual)
    - Sistema Logístico (dos)
    - Sistema de Tesorería (dos)
    - Sistema de Contabilidad General (dos)
    - Sistema de Contabilidad de Costos (dos)
    - Sistema de Control Patrimonial (dos)
    - Sistema de Personal (dos)
    - Sistema de Mantenimiento (dos)
    - Sistema de Parqueadero (visual)
    - Sistema de Requerimientos de Oficina (visual)
    - Sistema de Control de Pañoles (dos)
    - Sistema de Guías de Remisión (dos)
    - Sistema de Calidad (visual)
    - Sistema de backup (visual)
    - Sistema de Registro de Llamadas (visual)

Cada sistema es asignado de acuerdo al área y al cumplimiento de sus funciones a los usuarios con acceso permitido. Actualmente no existe un procedimiento para comunicar los incidentes que se producen cuando se está manipulando los sistemas informáticos. Los errores que se producen frecuentemente son bloqueo del sistema por saturación del servidor, desbordamiento por ingreso de parámetros no permitidos, sincronización inadecuada entre los servidores de base de datos. Problemas que causan muchas veces pérdida de información y que no son comunicados oportunamente a los analistas de sistemas.

- Los cambios en los sistemas informáticos se realizan a propuesta de los analistas de sistemas o requerimiento de los usuarios. Actualmente estos cambios son realizados pero en el 50% de los casos no son comunicados oportunamente a los usuarios implicados en estas transacciones, lo que ha provocado pérdida de información y bloqueo temporal de las aplicaciones; siendo necesarios la intervención de los analistas de sistemas y personal de soporte técnico.

- Los sistemas informáticos actualmente están implementados en Fox Pro 2.6 (57%) y Power Builder 11.5 (43%). El mayor porcentaje de sistemas están implementados en versión dos, el cual emplea el motor de base de datos DBase IV, mientras que los sistemas visuales emplean el motor de datos SQL Server 2000. Estos sistemas en su mayoría comparten los mismos datos para realizar ciertas transacciones, lo que ocasiona que la información no se encuentre sincronizado en las diferentes estaciones de trabajo; provocando así un inadecuado procesamiento de la información, para lo cual es necesario la intervención de los analistas de sistemas para la sincronización de la información.

- Para la puesta en marcha de un sistema informático nuevo o modificado, no se están tomando en cuenta los siguientes criterios:

    - Garantía de que operacionalmente cumplirá con los objetivos para los cuales fue implementado
    - No afectará el funcionamiento del resto de los sistemas
    - Mantendrá en todo momento una seguridad acorde al nivel de información a procesar
    - Cuenta con los controles necesarios para la recuperación en caso de errores

- Cuenta con los mecanismos necesarios para su baja en caso genere repercusión negativa frente al resto de los sistemas.

- Cada usuario tiene asignado un rol y en base a ello se le instala una cantidad de programas para el cumplimiento de sus funciones. Actualmente el personal de Soporte Técnico no realiza revisiones periódicas para comprobar si todos los programas autorizados inicialmente coinciden, lo que ha ocasionado encontrar en 01 usuario de la DTI programas no licenciados ni autorizados (desarrollo y diseño); lo cual pone a la Institución en riesgo de recibir una sanción por el uso de software no licenciado y a la vez producir estos programas daños en la computadora que es utilizada para el desarrollo y mantenimiento de sistemas DOS.

- Actualmente los puertos USB de todos los usuarios se encuentran deshabilitados, a excepción de la computadora del Administrador. La cual apoya a los diferentes usuarios a pasar información desde los dispositivos USB a sus computadoras a través de la red. Al no conocer la naturaleza de estos dispositivos externos es necesario analizarlo con el software antivirus en el modo avanzando, tarea que no siempre se realiza por tema de tiempo y que en 01 ocasión originó que troyanos infecten la red, provocando bloqueos y avisos de infección en las computadoras de la DTI y de las diferentes áreas.

- La infraestructura de la red actualmente no usa tecnología adecuada, lo cual hace carecer la implementación de controles y medidas para proteger y salvaguardar la información que se transmite entre los diferentes usuarios. Por ello se ha formulado la modernización de las tecnologías de la información (switch y servidores), tecnologías que cuenta con sistemas de encriptación y de detección de intrusos en toda la red.

- En la DTI actualmente se emplean medios removibles (CD, DVD, disquete) para el copiado o traslado de información (códigos, formatos, registros). Dichos medios una vez utilizados se dejan en lugares de fácil acceso o se botan a los tachos. No se toma en cuenta la importancia de la información que puede contener si es que es utilizado por usuarios de otras áreas, quienes llegan a solicitar apoyo de algún servicio informático.

e) Control de Accesos

Para este proceso aplicamos la ***Guía de Observación N° 05 – Control de Accesos (Anexo 05)***

- Actualmente la baja de un usuario (acceso a los sistemas informáticos, correo, PC) se realiza luego de haber transcurrido más de 07 días de la renuncia o despido del trabajador (con acceso a servicios informáticos). Lo que ha generado que en 01 oportunidad se utilicen los accesos de un usuario que ya no laboraba, para manipular sistemas de información y correo electrónico, siendo necesario la intervención del personal de Soporte Técnico para restringir el acceso.

- Actualmente la DTI no maneja un registro de altas y bajas, el cual permita tener un registro actualizado de los usuarios que cuentan o no con acceso a los servicios informáticos, criterio de gran importancia cuando se realizan auditorías de seguridad informática.

- Actualmente la DTI no maneja un registro de accesos a los servicios informáticos por cada usuario (bitácora), en el cual se visualicen los accesos iniciales y los que se den durante su permanencia en la Institución. Situación que no permite realizar verificaciones periódicas sobre los accesos de los usuarios para verificar si estos siguen teniendo los privilegios iniciales y poder

verificar si se han realizado cambios que afecten la confidencialidad de la información.

- La DTI actualmente no tiene definido niveles de acceso en relación a las áreas de la Institución y la información que éstas manipulan. Lo cual implica que para dar acceso a un nuevo usuario solamente se realiza en función al puesto de trabajo.

- Actualmente los accesos de un usuario son solicitados por el Jefe de Oficina solicitante. Luego son aprobados por el Jefe de la Oficina Estratégica y derivadas para su acción al Jefe de la DTI. Situación que ha generado que más de 01 usuario tenga accesos a sistemas que no se relacionan con sus funciones (Oficina de Logística). En este proceso la DTI no está realizando ninguna observación ya que para brindar un acceso debe existir una clasificación de las áreas y usuarios.

- Las contraseñas de acceso a la computadora y sistemas informáticos no cumplen con requisitos de seguridad, pudiéndose verificar que el 70% de usuarios usan contraseñas muy sencillas (números de 1 al 6, nombre de usuario, datos personales, etc.), lo cual ha provocado que en 03 ocasiones se ingrese a sistemas desde áreas no autorizadas, esto debido a que actualmente los sistemas informáticos no implementan políticas de seguridad que permitan que en caso de creación o modificación de las contraseñas estas se generen de manera segura y confiable.

- Una vez creada las contraseñas de acceso de un determinado usuario, se ha podido comprobar que en 03 ocasiones éstas se han escrito en los memorándum (documento interno de autorización). Luego estos documentos se archivaron de manera normal, con libre acceso a cualquier personal del área.

f) Adquisición, Desarrollo y Mantenimiento de Sistemas

Para este proceso aplicamos la ***Guía de Observación N° 06 – Adquisición, Desarrollo y Mantenimiento de Sistemas (Anexo 06)***

- Todos los sistemas actualmente realizan solo validación de campos vacios, obviándose las validaciones para evaluar valores fuera de rango, caracteres inválidos, datos incompletos, datos que exceden los rangos establecidos, datos inconsistentes, etc.; los cuales provocan en todo momento cierres inesperados del sistema y por lo tanto la pérdida de los datos de las operaciones (registro de facturas, cálculo de planillas, conciliaciones bancarias, emisión de vales de materiales, etc.).

- Solamente el 30% de las transacciones (procedimientos almacenados, desencadenadores, etc.) implementan dentro de su estructura rutinas de recuperación de datos (excepciones). Provocando en muchas ocasiones que se realice el procesamiento de una transacción incompleta, debido a la falta de parámetros o el ingreso de datos inconsistentes.

- Actualmente no existe ningún registro de fallas de los sistemas, los cuales involucren la pérdida de datos de gran importancia. Esto no ha permitido conocer por cada sistema cuales son las fallas que se generan al momento de su ejecución; para de esta manera evitar la pérdida de datos y el inadecuado procesamiento de los sistemas.

- Cuando se realiza el desarrollo o modificación de un sistema, en la fase de pruebas se realizan todas las revisiones necesarias para garantizar que el sistema obtiene como resultado la información que requieren las áreas usuarias; una vez aprobado esto se pone en operación el sistema. Pero una vez finalizado esto, ya no se realizan validaciones periódicas sobre todo en los sistemas que procesan información de importancia

(contabilidad, producción, comercial), con la finalidad de seguir garantizando la obtención de la información requerida. Lo cual ha provocado el reclamo de los usuarios en los reportes que procesan ciertos sistemas.

- Las modificaciones que involucran varias funcionalidades de los sistemas se realizan localmente en la computadora del Analista de Sistemas (previo memorándum del área solicitante), para que una vez finalizado y probado se pase a un ambiente de operación (servidor). Pero el 80% de las modificaciones pequeñas (el usuario se acerca personalmente) se realizan directamente del servidor, lo cual ha provocado en más de 02 ocasiones el bloqueo del sistema involucrado y la pérdida de los datos que se encontraban procesando por los diferentes usuarios del sistema.

- Debido a que la DTI cuenta con 16 Sistemas de Información, se le asigna a cada Analista de Sistemas una cantidad de sistemas para que se encuentren bajo su responsabilidad. Actualmente el código fuente se encuentra accesible a todos los Analistas, lo cual ha generado en 02 oportunidades que personal nuevo realice cambios sobre sistemas que no se encuentran bajo su responsabilidad. Provocando así la paralización del sistema, debiendo intervenir el Analista responsable para restablecer el servicio a los usuarios.

- Las modificaciones que involucran varias funcionalidades son solicitadas por medio de memorándum. Una vez recepcionado esto, el Analista responsable del sistema empieza a realizar los cambios solicitados. Obviándose así la evaluación de los impactos que pudieran provocar dichos cambios con relación a la información y al resto de los sistemas en operación. Esto ha generado en 01 oportunidad la pérdida de datos, ya que las modificaciones realizadas eran incompatibles con la estructura de la base de datos.

g) **Gestión de Continuidad del Negocio**

Para este proceso aplicamos la ***Guía de Observación N° 07 – Gestión de Continuidad del Negocio (Anexo 07)***

- Actualmente existe un documento de plan de contingencias 2009, el cual presenta las siguientes observaciones:

  ✓ No se identifican todos los riesgos a los que está expuesto la DTI en caso de producirse algún desastre natural o artificial.

  ✓ No se especifica la frecuencia y probabilidad de ocurrencia por cada riesgo identificado.

  ✓ No se especifica las acciones que se están realizando para mitigar los riesgos potenciales a los cuales se está expuesto cada día.

  ✓ No se especifican las acciones a seguir para la restauración de los sistemas de información en caso de producirse alguna contingencia.

  ✓ En los equipos de trabajo existen integrantes que actualmente no laboran en la Institución.

  ✓ No se encuentran definidas las actividades generales que debe realizar el personal operativo de evaluación.

  ✓ El personal no tiene claro conocimiento de las acciones que tiene que realizar durante un desastre, situación que provocaría mayores daños con respecto a los activos informáticos y el personal del área.

  ✓ No existe un cronograma de entrenamiento y simulacros donde participe todo el personal involucrado, de acuerdo

a los grupos definidos; con la finalidad de estar preparados frente a cualquier contingencia.

4.1.2 Do (Implementar y operar el SGSI)

Una vez identificado todos los problemas en la etapa anterior y en cada uno de los procesos, ahora definiremos las acciones y actividades necesarias para la implementación del SGSI por cada proceso.

a) Clasificación y Control de Activos

- **Clasificación de Software**

  La clasificación del software se realizará en base al uso e importancia, donde el total estará representado por el producto de ambos criterios.

  - ✓ **1:** Software usado frecuentemente; poca importancia
  - ✓ **2:** Software usado regularmente; mediana importancia
  - ✓ **3:** Software usado siempre; gran importancia

SOFTWARE LICENCIADO DE LA DTI					
SISTEMAS OPERATIVOS	**VERSION**	**CANTIDAD**	***USO***	***IMPORTANCIA***	***TOTAL***
Windows 95	95	1	1	1	1
Windows 98	98	12	1	1	1
Windows XP Profesional	2002	143	3	3	9
Windows Vista Bussines	2008	38	1	1	1
SISTEMAS OPERATIVOS SERVIDORES					
Windows Server Enterprise	2003	2	3	3	9
Windows Server Enterprise	2005	1	3	3	9
OFIMATICA					
Office Xp Standard	2002	2	1	1	1
Office Xp Profesional	2002	1	1	1	1
Office Profesional	2003	4	1	1	1
Office Standard	2003	32	2	3	6
Office Standard	2007	55	2	3	6
Office Profesional	2007	17	2	3	6
Microsoft Visio Pro	2007	1	1	1	1
Microsoft Project Standard	2000	2	1	1	1
Microsoft Project Profesional	2003	4	1	1	1
Microsoft Project Standard	2007	14	2	3	6
Microsoft Project Profesional	2007	3	1	1	1
SOFTWARE ANTIVIRUS					

Eset Smart Security Business	3	55	3	3	9
Kaspersky Server	6	2	2	2	4
BASE DATOS					
SQL SERVER	2005	1	3	3	9
Oracle Standard 7.3.4	7.3.4	1	1	2	2
SOFTWARE DE DESARROLLO					
MS FoxPro for dos	2.6	1	3	3	9
Power Builder Enterprise 11.1	11.1	1	3	3	9
Visual FoxPro Pro 8.0	8	1	1	1	1
IbExpert 2.0	2	1	1	1	1
Delphi Enterprise 7.0	7	1	1	1	1
SOFTWARE DE DISEÑO					
Intellicad Premium	2001	8	2	2	4
Autocad 2000I	2000	2	2	2	4
Autocad LT 2002	2002	3	2	1	2
Autocad LT 2004	2004	10	2	1	2
Autocad 2004	2004	1	2	1	2
Autocad LT 2005	2005	6	2	1	2
Autocad LT 2006	2006	7	2	1	2
Autocad LT 2007	2007	1	2	1	2
Autocad LT 2009	2009	2	3	3	9
AutoShip Pro	9.0.2	1	3	3	9
AutoHydro	6.1	1	2	2	4
AutoPower	3	1	2	2	4
AutoStructure	3.1	1	2	2	4
AutoPlate	9.2	1	2	2	4
Producction Manager (Autoship)	3.1	1	2	2	4
Lantek 2000 (software de corte)	2000	1	1	1	1
Algor Profesional Static/LM	23	1	1	1	1
Algor Linear Dynamic Analysis	23	1	1	1	1
Orcad 3D	1	1	1	1	1
Flamingo	2	1	1	1	1
Penguin	1	1	1	1	1
Bongo	1	1	1	1	1
Solid Edge Classic	1	1	2	2	4
OTROS					
Presupuestos S10 Ed. Empresarial	10	2	3	3	9
Power Translator Pro 7.0	7	3	2	1	2
Wincard	2000	1	1	1	1

Tabla N° 03: Clasificación de Software

- **Clasificación de Hardware**

  Para tener una mejor clasificación e inventario del hardware se utilizará la siguiente estructura:

		EQUIPO COMPUTACIONAL				MONITOR		OPERADOR/USUARIO		
C.C	USUARIO	C. ACTUAL1	TEC	DESCRIPCION	GHZ	C. ACTUAL2	MARCA	PR	CARGO	NOMBRE

Tabla Nº 04: Clasificación e Inventario de Hardware

Donde:

C.C, representa el centro de costo del hardware

Usuario, descripción del usuario

C. actual1, código actual del equipo

Tec, tecnología utilizada

Descripción, descripción de las características del hardware

Ghz, cantidad de ghz del hardware

C. actual2, código actual del monitor

Marca, descripción de la marca del monitor

PR, código de portaretrato del usuario

Cargo, descripción del cargo que desempeña el usuario

Nombre, nombre del usuario que utiliza el hardware

Con este nuevo formato se ha realizado el inventario de todo el hardware de la DTI y del resto de divisiones de la Institución.

- **Clasificación de Servidores**

La clasificación del servidor se realizará en base a su uso e importancia para la Institución, de igual manera el total está representado por el producto de ambos criterios:

- ✓ **1:** Usado frecuentemente; regular importancia
- ✓ **2:** Usado regularmente; mediana importancia
- ✓ **3:** Usado siempre; gran importancia

DESCRIPCIÓN	USO	IMPORTANCIA	TOTAL
Contingencias	2	2	4
Base de Datos	3	3	9
Archivos	3	3	9
Correo	3	3	9
Directorio Activo	2	2	4
Asterisk	2	2	4

Tabla N° 05: Clasificación de Servidores

- **Clasificación de Backup**

El backup diario actualmente se almacena en DVD's, y el último día de la semana se copia toda esta información a un disco duro externo (1 TB) como medida de contingencia. La clasificación a realizarse de ahora en adelante es la siguiente (el criterio será el mismo empleado en la clasificación de los servidores):

BACKUP	USO	IMPORTANCIA	TOTAL
Base de datos	3	3	9
Software	3	3	9
Correo	3	3	9
Archivos usuarios	3	3	9
Sistemas	3	3	9

Tabla N° 06: Clasificación de Backup

- **Clasificación de Documentos**

  La clasificación de los documentos archivados en la DTI se realizará de la siguiente manera (el criterio será el mismo empleado en la clasificación de backup):

DOCUMENTACIÓN	USO	IMPORTANCIA	TOTAL
Memorándum de accesos	2	3	**6**
Formatos de usuarios	3	2	**6**
Documentación de sistemas	3	3	**9**
Documentación de software	2	2	**4**
Memorándum internos	2	1	**2**

Tabla N° 07: Clasificación de Documentos

b) Seguridad Ligada al Personal

- **Acuerdo de Confidencialidad (Interno)**

  Encontrando la necesidad de contar con un documento en el cual todo el personal de la DTI (Analista de Sistemas, Coordinador de Soporte Informático, Analista de Seguridad de la Información y Jefe de la DTI), responsable de manipular información confidencial se comprometa en todo momento a mantener en reserva toda información "confidencial" perteneciente a la Institución, se ha elaborado el **Acuerdo de Confidencialidad para Personal Interno *(Anexo 08)***

- **Acuerdo de Confidencialidad (Externo)**

  Debido a que la DTI trabaja con personal externo es necesario tener el compromiso que no se divulgará y/o manipulará ningún tipo de información sin autorización y conocimiento del Analista de Seguridad y Jefe de la DTI. Por ello se ha elaborado el **Acuerdo de Confidencialidad para Personal Externo *(Anexo 09)***. Adicionalmente se realizarán supervisiones mensuales para hacer cumplir esta disposición.

- **Capacitación al Personal Nuevo**

  Se logró coordinar con la Oficina de Personal para que todo personal nuevo sea enviado antes de empezar sus funciones a la DTI, donde el Analista de Seguridad le brindará una pequeña capacitación en nociones básicas de seguridad de la información en base a los servicios informáticos que manipulará para el desarrollo de sus funciones en su área respectiva. Para evidenciar esta actividad se ha elaborado el **Formato de Capacitación en Seguridad de la Información** ***(Anexo 10)***. Adicional a esto se programará periódicamente capacitaciones a las divisiones para mantener a los usuarios actualizados en temas de seguridad de la información, lo cual será supervisado mensualmente por el Jefe de la DTIC.

c) Seguridad Física y del Entorno

- **Ingreso de Personal Externo a la DTIC**

  En la DTI se ha dispuesto que todo personal externo deba ingresar por la segunda puerta y no por la principal. En todo momento estará acompañado de un personal de Soporte Técnico hasta la finalización de las actividades programadas, adicionalmente se ha elaborado el **Registro de Ingreso de Personal Externo** ***(Anexo 11)***, especificándose detalladamente los datos de la persona y el motivo de la visita. Este registro será supervisado mensualmente por el Jefe de la DTI.

- **Seguridad Física de la DTI**

  Frente a esta situación se ha propuesto al Jefe de la Oficina Estratégica, considerar un presupuesto para la adquisición de cámaras de vigilancia y sistema de cierre automático de la puerta de ingreso a las instalaciones de la DTI. Con la finalidad de establecer una seguridad física adecuada a los activos informáticos almacenados interiormente.

- **Vigilancia de la DTI**

  Se ha coordinado con vigilancia para que en todo momento se resguarde las instalaciones de la DTI; sobre todo en meses de producción (Agosto – Noviembre y Enero – Abril) que es donde en las instalaciones del Sima Chimbote laboran una gran cantidad de contratistas; quienes de desplazan por diferentes oficinas y talleres hasta altas hora de la noche.

  Las incidencias ocurridas serán reportadas de inmediato al Jefe de Oficina; quién a la vez le comunicará al Jefe de la DTI para que se realicen las coordinaciones respectivas e investigar lo ocurrido. Este incidente se registrará en el **Registro de Incidentes en horario anormal** (***Anexo 12***).

d) Gestión de Comunicaciones y Operaciones

- **Documentación de Procesos Informáticos Operativos**

  Con la finalidad de facilitar a los usuarios la realización de sus actividades, se documentarán y publicarán los siguientes procesos a cargo del Coordinador de Soporte Informático.

  - ✓ Backup
  - ✓ Correo electrónico
  - ✓ Acceso internet
  - ✓ Uso de equipos de cómputo

  A la vez se programará una capacitación periódica por parte de la DTI a todas las áreas del Sima Chimbote, empleando para ello el **Registro de Capacitación de Procesos Informáticos Operativos** ***(Anexo 13)***.

- **Gestión de Comunicación**

  La DTI ha establecido que cuando se produzca cualquier incidente relacionado a los procesos del área, se realicen las siguientes acciones:

- ✓ El usuario reportará el incidente al Jefe de la DTI con copia a toda el área, vía correo electrónico.

- ✓ El Coordinador de Soporte Informático asignará a un Técnico para que brinde el apoyo correspondiente al usuario y evalúe el incidente.

- ✓ Una vez solucionado el incidente el Técnico reportará esta información al Coordinador de Soporte Informático, Analista de Seguridad de la Información y Jefe de la DTI.

- ✓ El Analista de Seguridad de la Información registrará el incidente en el **Registro de Incidentes de Seguridad de la Información** (***Anexo 14***). A la vez evaluará el incidente y junto al Coordinador de Soporte Informático solucionarán el incidente para casos futuros.

- ✓ El Jefe de la DTI comunicará vía correo electrónico al usuario que el incidente se encuentra identificado y solucionado.

- o **Gestión de Cambios**

  La DTI ha establecido comunicar vía correo electrónico a todos los usuarios de los servicios informáticos, las siguientes actividades:

  - ✓ Cambios en los sistemas informáticos (a solicitud de los usuarios o a propuesta de la DTI).

  - ✓ Mantenimiento de los servidores (base de datos, archivos, etc.).

  - ✓ Mantenimiento de algún sistema informático.

  - ✓ Incidentes con algún servicio informático

Todo ello con la finalidad de que los usuarios estén informados y eviten la pérdida de información o algún incidente relacionado a los servicios informáticos brindados por la DTI.

- **Protección contra Software Malicioso**

  La DTI protege la información de la Institución de cualquier software malicioso a través de las siguientes acciones:

  - ✓ Todo el software (diseño, editores, desarrollo, etc.) es licenciado y se actualizan a través de upgrade. Cumpliendo de esta manera con las normas relacionadas al uso de software licenciado en las Entidades del Estado y garantizando la protección contra cualquier software malicioso.

  - ✓ Ningún usuario tiene el privilegio de instalar software; a excepción del área de Soporte Técnico. Esto con la finalidad de evitar que se instalen software no licenciados, software no relacionados a sus actividades, software que consuman recursos innecesarios o software maliciosos con intenciones de infectar el equipo y la red de la Institución.

  - ✓ Revisiones trimestrales para la verificación del software instalado en los equipos de cómputo de los usuarios; esto con la finalidad de comprobar que solamente software licenciado se encuentran siendo usado por los usuarios.

  - ✓ Cuando se adquiere o licita algún software, este pasa por un periodo de evaluación en base a las especificaciones técnicas; esto con la finalidad de que se garantice un eficiente uso del software, no se reduzca la capacidad de los equipos y no produzca alguna infección en la red.

- **Gestión de Respaldo y Recuperación**

  El respaldo y recuperación de la información es un proceso de gran importancia para la DTI, por que se han establecido las siguientes acciones:

  - ✓ El personal de Soporte Técnico realiza un Backup diario de los servidores (base de datos, correo) y de los archivos de los usuarios (realizados a través del sistema de Backup).
  - ✓ El personal de Soporte Técnico realiza un Backup semanal (día sábado) donde se recopila el Backup diario de la semana.
  - ✓ Esta información se almacena en 02 discos duros externos, de los cuales una copia se guarda en un estante de la DTI y la otra copia en las instalaciones de Sima Metal Mecánica (ubicado por Sider Perú).
  - ✓ Para ello se emplea el **Registro de Backup Semanal** (***Anexo 15***), formato supervisado semanalmente por el Jefe de la DTI.
  - ✓ En caso de que algún usuario desee recuperar alguna información y haya realizado su Backup respectivo, comunicará vía correo al Jefe de la DTI con copia al personal de Soporte Técnico, para que se realice un respaldo de la información solicitada.

- **Gestión de Seguridad en Redes**

  La seguridad de la red de la Institución se protege de la siguiente manera:

  - ✓ Implementación de Firewall en el router principal (filtro de paquetes), creándose de esta manera una capa de

aislamiento entre la red interna y externa; con la finalidad de que el firewall filtre todos los paquetes entrantes y salientes a través de las direcciones IP/TCP de origen y destino.

- ✓ Implementación de VPN (Red Privada Virtual) para brindar una comunicación segura entre los usuarios y la red de internet. Esta tecnología encripta mediante algoritmos muy complejos toda la información que sale desde las estaciones de red. Brindando una garantía en la seguridad informática de la red institucional.

- ✓ Se ha propuesto y expuesto al Jefe de la Oficina Estratégica la compra de switch de última generación, quien implementa tecnología para encriptar de manera eficiente toda la información de la red y evitar todo tipo de ataques externos. Modernizando así los equipos de comunicaciones.

- ✓ Se está evaluando la adquisición de software para monitorear redes (GFI LANguard, ISS Internet Scanner, Tripwire, etc.); Con la finalidad de administrar eficientemente la red institucional y evitar ataques contra alguna vulnerabilidad interna.

- ✓ Se ha coordinado con Vigilancia que informe cualquier ingreso de equipos de cómputo (laptop) de personal externo (contratistas), ya que por la naturaleza de la Institución el ingreso de estos equipos es muy frecuente, debido a que se comparte información de planos, diseños, presupuestos, etc. Luego el personal de Soporte Técnico se encarga de brindar el apoyo correspondiente, supervisado en todo momento por el Analista de Seguridad de la Información para verificar que la red

interna no sufra ninguna exposición y se brinde accesos innecesarios.

- **Gestión de Sistemas Informáticos**

  Con la finalidad de brindar una operatividad adecuada a los Sistemas Informáticos, se han establecido las siguientes acciones:

  - ✓ Implementar una rutina en Java, cuya función sea sincronizar las bases de datos de DBase y SQL Server por cada vez que se manipulen los procedimientos que trabajan con ambos sistemas gestores de base de datos. Este es un problema que ocasiona la utilización de tiempo extra en solucionar los problemas de pérdida o sincronización de la información.

  - ✓ Para la puesta en marcha de un sistema (nuevo o por mantenimiento) se coordinará entre el Analista de Sistemas y Seguridad de la Información para que se garantice lo siguiente:

    - Operacionalmente cumple con todos los objetivos para cuales fue creado o modificado, esto será validado por el Analista de Sistemas y usuarios.

    - No afecta el funcionamiento del resto de los sistemas, esto debido a que más del 50% de los sistemas comparten procedimientos, tablas, funciones, etc. Validado por el Analista de Sistemas y usuarios.

    - La seguridad de la información tendrá el mismo nivel al del resto de los sistemas operativos. Validado por el Analista de Seguridad de la Información.

- Implementa controles adecuados en caso de presentarse errores en tiempo de ejecución, quienes permitan recuperar la información de manera adecuada. Validado por el Analista de Sistemas y Seguridad de la Información.

- Todas estas acciones serán reportadas al Jefe de la DTI para su respectiva aprobación y supervisión.

o **Gestión de Medios de Almacenamiento**

La DTI utiliza diferentes medios para el almacenamiento y desplazamiento de información entre el personal del área. Para establecer una seguridad adecuada se ha establecido las siguientes acciones:

✓ A excepción de Soporte Técnico, todos los usuarios tienen bloqueado los puertos USB, disquetera y lectora CD/DVD. Para garantizar esta política el Analista de Seguridad de la información realizará revisiones mensuales en las áreas críticas (Contabilidad, Tesorería, Remuneraciones, Evaluación y Control). Comunicando en todo momento al Jefe de la DTI y Coordinador de Soporte Informático sobre cualquier incidente.

✓ Todo usuario que desee copiar información desde un dispositivo USB (memoria, cámara, filmadora, disco duro externo, mp3, etc.) a su equipo de cómputo o viceversa deberá recurrir al área de Soporte Técnico para que le brinden el apoyo correspondiente, debiendo realizar lo siguiente:

- Analizar el dispositivo USB en modo avanzado (ESET NOD 32), hasta completar todas las

revisiones correspondientes y comprobar que no existe ninguna infección del dispositivo.

- Revisar que los archivos a copiar no tengan extensiones .exe, .inf, .bat, etc. (entrada). De ser así copiar solamente los archivos necesarios en la Carpeta Compartida de red o directamente en el directorio del usuario.

- Usar el **Registro de Ingreso y/o Salida de Información** (***Anexo 16***). Documento supervisado mensualmente por el Analista de Seguridad de la Información y Jefe de la DTI.

✓ Los dispositivos USB utilizados por personal interno y que contienen información de importancia deben almacenarse en lugares seguros, donde solo personal autorizado tenga acceso a ellos. Esto será supervisado por el Analista de Seguridad de la Información, reportando al Jefe de la DTI cualquier incidencia.

✓ Se ha propuesto y expuesto al Jefe de la Oficina Estratégica incluya en el presupuesto anual la adquisición de una máquina trituradora. Inicialmente en la DTI, que es el área que debido al gran uso de dispositivos de almacenamiento se requiere un mecanismo que garantice la pérdida total de la información almacenada en dichos medios. Luego se adquirirán más unidades para las áreas críticas de la Institución.

e) **Control de Accesos**

- **Gestión de Acceso de Usuarios**

Para brindar una seguridad adecuada en el acceso de usuarios a los servicios informáticos, se ha complementado la seguridad de la siguiente manera:

✓ El alta de un usuario se complementará con las siguientes acciones:

- El Jefe de la Oficina solicitante enviará un memorándum de acceso a la red, al Jefe de la Oficina Estratégica.

- El Jefe de la Oficina Estratégica aprobará el documento respectivo y lo derivará al Jefe de la DTI.

- El Jefe de la DTI comunicará vía correo electrónico al Coordinador de Soporte Informático para que realice dicha acción, con copia al Analista de Seguridad de la Información para que pueda monitorear dicha acción.

- El Coordinador de Soporte Informático brindará el acceso del nuevo usuario a la red de la Institución (correo electrónico, sistemas informáticos y pc), de acuerdo al perfil solicitado.

- El Coordinador de Soporte Técnico actualizará el **Registro de Alta/Baja de usuarios** (***Anexo 17***), formato supervisado mensualmente por el Jefe de la DTI y periódicamente por el Analista de Seguridad de la Información.

✓ La baja de un usuario por renuncia o despido se complementará con las siguientes acciones:

- El usuario con acceso a los servicios informáticos que renuncie o sea despedido comunicará vía correo electrónico al Jefe de la DTI, la fecha de permanencia en la Institución. Este correo se enviará con copia a su Jefe inmediato y al Jefe de la Oficina de Personal (adicional a la carta en caso de renuncia).

- El Jefe de la DTI comunicará al Coordinador de Soporte Informático y Analista de Seguridad de la Información dicha información, con la finalidad de que se revisen oportunamente todos los accesos con los que cuenta el usuario.

- El Jefe de la Oficina de Personal enviará un memorándum al Jefe de la Oficina Estratégica indicándole el cese del personal.

- El Jefe de la Oficina Estratégica derivará dicha información al Jefe de la DTI para su acción.

- El Jefe de la DTI derivará dicha acción al Coordinador de Soporte Informático para su ejecución.

- El coordinador de Soporte Informático realizará la baja respectiva y actualizará el **Registro de Alta/Baja de usuarios**. Formato supervisado por el Jefe de la DTI y Analista de Seguridad de la Información.

- **Gestión de Accesos a los Sistemas**

  Con la finalidad de garantizar una adecuada supervisión a los accesos que realizan los usuarios, este proceso se complementará con las siguientes acciones:

  - ✓ Implementación de una bitácora en cada sistema de información operativo, cuyo objetivo será registrar todos los eventos que realicen los usuarios una vez ingresados al sistema.

  - ✓ Las altas y/o modificaciones de accesos de usuarios (previa solicitud y aprobación), serán informados al Analista de Seguridad de la Información por parte del Analista de Sistemas.

  - ✓ El Analista de Seguridad de la Información verificará trimestralmente estos eventos, y en caso de encontrar algún acceso no permitido lo reportará al Analista de Sistemas y Jefe de la DTI. Esto será supervisado por el Jefe de la DTI.

  - ✓ El Analista de Seguridad de la Información verificará la estructura de la bitácora y planteará modificaciones para facilitar la obtención de incidentes de seguridad.

- **Clasificación de Sistemas**

  Para brindar un acceso adecuado de los sistemas a los usuarios solicitantes, el Analista de Sistemas y Analista de Seguridad de la Información han elaborada la siguiente clasificación de los sistemas en base a las áreas de la Institución. Sirviendo de esquema para garantizar accesos de manera adecuada y en función de las actividades que realizan (***Anexo 18***).

- **Gestión de Contraseñas**

  Debido a la ausencia de un esquema de seguridad para la creación de las contraseñas de acceso a servidores, sistemas y computadoras, se han establecido las siguientes acciones:

  - ✓ El Analista de Seguridad de la Información estableció el **Esquema de Seguridad para Contraseñas (*Anexo 19*)**.
  - ✓ El Analista de Sistema implementó el **Módulo de Contraseñas**, cuya función es la generación de contraseñas seguras de acuerdo al perfil del usuario. A la vez se encarga de generar las contraseñas de acceso a los servidores.
  - ✓ El cambio de contraseñas se realizó por áreas, empezando por las más críticas. Cumpliendo así el proceso de Gestión de Contraseñas.
  - ✓ Las contraseñas generadas se entregarán personalmente al usuario, evitándose el envío por correo electrónico o escritura en documentos de fácil acceso. Esto será supervisado por el Analista de Seguridad de la Información y reportado directamente al Jefe de la DTI.
  - ✓ El Analista de Seguridad de la Información se encargará de supervisar que el proceso se desarrolle de manera segura. A la vez propondrá al Jefe de la DTI mejoras en la seguridad en base a los estándares de seguridad informática, de manera periódica.
  - ✓ El Jefe de la DTI supervisará mensualmente todas las acciones referidas al proceso de Gestión de Contraseñas.

- **Gestión de Acceso a la Red**

  La gestión de acceso de la Red Institucional se complementará con las siguientes acciones:

  - ✓ Restricción de ingreso de laptops o equipos computacionales sin autorización respectiva. En caso de producirse lo contrario, se reportará a la DTI.

  - ✓ Para personal contratista que desee hacer uso de equipo de cómputo y red, se usará el registro **Autorización de Ingreso de Equipos Externos** (***Anexo 20***) y **Autorización de Acceso a la Red** (***Anexo 21***); formatos proporcionados por personal de Soporte Técnico y autorizados por el Jefe de la oficina o área donde se realizará el trabajo y Jefe de la DTI.

  - ✓ Para personal interno se coordinará con Soporte Técnico, y se emplearán los formatos correspondientes.

  - ✓ La red wifi utilizará el sistema de seguridad WPA-PSK/WPA2-PSK.

  - ✓ El Analista de Seguridad de la Información supervisará estas acciones y propondrá alternativas para mejorar la seguridad de la información.

  - ✓ El Jefe de la DTI supervisará trimestralmente el desarrollo adecuado de todas las acciones establecidas.

f) **Adquisición, Desarrollo y Mantenimiento de Sistemas**

- **Seguridad en los sistemas**

Para implementar una adecuada seguridad a los sistemas informáticos, tomaremos en cuenta lo siguiente:

✓ **Validación de los datos de entrada**

- Verificación de datos duplicados u otras verificaciones para detectar los siguientes errores:
  - Valores fuera de rango
  - Caracteres inválidos en los campos de datos
  - Datos faltantes o incompletos
  - Datos que exceden el límite de volumen
- Revisión periódica del contenido de los campos clave o los archivos de datos para comprobar su validez e integridad.
- Inspección de los documentos físicos de entrada para ver si hay cambios autorizados.
- Elaboración de procedimientos para actuar frente a los errores de validación.

✓ **Control del proceso interno**

- Implementación de excepciones dentro de las transacciones (procedimientos almacenados y desencadenadores), con la finalidad de evitar que se ejecuten líneas de código después de un error.
- Control del orden de las aplicaciones en la ejecución de los sistemas, con la finalidad de asegurar la integridad de los datos.

- Verificación de los equipos de cómputo involucrados en el procesamiento de los sistemas informáticos.

- Implementar un procedimiento para recuperar los procesos internos de los sistemas informáticos.

✓ **Validación de datos de salida**

- Validaciones de verosimilitud para comprobar que los datos de salida son los que el usuario solicitó.

- Proporcionar a los usuarios una adecuada información para poder determinar la exactitud, completitud, precisión y clasificación de la información.

o **Seguridad de los archivos**

Los archivos de los sistemas deberán estar disponibles solamente para personal autorizado de la DTI.

✓ **Control del software en producción**

- Verificar que las librerías de funciones, procedimientos, estructuras, etc., sean modificados solo por personal de desarrollo debidamente capacitado.

- El Analista de Seguridad de la Información deberá impedir que se instale código ejecutable mientras que todas las pruebas no sean exitosas. En caso de probar códigos incompletos, éstos deberán ejecutarse en ambientes separados.

- Documentar las versiones antiguas de los sistemas, junto a toda la información requerida (parámetros, funciones, procedimientos, bases de datos, etc.), con

la finalidad de que el área tenga un respaldo frente alguna contingencia con las actualizaciones realizadas.

- Elaborar un registro de todas las actualizaciones realizadas a las librerías de los sistemas informáticos operativos, indicando datos del Analista, fecha, cambios realizados y motivo de la actualización.

- El Jefe de la DTI y el Analista de Seguridad de la Información supervisarán todas estas indicaciones.

✓ **Protección de los datos de prueba**

- Evitar el uso de bases de datos operativas, ya que éstas almacenan todos los datos importantes de la Institución (contabilidad, personal, logística, producción, etc.).

- Solicitar autorización al Jefe de la DTI en coordinación con el Analista de Seguridad de la Información, cuando se copie información de las bases de datos operativas para un ambiente de prueba. Ello con la finalidad de no afectar la integridad de los datos utilizados en los sistemas de información, pudiendo originarse cierres inesperados y dejar sin servicio a todos los usuarios.

- Eliminar todos los datos de pruebas una vez que las pruebas se han completado exitosamente, ello con la finalidad de evitar que estos datos se almacenen en las bases de datos operativas.

- El Jefe de la DTI y el Analista de Seguridad de la Información supervisarán el cumplimiento de lo establecido.

✓ **Control de acceso al código**

- Implementación de un perfil para el acceso a las librerías de código fuente de los sistemas de información, con la finalidad de evitar cambios no intencionales. Con lo cual cada Analista de Sistemas contará con un listado de accesos de acuerdo a los sistemas que tiene asignado.

- Contar con un ambiente separado para el personal de apoyo (practicantes o terceros), el cual contenga información de los códigos y librerías de los sistemas de información.

- Mantener un registro de todos los accesos al código fuente de los sistemas de información en producción.

- El Jefe de la DTI y el Analista de Seguridad de la Información supervisarán el cumplimiento de lo establecido.

o **Seguridad en los procesos de desarrollo y soporte**

Se realizarán las acciones necesarias para garantizar una adecuada seguridad en desarrollo y mantenimiento de los sistemas de información.

✓ **Procedimiento de control de cambios**

- Verificar que los cambios a un sistema se realicen por parte del Analista de Sistemas autorizado, ello con la finalidad de evitar cambios no intencionales.

- Verificación de los controles de seguridad por parte del Analista de Seguridad de la Información, con la finalidad de garantizar que los cambios realizados no debilitan la seguridad de los sistemas.

- Identificación de todo el software, información y entidades que requieren aumentar el nivel de seguridad para los sistemas de información.

- Verificar que para iniciar un cambio o desarrollo de un sistema de información exista una autorización formal por parte del Jefe de la DTI, con pleno conocimiento del Jefe de la oficina Estratégica.

- Coordinar con los usuarios antes de dar inicio a una actualización del sistema de información, detallando las acciones a realizar, tiempo estimado y el objetivo.

- Documentar toda la información de un sistema antes de una modificación, incluyendo toda la información relacionada (bases de datos, funciones, procedimientos).

✓ **Revisión técnica de los cambios**

- Revisión periódica de los controles de seguridad de los sistemas, para asegurar que los cambios realizados no han comprometido la seguridad implementada.

- Elaboración de un plan anual de modificaciones a los sistemas de información, con la finalidad de garantizar un adecuado procesamiento de los datos y proporcionar una información adecuada a las oficinas de la Institución.

- El Analista de Seguridad de la Información supervisará que los cambios realizados son los mismos que han sido autorizados por el Jefe de la DTI, con la finalidad de evitar cambios no

intencionados sobre los sistemas de información operativos.

✓ **Fuga de información**

- El Jefe de DTI monitoreará regularmente bajo los procedimientos internos y la legislación vigente, las actividades que realice el personal de desarrollo y seguridad de la información.

- El Coordinador de Soporte Informático en coordinación con el Analista de Seguridad de la Información, supervisarán regularmente todos los equipos de cómputo encargados del procesamiento de los datos.

✓ **Desarrollo de software externo**

- La DTI trabaja con personal externo para el desarrollo de sistemas (dos), para lo cual se tendrá en cuenta los siguientes aspectos:

  - Acuerdo bajo licencia sobre la propiedad del código y derechos de propiedad intelectual.

  - Calidad del trabajo realizado con respecto al desarrollo del sistema.

  - Derechos de acceso para auditar el desarrollo del sistema.

  - Requisitos de funcionalidad segura del código desarrollado.

  - Informe de pruebas completas y exitosas en relación a los requerimientos solicitados.

g) Gestión de Continuidad del Negocio

La DTI tomará en cuenta los siguientes aspectos para implementar una adecuada Gestión de Continuidad del Negocio.

- **Seguridad de la información en la continuidad del negocio**
  - Comprender los riesgos que la Institución corre desde el punto de vista de su vulnerabilidad e impacto, incluyendo la identificación y priorización de los procesos críticos del negocio.
  - Identificar todos los activos implicados en los procesos críticos del negocio.
  - Comprender el impacto que tendrían las interrupciones en los procesos de la DTI y su repercusión hacia el resto de área de la Institución.
  - Identificar los recursos financieros, institucionales, técnicos y ambientales necesarios para actuar frente el desarrollo de alguna contingencia en la Institución.
  - Considerar un plan de seguridad del personal y protección de las instalaciones de procesamiento de información (servidores, Backup y equipos computacionales).
  - Actualizar y documentar el plan de continuidad del negocio, incorporando los requisitos de seguridad de la información identificados en las etapas anteriores.

- **Continuidad del negocio y evaluación de riesgos**
  - Identificar los eventos que pueden ocasionar interrupciones en los procesos de la Institución.

- Evaluación de los riesgos por parte de las personas encargadas de la dirección de la Institución, asesorado en todo momento por el Jefe de la DTI y en Analista de Seguridad de la Información.

- Cuantificar y priorizar los riesgos contra criterios y objetivos relevantes para la Institución, incluyendo recursos críticos, impacto de las interrupciones y tiempo de recuperación.

- Elaborar el Plan Estratégico, con la finalidad de determinar un enfoque global de la continuidad de los procesos de la DTI.

o **Marco de planificación para la continuidad del negocio**

- Establecer adecuadamente el alcance para garantizar la seguridad y disponibilidad de los sistemas de información, incluyendo los datos almacenados en los servidores de la DTI.

- Designar formalmente equipos de trabajo y responsabilidades sobre cada personal de la DTI, a propuesta del Jefe de la DTI.

- Establecer un cronograma de simulacros, el cual permita brindar un entrenamiento adecuado al personal de la DTI.

- Elaborar un procedimiento de emergencia, que describa las actividades a realizar y los responsables de la ejecución, cuando alguna contingencia amenace las operaciones de la DTI.

- Designar activos y recursos, los cuales permitan realizas los procedimientos de emergencia.

4.1.3 Check (Monitorizar y revisar el SGSI)

Una vez realizado los 07 procesos del SGSI, se realizará un monitoreo de cada proceso del SGSI, con la finalidad de verificar si todo lo establecido ha brindado resultados positivos con la seguridad de la información en la DTI. La frecuencia de monitoreo será de cada 04 meses, teniendo la participación del Analista de Sistemas, Analista de Seguridad de la Información y Coordinador de Soporte Informático y estará supervisada por el Jefe de la DTI y Jefe de la Oficina Estratégica.

El formato a utilizar para el monitoreo es el siguiente:

PROCESO	
Resultados positivos	Resultados negativos
Alternativas a realizar	
Observaciones adicionales	
V°B° Jefe DTI	V°B° Jefe OE

Tabla N° 08: Formato de Monitoreo por proceso

4.1.4 Act (Mantener y mejorar el SGSI)

Para lograr mantener y mejorar el SGSI se ha impartido responsabilidades a todos los miembros de la DTI, con la finalidad de contribuir al mejoramiento de la seguridad de la información de la DTI y de la Institución. Estas responsabilidades se detallan en la siguiente tabla:

RESPONSABILIDADES PARA EL MANTENIMIENTO DEL SGSI
Jefe de la Oficina Estratégica
- Liderar el equipo de trabajo. - Proponer al Jefe de la Institución la asignación de los recursos necesarios para el mejoramiento de la seguridad de la información. - Proponer mejorar al equipo de trabajo en los aspectos de seguridad de la información.
Jefe de la DTI
- Supervisar el cumplimiento de las acciones establecidas por el SGSI - Proponer procesos de mejoras en el aspecto de seguridad de la información. - Coordinar equipos de trabajo para la implementación de alternativas de seguridad. - Asignar responsabilidades para mantener y mejorar el SGSI. - Aprobar las alternativas de seguridad propuestas por el personal de la DTI.
Analista de Seguridad de la Información
- Liderar el equipo frente a aspectos de seguridad de la información. - Proponer al Jefe de la DTI nuevas metodologías, técnicas o procedimientos de seguridad de la información. - Sustentar alternativas de mejora de los procesos de seguridad de la información. - Investigar e implementar todo lo relacionado a seguridad de la información. - Supervisar y coordinar las acciones propuestas por el personal de la DTI, relacionados a seguridad de la información.

Analista de Sistemas
- Implementar los procesos del SGSI en el desarrollo y mantenimiento de los sistemas de información. - Coordinar con el Analista de Seguridad de la Información la implementación de procedimientos de seguridad. - Proponer nuevas técnicas y procedimientos que permitan mejorar la seguridad de la información de los sistemas en funcionamiento. - Implementar metodologías de desarrollo que involucren aspectos de seguridad de la información.
Coordinador de Soporte Informático
- Implementar los procesos del SGSI en las actividades de soporte técnico. - Proponer la adquisición de software y hardware que permita brindar una adecuada seguridad de la información. - Implementar procedimientos de seguridad a la infraestructura con que cuenta la Institución. - Implementar planes y procedimientos que permitan una fácil restauración de los procesos de la DTI, en caso de producirse alguna contingencia.

4.2 Resultados para el pre-test

Para la obtención de los resultados de la investigación en el pre-test utilizaremos las Guías de Observación de los anexos correspondientes a cada proceso (01 al 07).

Para la ponderación respectiva se utilizó el criterio siguiente:

- **Si:** 10 puntos (cumple, realiza o implementa lo indicado)
- **Avance:** 6 puntos (cumple, realiza o implementa lo indicado parcialmente)
- **No:** 2 puntos (no cumple, realiza o implementa lo indicado)

4.2.1 Clasificación y control de activos

N°	Pregunta	Puntaje
01	El software operativo se encuentra clasificado en base a algún criterio	02
02	Se conoce la cantidad de software con la que cuenta la Institución	02
03	Se conoce la cantidad de software que se actualizó mediante upgrade	10
04	Conoce el número de computadoras operativas e inoperativas	02
05	Conoce el número de impresoras por tipo con los que cuenta la Institución	10
06	Los servidores se encuentran clasificados de acuerdo a su nivel de importancia frente a algún siniestro	06
07	Para el almacenamiento del backup se utilizó algún criterio de clasificación, el cual asegure su disponibilidad, integridad y confidencialidad	02
08	La documentación de los sistemas informáticos se controla periódicamente	02
09	Revisa o recopila información sobre controles de seguridad para respaldar los activos informáticos	02
10	En caso de producirse algún siniestro sabe qué tipo de documentación tiene que respaldar primeramente	02
TOTAL		**40**

Tabla N° 09: Clasificación y control de activos del pre-test

Fuente: Elaboración propia

4.2.2 Seguridad ligada al personal

N°	Pregunta	Puntaje
01	Existe algún acuerdo de confidencialidad de información para personal nuevo dentro del área	02
02	Se incluyen charlas relacionadas a seguridad de la información en las inducciones a nuevo personal	02
03	Existe algún control para asegurar que la información no sea comprometida en los trabajos de personal tercero	06
04	Es consciente de las amenazas y riesgos en el ámbito de la seguridad de la información	02
05	Existe algún procedimiento de entrenamiento al personal sobre la adecuada manipulación de los equipos informáticos	02
06	Sabe que hacer en caso de presentarse alguna fuga o robo de información en el área	02
07	El cese de personal incluye actividades de verificación de la seguridad de la información, durante el tiempo de permanencia	06
08	Se analizan y solucionan los errores producidos por mala manipulación de información	02
09	Existe planificación alguna de como difundir en la Institución las nociones de seguridad de la información	02
10	Dentro de las sanciones al personal se encuentra incluido aquellas relacionadas con la pérdida o robo de información confidencial	02
TOTAL		**28**

Tabla N° 10: Seguridad ligada al personal del pre-test

Fuente: Elaboración propia

4.2.3 Seguridad física y del entorno

N°	Pregunta	Puntaje
01	El acceso a las instalaciones de la DTI permite el ingreso de personal interno como externo por diferentes situaciones	02
02	Existen dispositivos de seguridad (cámaras, alarmas, etc.) instalados en puntos estratégicos del área o de la Institución	02
03	En los meses de producción hay algún resguardo adicional debido a la presencia de una gran cantidad de personal tercero	02
04	Existe una bitácora con información de fecha, hora y motivo de ingreso de personal externo al área	06
05	La estructura física que contiene los equipos de comunicaciones es la adecuada en relación la información que almacena	02
06	La DTI tiene señalizaciones adecuadas para diferenciar las diferentes áreas internas (desarrollo, soporte técnico, etc.)	02
07	El personal de la DTI cuenta con capacitación sobre uso adecuado de extinguidores frente a posibles incendios dentro de las instalaciones	06
08	Dentro de la DTI se diferencia las áreas seguras e inseguras, en caso de producirse algún siniestro	02
09	El cableado eléctrico implementado para los equipos de comunicaciones es adecuado	10
10	Los equipos computacionales tienen una adecuado plan de mantenimiento para evitar fallas eléctricas al personal	02
	TOTAL	**36**

Tabla N° 11: Seguridad física y del entorno del pre-test

Fuente: Elaboración propia

4.2.4 Gestión de comunicaciones y operaciones

N°	Pregunta	Puntaje
01	Existe definido procedimientos necesarios para una correcta operación de los equipos informáticos	02
02	Se realizan capacitaciones periódicas a los usuarios de los servicios informáticos (sobre diversos temas)	06
03	Existe un procedimiento de comunicación de incidentes relacionados a sistemas o equipos informáticos	02
04	La información perdida por un falla en el funcionamiento de un sistema o equipo informático es recuperada	02
05	Existe una adecuada coordinación entre los Analistas de Sistemas y usuarios con respecto al uso de los sistemas informáticos	02
06	La información se encuentra sincronizada y actualizada en todos los sistemas informáticos de la DTI	06
07	Se ejecutan revisiones a los sistemas después de un mantenimiento finalizado para comprobar que no se ha alterado los controles de seguridad de la información	06
08	Operacionalmente un sistema informático después de un mantenimiento solicitado, sigue manteniendo los mismo objetivos por los cuales fue diseñado	10
09	Se realizan verificaciones periódicas sobre los equipos de cómputo a fin de evitar el uso o instalación de software no licenciado	06
10	El proceso de desinfección de medios extraíbles de usuarios se realizan en todo momento	02
	TOTAL	**44**

Tabla N° 12: Gestión de comunicaciones y operaciones del pre-test

Fuente: Elaboración propia

4.2.5 Control de accesos

N°	Pregunta	Puntaje
01	Está definido las actividades a realizarse cuando un usuario de servicios informáticos cesa de la Institución	06
02	Existe un registro actualizado de las altas y bajas de usuarios, el cual permita mostrar información de historial de usuarios	02
03	Existe un registro de perfiles y accesos de los usuarios a los servicios informáticos operativos	02
04	Existe una clasificación de perfiles para el acceso a la información en base a las áreas de la Institución	02
05	Los accesos a los sistemas informáticos se han brindado siempre en función a las actividades del usuario solicitante	02
06	Las contraseñas de usuarios para el acceso a los sistemas informáticos son seguras, teniendo en cuenta la información que procesan y almacenan	06
07	Existe algún control que brinde seguridad adecuada a los documentos (memorándum), que contienen información de acceso a servicios informáticos	02
08	La alta de servicios informáticos cuenta con un procedimiento establecido a fin de evitar brindar acceso antes de tener todas las aprobaciones correspondientes	06
09	Los archivos utilizados para almacenar contraseñas de acceso a los diferentes servicios informáticos se encuentran protegidos	02
10	Existe algún procedimiento para controlar el acceso a la red Institucional	02
	TOTAL	**32**

Tabla N° 13: Control de accesos del pre-test

Fuente: Elaboración propia

4.2.6 Adquisición, desarrollo y mantenimiento de sistemas

N°	Pregunta	Puntaje
01	Se utiliza más de un criterio de validación de datos en el procesamiento de la información de los sistemas informáticos	06
02	Todos los sistemas informáticos implementan rutinas de recuperación de datos, a fin de evitar procesamientos erróneos o incompletos de información	02
03	Existe un registro actualizado de los errores producidos por los sistemas informáticos, en los cuales se haya perdido una gran cantidad información para su posterior revisión y solución	02
04	Se realizan revisiones periódicas a los sistemas informáticos en producción, a fin de garantizar que cumplen con los objetivos iniciales e implementan los controles de seguridad adecuados	02
05	Todas las modificaciones solicitadas por los usuarios se realizan en un ambiente de prueba y luego se ejecutan en el ambiente de producción	06
06	Existe una asignación de los sistemas informáticos por cada Analista de Sistemas, para que estos se hagan responsable de su implementación y mantenimiento; en la cual el acceso al código fuente se encuentra restringido	02
07	Los archivos de datos se encuentran debidamente documentados y almacenados, debido a las migraciones realizadas	06
08	La implantación de código ejecutable en los equipos de cómputo siempre se realiza luego de concluir con todas las pruebas respectivas	02
09	Se realiza una coordinación adecuada entre el personal de soporte técnico para la configuración de los archivos y software necesario	06
10	Se autoriza el copiado de información en producción a ambientes de prueba o viceversa	02
TOTAL		**36**

Tabla N° 14: Adquisición, desarrollo y mantenimiento de sistemas del pre-test

Fuente: Elaboración propia

4.2.7 Gestión de continuidad del negocio

N°	Pregunta	Puntaje
01	Se tiene identificado todos los riesgos a los que está expuesto la DTI	06
02	De los riesgos identificados, se ha elaborada el conjunto de acciones necesarias a realizar para su mitigación	02
03	Se tiene definido el grupo de trabajo y las actividades a realizar en caso de presentarse algún siniestro en la DTI o en la Institución	06
04	Se planifican entrenamientos del personal a través de simulacros internos del área, con la finalidad de que se pongan en práctica las acciones a realizar en caso de un siniestro	02
05	Se tiene un presupuesto asignado para una posible recuperación de los activos informáticos de la Institución	02
06	La Jefatura de la Institución tiene alcance de los riesgos a los que se encuentran expuestos los equipos de informáticos y el impacto que éstos pueden ocasionar	02
07	Existe una coordinación con las áreas de seguridad y patrimonio para que brinden su apoyo en caso de presentarse un siniestro en la DTI (incendio, corto circuito, explosiones, etc.)	06
08	Existe una coordinación con los proveedores de servicios para que restauren los servicios interrumpidos en un corto plazo	02
09	Existe una coordinación con la sede de Metal Mecánica en la provisión temporal de los equipos informáticos	06
10	Los lineamientos estratégicos de la Institución incluyen planes de continuidad del negocio y recuperación de los daños ocasionados frente algún siniestro	02
	TOTAL	**36**

Tabla N° 15: Gestión de continuidad del negocio del pre-test

Fuente: Elaboración propia

4.3 Resultados para el post-test

4.3.1 Clasificación y control de activos

N°	Pregunta	Puntaje
01	El software operativo se encuentra clasificado en base a algún criterio	10
02	Se conoce la cantidad de software con la que cuenta la Institución	10
03	Se conoce la cantidad de software que se actualizó mediante upgrade	10
04	Conoce el número de computadoras operativas e inoperativas	10
05	Conoce el número de impresoras por tipo con los que cuenta la Institución	10
06	Los servidores se encuentran clasificados de acuerdo a su nivel de importancia frente a algún siniestro	10
07	Para el almacenamiento del backup se utilizó algún criterio de clasificación, el cual asegure su disponibilidad, integridad y confidencialidad	06
08	La documentación de los sistemas informáticos se controla periódicamente	10
09	Revisa o recopila información sobre controles de seguridad para respaldar los activos informáticos	06
10	En caso de producirse algún siniestro sabe qué tipo de documentación tiene que respaldar primeramente	10
TOTAL		**92**

Tabla N° 16: Clasificación y control de activos del post-test

Fuente: Elaboración propia

4.3.2 Seguridad ligada al personal

N°	Pregunta	Puntaje
01	Existe algún acuerdo de confidencialidad de información para personal nuevo dentro del área	10
02	Se incluyen charlas relacionadas a seguridad de la información en las inducciones a nuevo personal	10
03	Existe algún control para asegurar que la información no sea comprometida en los trabajos de personal tercero	10
04	Es consciente de las amenazas y riesgos en el ámbito de la seguridad de la información	10
05	Existe algún procedimiento de entrenamiento al personal sobre la adecuada manipulación de los equipos informáticos	10
06	Sabe que hacer en caso de presentarse alguna fuga o robo de información en el área	10
07	El cese de personal incluye actividades de verificación de la seguridad de la información, durante el tiempo de permanencia	10
08	Se analizan y solucionan los errores producidos por mala manipulación de información	10
09	Existe planificación alguna de como difundir en la Institución las nociones de seguridad de la información	10
10	Dentro de las sanciones al personal se encuentra incluido aquellas relacionadas con la pérdida o robo de información confidencial	06
TOTAL		**96**

Tabla N° 17: Seguridad ligada al personal del post-test

Fuente: Elaboración propia

4.3.3 Seguridad física y del entorno

N°	Pregunta	Puntaje
01	El acceso a las instalaciones de la DTI permite el ingreso de personal interno como externo por diferentes situaciones	10
02	Existen dispositivos de seguridad (cámaras, alarmas, etc.) instalados en puntos estratégicos del área o de la Institución	06
03	En los meses de producción hay algún resguardo adicional debido a la presencia de una gran cantidad de personal tercero	10
04	Existe una bitácora con información de fecha, hora y motivo de ingreso de personal externo al área	10
05	La estructura física que contiene los equipos de comunicaciones es la adecuada en relación la información que almacena	06
06	La DTI tiene señalizaciones adecuadas para diferenciar las diferentes áreas internas (desarrollo, soporte técnico, etc.)	10
07	El personal de la DTI cuenta con capacitación sobre uso adecuado de extinguidores frente a posibles incendios dentro de las instalaciones	10
08	Dentro de la DTI se diferencia las áreas seguras e inseguras, en caso de producirse algún siniestro	10
09	El cableado eléctrico implementado para los equipos de comunicaciones es adecuado	10
10	Los equipos computacionales tienen una adecuado plan de mantenimiento para evitar fallas eléctricas al personal	10
	TOTAL	**92**

Tabla N° 18: Seguridad física y del entorno del post-test

Fuente: Elaboración propia

4.3.4 Gestión de comunicaciones y operaciones

N°	Pregunta	Puntaje
01	Existe definido procedimientos necesarios para una correcta operación de los equipos informáticos	10
02	Se realizan capacitaciones periódicas a los usuarios de los servicios informáticos (sobre diversos temas)	10
03	Existe un procedimiento de comunicación de incidentes relacionados a sistemas o equipos informáticos	10
04	La información perdida por un falla en el funcionamiento de un sistema o equipo informático es recuperada	06
05	Existe una adecuada coordinación entre los Analistas de Sistemas y usuarios con respecto al uso de los sistemas informáticos	10
06	La información se encuentra sincronizada y actualizada en todos los sistemas informáticos de la DTI	10
07	Se ejecutan revisiones a los sistemas después de un mantenimiento finalizado para comprobar que no se ha alterado los controles de seguridad de la información	10
08	Operacionalmente un sistema informático después de un mantenimiento solicitado, sigue manteniendo los mismo objetivos por los cuales fue diseñado	10
09	Se realizan verificaciones periódicas sobre los equipos de cómputo a fin de evitar el uso o instalación de software no licenciado	10
10	El proceso de desinfección de medios extraíbles de usuarios se realizan en todo momento	10
	TOTAL	**96**

Tabla N° 19: Gestión de comunicaciones y operaciones del post-test

Fuente: Elaboración propia

4.3.5 Control de accesos

N°	Pregunta	Puntaje
01	Está definido las actividades a realizarse cuando un usuario de servicios informáticos cesa de la Institución	10
02	Existe un registro actualizado de las altas y bajas de usuarios, el cual permita mostrar información de historial de usuarios	10
03	Existe un registro de perfiles y accesos de los usuarios a los servicios informáticos operativos	10
04	Existe una clasificación de perfiles para el acceso a la información en base a las áreas de la Institución	10
05	Los accesos a los sistemas informáticos se han brindado siempre en función a las actividades del usuario solicitante	06
06	Las contraseñas de usuarios para el acceso a los sistemas informáticos son seguras, teniendo en cuenta la información que procesan y almacenan	10
07	Existe algún control que brinde seguridad adecuada a los documentos (memorándum), que contienen información de acceso a servicios informáticos	10
08	La alta de servicios informáticos cuenta con un procedimiento establecido a fin de evitar brindar acceso antes de tener todas las aprobaciones correspondientes	10
09	Los archivos utilizados para almacenar contraseñas de acceso a los diferentes servicios informáticos se encuentran protegidos	10
10	Existe algún procedimiento para controlar el acceso a la red Institucional	10
	TOTAL	**96**

Tabla N° 20: Control de accesos del post-test

Fuente: Elaboración propia

4.3.6 Adquisición, desarrollo y mantenimiento de sistemas

N°	Pregunta	Puntaje
01	Se utiliza más de un criterio de validación de datos en el procesamiento de la información de los sistemas informáticos	10
02	Todos los sistemas informáticos implementan rutinas de recuperación de datos, a fin de evitar procesamientos erróneos o incompletos de información	10
03	Existe un registro actualizado de los errores producidos por los sistemas informáticos, en los cuales se haya perdido una gran cantidad información para su posterior revisión y solución	10
04	Se realizan revisiones periódicas a los sistemas informáticos en producción, a fin de garantizar que cumplen con los objetivos iniciales e implementan los controles de seguridad adecuados	10
05	Todas las modificaciones solicitadas por los usuarios se realizan en un ambiente de prueba y luego se ejecutan en el ambiente de producción	06
06	Existe una asignación de los sistemas informáticos por cada Analista de Sistemas, para que estos se hagan responsable de su implementación y mantenimiento; en la cual el acceso al código fuente se encuentra restringido	10
07	Los archivos de datos se encuentran debidamente documentados y almacenados, debido a las migraciones realizadas	10
08	La implantación de código ejecutable en los equipos de cómputo siempre se realiza luego de concluir con todas las pruebas respectivas	06
09	Se realiza una coordinación adecuada entre el personal de soporte técnico para la configuración de los archivos y software necesario	10
10	Se autoriza el copiado de información en producción a ambientes de prueba o viceversa	10
TOTAL		**92**

Tabla N° 21: Adquisición, desarrollo y mantenimiento de sistemas del post-test

Fuente: Elaboración propia

4.3.7 Gestión de continuidad del negocio

N°	Pregunta	Puntaje
01	Se tiene identificado todos los riesgos a los que está expuesto la DTI	10
02	De los riesgos identificados, se ha elaborada el conjunto de acciones necesarias a realizar para su mitigación	10
03	Se tiene definido el grupo de trabajo y las actividades a realizar en caso de presentarse algún siniestro en la DTI o en la Institución	10
04	Se planifican entrenamientos del personal a través de simulacros internos del área, con la finalidad de que se pongan en práctica las acciones a realizar en caso de un siniestro	10
05	Se tiene un presupuesto asignado para una posible recuperación de los activos informáticos de la Institución	06
06	La Jefatura de la Institución tiene alcance de los riesgos a los que se encuentran expuestos los equipos de informáticos y el impacto que éstos pueden ocasionar	10
07	Existe una coordinación con las áreas de seguridad y patrimonio para que brinden su apoyo en caso de presentarse un siniestro en la DTI (incendio, corto circuito, explosiones, etc.)	10
08	Existe una coordinación con los proveedores de servicios para que restauren los servicios interrumpidos en un corto plazo	10
09	Existe una coordinación con la sede de Metal Mecánica en la provisión temporal de los equipos informáticos	10
10	Los lineamientos estratégicos de la Institución incluyen planes de continuidad del negocio y recuperación de los daños ocasionados frente algún siniestro	06
	TOTAL	**92**

Tabla N° 22: Gestión de continuidad del negocio del post-test

Fuente: Elaboración propia

CAPÍTULO V

DISCUSIÓN

El problema que el presente trabajo de investigación pretende resolver es ¿En qué medida el Sistema de Gestión permitirá mejorar la Seguridad de la Información en la Institución Servicios Industriales de la Marina?

Para dar solución a este problema se planteó la siguiente hipótesis:

El Sistema de Gestión permite mejorar la Seguridad de la Información en la Institución Servicios Industriales de la Marina.

5.1 Demostración de la hipótesis

Para medir los indicadores de la variable dependiente utilizaremos las Guías de Observación realizadas (anexos) y la siguiente clasificación:

PROCESO	INDICADOR
Seguridad ligada al personal	Confidencialidad
Seguridad física y del entorno	
Gestión de comunicaciones y operaciones	Disponibilidad
Adquisición, desarrollo y mantenimiento de sistemas	
Gestión de continuidad del negocio	
Clasificación y control de activos	Integridad
Control de accesos	

Tabla N° 23: Clasificación de indicadores de la variable dependiente

Fuente: Elaboración propia

5.1.1 Indicador 1

y1: Confidencialidad de la información

a) Seguridad ligada al personal

Resultado:

Para la aplicación de la Guía de Observación N° 02 se utilizó las preguntas de la tabla (Anexo 02), con la finalidad de establecer un promedio de las preguntas en relación a las respuestas y el tamaño de la muestra.

El resultado se muestra a continuación:

N°	Pregunta	Puntaje
01	Existe algún acuerdo de confidencialidad de información para personal nuevo dentro del área	10
02	Se incluyen charlas relacionadas a seguridad de la información en las inducciones a nuevo personal	10
03	Existe algún control para asegurar que la información no sea comprometida en los trabajos de personal tercero	10
04	Es consciente de las amenazas y riesgos en el ámbito de la seguridad de la información	10
05	Existe algún procedimiento de entrenamiento al personal sobre la adecuada manipulación de los equipos informáticos	10
06	Sabe que hacer en caso de presentarse alguna fuga o robo de información en el área	10
07	El cese de personal incluye actividades de verificación de la seguridad de la información, durante el tiempo de permanencia	10
08	Se analizan y solucionan los errores producidos por mala manipulación de información	10
09	Existe planificación alguna de como difundir en la Institución las nociones de seguridad de la información	10

10	Dentro de las sanciones al personal se encuentra incluido aquellas relacionadas con la pérdida o robo de información confidencial	06
	PROMEDIO	**9,6**

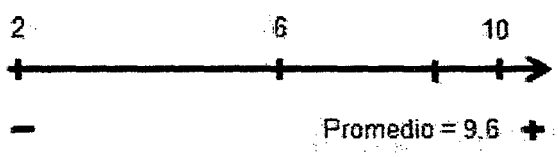
Tabla N° 24: Resultados por pregunta

Fuente: Elaboración propia

Para la obtención del puntaje se utilizó 03 criterios:

- **Si:** 10 puntos
- **Avance:** 6 puntos
- **No:** 2 puntos

El rango de puntuación se muestra a continuación:



Se consideró 2 en el extremo izquierdo, debido a que representa el puntaje mínimo que se puede ponderar a una pregunta, mientras que en el extremo derecho se consideró 10, el cual representa el puntaje óptimo (ideal).

El resultado de la aplicación de la Guía de Observación N° 02 es 9.6, el cual nos indica que la **Seguridad ligada al personal** es la adecuada y contribuye a mejorar la **confidencialidad de la información.**

Prueba de t student

Adicional a la aplicación de la Guía de Observación, también probaremos si es estadísticamente significativo. Esto lo lograremos a través de la prueba de t student, tal como se muestra a continuación:

Paso 1: Planteamiento de las hipótesis estadísticas

Seleccionamos la hipótesis nula y la hipótesis alternativa

H_0: $\mu = 6$: No se aplica una adecuada seguridad ligada al personal

Ha: $\mu > 6$: Se aplica una adecuada seguridad ligada al personal

Paso 2: Nivel de confianza o significancia: (95%)

$\alpha = 5\%$ (margen de error)

Paso 3: Regiones de aceptación y rechazo

Según la tabla de t student:

$t(0.95,9) = 1.833$

Si $\mathbf{t_0} <= 1.833$ entonces H_0 se acepta

Si $\mathbf{t_0} > 1.833$ entonces H_0 se rechaza

Paso 4: Cálculos

Las fórmulas para calcular el valor del t student y la desviación estándar de la muestra, son las siguientes:

$$S = \sqrt{\frac{\sum_{i=1}^{N} (X_i - \bar{X})^2}{N}}$$

$$t = \frac{\bar{X} - \mu}{S} \sqrt{N-1}$$

Donde:

t : Formula estadística t de Student

S : Desviación estándar

N : Número de elementos

$\bar{X}$: Media obtenida

μ : Media estadística

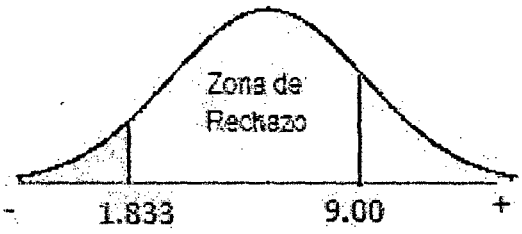
Entonces para:

N= 10 $\bar{X}$= 9,6 μ= 6

Calculamos la desviación estándar **S= 1,20**

Por lo tanto $\mathbf{t_o}$ **= 9,00**

$\mathbf{t_0}$ = 9,00 > 1.833 entonces H_0 se rechaza



Paso 5: Conclusión

Como el resultado no cae en la zona de aceptación ($\mathbf{t_0}$ > 1.833) se rechaza la hipótesis nula y se acepta la hipótesis alternativa, por lo tanto podemos decir que ante la hipótesis "El Sistema de Gestión permite mejorar la Seguridad de la Información en la Institución Servicios Industriales de la Marina" el indicador **confidencialidad de la información** es **válido**, ya que está demostrado.

b) Seguridad física y del entorno

Resultado:

Para la aplicación de la Guía de Observación N° 03 se utilizó las preguntas de la tabla (Anexo 03), con la finalidad de establecer un promedio de las preguntas en relación a las respuestas y el tamaño de la muestra.

El resultado se muestra a continuación:

N°	Pregunta	Puntaje
01	El acceso a las instalaciones de la DTI permite el ingreso de personal interno como externo por diferentes situaciones	10
02	Existen dispositivos de seguridad (cámaras, alarmas, etc.) instalados en puntos estratégicos del área o de la Institución	06
03	En los meses de producción hay algún resguardo adicional debido a la presencia de una gran cantidad de personal tercero	10
04	Existe una bitácora con información de fecha, hora y motivo de ingreso de personal externo al área	10
05	La estructura física que contiene los equipos de comunicaciones es la adecuada en relación la información que almacena	06
06	La DTI tiene señalizaciones adecuadas para diferenciar las diferentes áreas internas (desarrollo, soporte técnico, etc.)	10
07	El personal de la DTI cuenta con capacitación sobre uso adecuado de extinguidores frente a posibles incendios dentro de las instalaciones	10
08	Dentro de la DTI se diferencia las áreas seguras e inseguras, en caso de producirse algún siniestro	10
09	El cableado eléctrico implementado para los equipos de comunicaciones es adecuado	10
10	Los equipos computacionales tienen una adecuado plan de mantenimiento para evitar fallas eléctricas al personal	10
PROMEDIO		**9,2**

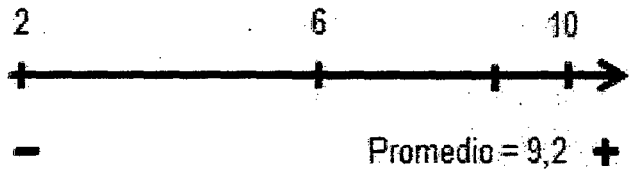
Tabla N° 25: Resultados por pregunta

Fuente: Elaboración propia

Para la obtención del puntaje se utilizó 03 criterios:

- **Si:** 10 puntos
- **Avance:** 6 puntos
- **No:** 2 puntos

El rango de puntuación se muestra a continuación:



Se consideró 2 en el extremo izquierdo, debido a que representa el puntaje mínimo que se puede ponderar a una pregunta, mientras que en el extremo derecho se consideró 10, el cual representa el puntaje óptimo (ideal).

El resultado de la aplicación de la Guía de Observación N° 03 es 9.2, el cual nos indica que la **Seguridad física y del entorno** es la adecuada y contribuye a mejorar la **confidencialidad de la información**.

Prueba de t student

Adicional a la aplicación de la Guía de Observación, también probaremos si es estadísticamente significativo. Esto lo lograremos a través de la prueba de t student, tal como se muestra a continuación:

Paso 1: Planteamiento de las hipótesis estadísticas

Seleccionamos la hipótesis nula y la hipótesis alternativa

H_0: $\mu = 6$: No se aplica una adecuada seguridad física y del entorno

Ha: $\mu > 6$: Se aplica una adecuada seguridad física y del entorno

Paso 2: Nivel de confianza o significancia: (95%)

$\alpha = 5\%$ (margen de error)

Paso 3: Regiones de aceptación y rechazo

Según la tabla de t student:

$t(0.95,9) = 1.833$

Si t_0 <= 1.833 entonces H_0 se acepta

Si t_0 > 1.833 entonces H_0 se rechaza

Paso 4: Cálculos

Las fórmulas para calcular el valor del t student y la desviación estándar de la muestra, son las siguientes:

$$S = \sqrt{\frac{\sum_{i=1}^{N} (X_i - \bar{X})^2}{N}}$$

$$t = \frac{\bar{X} - \mu}{\frac{S}{\sqrt{N-1}}}$$

Donde:

t : Formula estadística t de Student

S : Desviación estándar

N : Número de elementos

$\bar{X}$: Media obtenida

μ : Media estadística

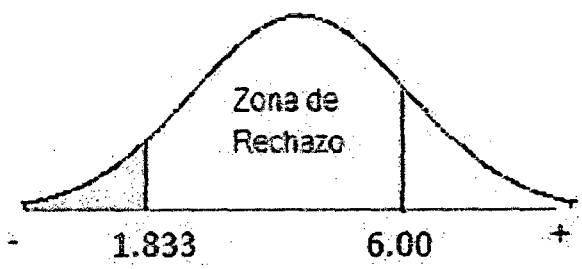
Entonces para:

N= 10 $\bar{X}$= 9,2 μ= 6

Calculamos la desviación estándar **S= 1,60**

Por lo tanto t_o = **6,00**

t_0 = 6,00 > 1.833 entonces H_0 se rechaza



Paso 5: Conclusión

Como el resultado no cae en la zona de aceptación ($t_0 > 1.833$) se rechaza la hipótesis nula y se acepta la hipótesis alternativa, por lo tanto podemos decir que ante la hipótesis "El Sistema de Gestión permite mejorar la Seguridad de la Información en la Institución Servicios Industriales de la Marina" el indicador **confidencialidad de la información** es **válido,** ya que está demostrado.

5.1.2 Indicador 2

y2: Disponibilidad de la información

a) Gestión de comunicaciones y operaciones

Resultado:

Para la aplicación de la Guía de Observación N° 04 se utilizó las preguntas de la tabla (Anexo 04), con la finalidad de establecer un promedio de las preguntas en relación a las respuestas y el tamaño de la muestra.

El resultado se muestra a continuación:

N°	Pregunta	Puntaje
01	Existe definido procedimientos necesarios para una correcta operación de los equipos informáticos	10
02	Se realizan capacitaciones periódicas a los usuarios de los servicios informáticos (sobre diversos temas)	10
03	Existe un procedimiento de comunicación de incidentes relacionados a sistemas o equipos informáticos	10
04	La información perdida por un falla en el funcionamiento de un sistema o equipo informático es recuperada	06
05	Existe una adecuada coordinación entre los Analistas de Sistemas y usuarios con respecto al uso de los sistemas informáticos	10
06	La información se encuentra sincronizada y actualizada en todos los	10

	sistemas informáticos de la DTI	
07	Se ejecutan revisiones a los sistemas después de un mantenimiento finalizado para comprobar que no se ha alterado los controles de seguridad de la información	10
08	Operacionalmente un sistema informático después de un mantenimiento solicitado, sigue manteniendo los mismo objetivos por los cuales fue diseñado	10
09	Se realizan verificaciones periódicas sobre los equipos de cómputo a fin de evitar el uso o instalación de software no licenciado	10
10	El proceso de desinfección de medios extraíbles de usuarios se realizan en todo momento	10
PROMEDIO		**9,6**

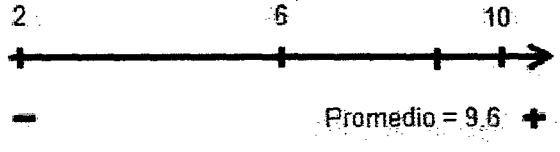
Tabla N° 26: Resultados por pregunta

Fuente: Elaboración propia

Para la obtención del puntaje se utilizó 03 criterios:

- **Si:** 10 puntos
- **Avance:** 6 puntos
- **No:** 2 puntos

El rango de puntuación se muestra a continuación:



Se consideró 2 en el extremo izquierdo, debido a que representa el puntaje mínimo que se puede ponderar a una pregunta, mientras que en el extremo derecho se consideró 10, el cual representa el puntaje óptimo (ideal).

El resultado de la aplicación de la Guía de Observación N° 04 es 9.6, el cual nos indica que la **Gestión de Comunicaciones y Operaciones** es la adecuada y contribuye a mejorar la **confidencialidad de la información.**

Prueba de t student

Adicional a la aplicación de la Guía de Observación, también probaremos si es estadísticamente significativo. Esto lo lograremos a través de la prueba de t student, tal como se muestra a continuación:

Paso 1: Planteamiento de las hipótesis estadísticas

Seleccionamos la hipótesis nula y la hipótesis alternativa

H_0: $\mu = 6$: No se aplica una adecuada gestión de operaciones y comunicaciones

Ha: $\mu > 6$: Se aplica una adecuada gestión de operaciones y comunicaciones

Paso 2: Nivel de confianza o significancia: (95%)

$\alpha = 5\%$ (margen de error)

Paso 3: Regiones de aceptación y rechazo

Según la tabla de t student:

$t(0.95,9) = 1.833$

Si $\mathbf{t_0} <= 1.833$ entonces H_0 se acepta

Si $\mathbf{t_0} > 1.833$ entonces H_0 se rechaza

Paso 4: Cálculos

Las fórmulas para calcular el valor del t student y la desviación estándar de la muestra, son las siguientes:

$$S = \sqrt{\frac{\sum_{i=1}^{N} (X_i - \bar{X})^2}{N}}$$

$$t = \frac{\bar{X} - \mu}{\frac{S}{\sqrt{N-1}}}$$

Donde:

t : Formula estadística t de Student

S : Desviación estándar

N : Número de elementos

$\bar{X}$: Media obtenida

μ : Media estadística

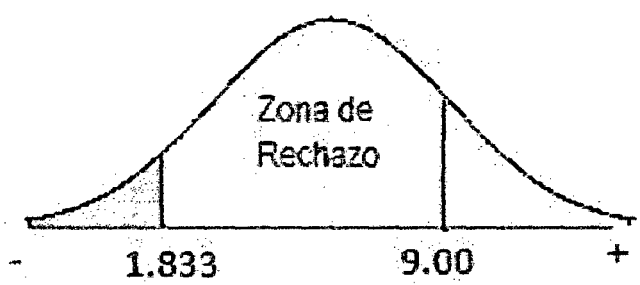
Entonces para:

N= 10 $\bar{X}$= 9,6 μ= 6

Calculamos la desviación estándar **S= 1,20**

Por lo tanto $\mathbf{t_o = 9{,}00}$

$\mathbf{t_0}$ = 9,00 > 1.833 entonces H_0 se rechaza



Paso 5: Conclusión

Como el resultado no cae en la zona de aceptación ($\mathbf{t_0}$ > 1.833) se rechaza la hipótesis nula y se acepta la hipótesis alternativa, por lo tanto podemos decir que ante la hipótesis "El Sistema de Gestión permite mejorar la Seguridad de la Información en la Institución

Servicios Industriales de la Marina" el indicador **disponibilidad de la información** es **válido**, ya que está demostrado.

b) Adquisición, desarrollo y mantenimiento de sistemas

Resultado:

Para la aplicación de la Guía de Observación N° 06 se utilizó las preguntas de la tabla (Anexo 06), con la finalidad de establecer un promedio de las preguntas en relación a las respuestas y el tamaño de la muestra.

El resultado se muestra a continuación:

N°	Pregunta	Puntaje
01	Se utiliza más de un criterio de validación de datos en el procesamiento de la información de los sistemas informáticos	10
02	Todos los sistemas informáticos implementan rutinas de recuperación de datos, a fin de evitar procesamientos erróneos o incompletos de información	10
03	Existe un registro actualizado de los errores producidos por los sistemas informáticos, en los cuales se haya perdido una gran cantidad información para su posterior revisión y solución	10
04	Se realizan revisiones periódicas a los sistemas informáticos en producción, a fin de garantizar que cumplen con los objetivos iniciales e implementan los controles de seguridad adecuados	10
05	Todas las modificaciones solicitadas por los usuarios se realizan en un ambiente de prueba y luego se ejecutan en el ambiente de producción	06
06	Existe una asignación de los sistemas informáticos por cada Analista de Sistemas, para que estos se hagan responsable de su implementación y mantenimiento; en la cual el acceso al código fuente se encuentra restringido	10
07	Los archivos de datos se encuentran debidamente documentados y almacenados, debido a las migraciones realizadas	10

08	La implantación de código ejecutable en los equipos de cómputo siempre se realiza luego de concluir con todas las pruebas respectivas	06
09	Se realiza una coordinación adecuada entre el personal de soporte técnico para la configuración de los archivos y software necesario	10
10	Se autoriza el copiado de información en producción a ambientes de prueba o viceversa	10
	PROMEDIO	**9,2**

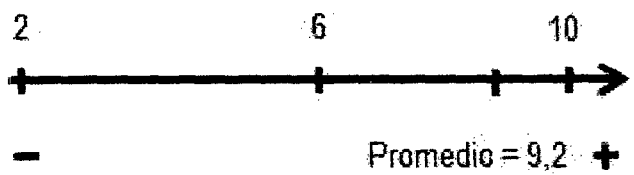
Tabla N° 27: Resultados por pregunta

Fuente: Elaboración propia

Para la obtención del puntaje se utilizó 03 criterios:

- **Si:** 10 puntos
- **Avance:** 6 puntos
- **No:** 2 puntos

El rango de puntuación se muestra a continuación:



Se consideró 2 en el extremo izquierdo, debido a que representa el puntaje mínimo que se puede ponderar a una pregunta, mientras que en el extremo derecho se consideró 10, el cual representa el puntaje óptimo (ideal).

El resultado de la aplicación de la Guía de Observación N° 06 es 9.2, el cual nos indica que la **Adquisición, desarrollo y mantenimiento de sistemas** es la adecuada y contribuye a mejorar la **disponibilidad de la información.**

Prueba de t student

Adicional a la aplicación de la Guía de Observación, también probaremos si es estadísticamente significativo. Esto lo lograremos a través de la prueba de t student, tal como se muestra a continuación:

Paso 1: Planteamiento de las hipótesis estadísticas

Seleccionamos la hipótesis nula y la hipótesis alternativa

H_0: $\mu = 6$: No se aplica una adecuada adquisición, desarrollo y mantenimiento de sistemas

Ha: $\mu > 6$: Se aplica una adecuada adquisición, desarrollo y mantenimiento de sistemas

Paso 2: Nivel de confianza o significancia: (95%)

$\alpha = 5\%$ (margen de error)

Paso 3: Regiones de aceptación y rechazo

Según la tabla de t student:

$t(0.95,9) = 1.833$

Si $\mathbf{t_0} <= 1.833$ entonces H_0 se acepta

Si $\mathbf{t_0} > 1.833$ entonces H_0 se rechaza

Paso 4: Cálculos

Las fórmulas para calcular el valor del t student y la desviación estándar de la muestra, son las siguientes:

$$S = \sqrt{\frac{\sum_{i=1}^{N} (X_i - \bar{X})^2}{N}}$$

$$t = \frac{\bar{X} - \mu}{S} \sqrt{N-1}$$

Donde:

t : Formula estadística t de Student

S : Desviación estándar

N : Número de elementos

$\bar{X}$: Media obtenida

μ : Media estadística

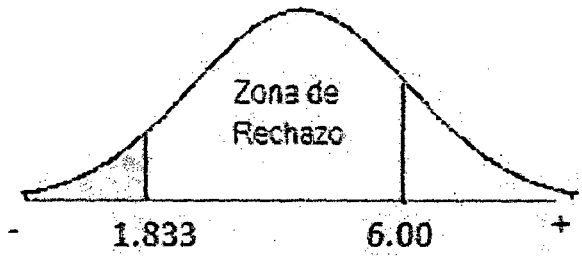
Entonces para:

N= 10 $\bar{X}$= 9,2 μ= 6

Calculamos la desviación estándar **S= 1,60**

Por lo tanto $\mathbf{t_o = 6{,}00}$

$\mathbf{t_0}$ = 6,00 > 1.833 entonces H_0 se rechaza



Paso 5: Conclusión

Como el resultado no cae en la zona de aceptación ($\mathbf{t_0}$ > 1.833) se rechaza la hipótesis nula y se acepta la hipótesis alternativa, por lo tanto podemos decir que ante la hipótesis "El Sistema de Gestión permite mejorar la Seguridad de la Información en la Institución

Servicios Industriales de la Marina" el indicador **disponibilidad de la información** es **válido**, ya que está demostrado.

c) Gestión de continuidad del negocio

Resultado:

Para la aplicación de la Guía de Observación N° 07 se utilizó las preguntas de la tabla (Anexo 07), con la finalidad de establecer un promedio de las preguntas en relación a las respuestas y el tamaño de la muestra.

El resultado se muestra a continuación:

N°	Pregunta	Puntaje
01	Se tiene identificado todos los riesgos a los que está expuesto la DTI	10
02	De los riesgos identificados, se ha elaborada el conjunto de acciones necesarias a realizar para su mitigación	10
03	Se tiene definido el grupo de trabajo y las actividades a realizar en caso de presentarse algún siniestro en la DTI o en la Institución	10
04	Se planifican entrenamientos del personal a través de simulacros internos del área, con la finalidad de que se pongan en práctica las acciones a realizar en caso de un siniestro	10
05	Se tiene un presupuesto asignado para una posible recuperación de los activos informáticos de la Institución	06
06	La Jefatura de la Institución tiene alcance de los riesgos a los que se encuentran expuestos los equipos de informáticos y el impacto que éstos pueden ocasionar	10
07	Existe una coordinación con las áreas de seguridad y patrimonio para que brinden su apoyo en caso de presentarse un siniestro en la DTI (incendio, corto circuito, explosiones, etc.)	10
08	Existe una coordinación con los proveedores de servicios para que restauren los servicios interrumpidos en un corto plazo	10
09	Existe una coordinación con la sede de Metal Mecánica en la	10

	provisión temporal de los equipos informáticos	
10	Los lineamientos estratégicos de la Institución incluyen planes de continuidad del negocio y recuperación de los daños ocasionados frente algún siniestro	06
PROMEDIO		**9,2**

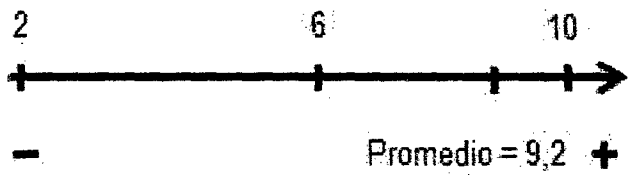
Tabla N° 28: Resultados por pregunta

Fuente: Elaboración propia

Para la obtención del puntaje se utilizó 03 criterios:

- **Si:** 10 puntos
- **Avance:** 6 puntos
- **No:** 2 puntos

El rango de puntuación se muestra a continuación:



Se consideró 2 en el extremo izquierdo, debido a que representa el puntaje mínimo que se puede ponderar a una pregunta, mientras que en el extremo derecho se consideró 10, el cual representa el puntaje óptimo (ideal).

El resultado de la aplicación de la Guía de Observación N° 07 es 9.2, el cual nos indica que la **Gestión de continuidad del negocio** es la adecuada y contribuye a mejorar la **disponibilidad de la información.**

Prueba de t student

Adicional a la aplicación de la Guía de Observación, también probaremos si es estadísticamente significativo. Esto lo lograremos a través de la prueba de t student, tal como se muestra a continuación:

Paso 1: Planteamiento de las hipótesis estadísticas

Seleccionamos la hipótesis nula y la hipótesis alternativa

H_0: $\mu = 6$: No se aplica una adecuada gestión de continuidad del negocio

Ha: $\mu > 6$: Se aplica una adecuada gestión de continuidad del negocio

Paso 2: Nivel de confianza o significancia: (95%)

$\alpha = 5\%$ (margen de error)

Paso 3: Regiones de aceptación y rechazo

Según la tabla de t student:

$t(0.95,9) = 1.833$

Si $t_0 <= 1.833$ entonces H_0 se acepta

Si $t_0 > 1.833$ entonces H_0 se rechaza

Paso 4: Cálculos

Las fórmulas para calcular el valor del t student y la desviación estándar de la muestra, son las siguientes:

$$S = \sqrt{\frac{\sum_{i=1}^{N} (X_i - \bar{X})^2}{N}}$$

$$t = \frac{\bar{X} - \mu}{S} \sqrt{N-1}$$

Donde:

t : Fórmula estadística t de Student

S : Desviación estándar

N : Número de elementos

$\bar{X}$: Media obtenida

μ : Media estadística

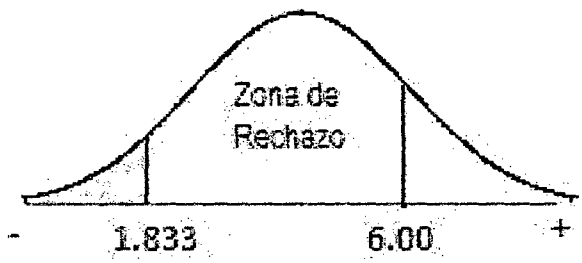
Entonces para:

N= 10 $\bar{X}$= 9,2 μ= 6

Calculamos la desviación estándar **S= 1,60**

Por lo tanto $\mathbf{t_0 = 6,00}$

$\mathbf{t_0}$ = 6,00 > 1.833 entonces H_0 se rechaza



Paso 5: Conclusión

Como el resultado no cae en la zona de aceptación ($\mathbf{t_0}$ > 1.833) se rechaza la hipótesis nula y se acepta la hipótesis alternativa, por lo tanto podemos decir que ante la hipótesis "El Sistema de Gestión permite mejorar la Seguridad de la Información en la Institución Servicios Industriales de la Marina" el indicador **disponibilidad de la información** es **válido,** ya que está demostrado.

5.1.3 Indicador 3

y3: Integridad de la información

a) **Clasificación y control de activos**

Resultado:

Para la aplicación de la Guía de Observación N° 01 se utilizó las preguntas de la tabla (Anexo 01), con la finalidad de establecer un promedio de las preguntas en relación a las respuestas y el tamaño de la muestra.

El resultado se muestra a continuación:

N°	Pregunta	Puntaje
01	El software operativo se encuentra clasificado en base a algún criterio	10
02	Se conoce la cantidad de software con la que cuenta la Institución	10
03	Se conoce la cantidad de software que se actualizó mediante upgrade	10
04	Conoce el número de computadoras operativas e inoperativas	10
05	Conoce el número de impresoras por tipo con los que cuenta la Institución	10
06	Los servidores se encuentran clasificados de acuerdo a su nivel de importancia frente a algún siniestro	10
07	Para el almacenamiento del backup se utilizó algún criterio de clasificación, el cual asegure su disponibilidad, integridad y confidencialidad	06
08	La documentación de los sistemas informáticos se controla periódicamente	10
09	Revisa o recopila información sobre controles de seguridad para respaldar los activos informáticos	06
10	En caso de producirse algún siniestro sabe qué tipo de documentación tiene que respaldar primeramente	10
PROMEDIO		**9,2**

Tabla N° 29: Resultados por pregunta

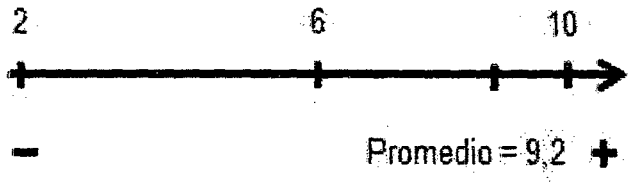
Fuente: Elaboración propia

Para la obtención del puntaje se utilizó 03 criterios:

- **Si:** 10 puntos
- **Avance:** 6 puntos

- **No:** 2 puntos

El rango de puntuación se muestra a continuación:



Se consideró 2 en el extremo izquierdo, debido a que representa el puntaje mínimo que se puede ponderar a una pregunta, mientras que en el extremo derecho se consideró 10, el cual representa el puntaje óptimo (ideal).

El resultado de la aplicación de la Guía de Observación N° 07 es 9.2, el cual nos indica que la **Clasificación y control de activos** es la adecuada y contribuye a mejorar la **integridad de la información**.

Prueba de t student

Adicional a la aplicación de la Guía de Observación, también probaremos si es estadísticamente significativo. Esto lo lograremos a través de la prueba de t student, tal como se muestra a continuación:

Paso 1: Planteamiento de las hipótesis estadísticas

Seleccionamos la hipótesis nula y la hipótesis alternativa

H_0: $\mu = 6$: No se aplica una adecuada clasificación y control de activos

Ha: $\mu > 6$: Se aplica una adecuada clasificación y control de activos

Paso 2: Nivel de confianza o significancia: (95%)

$\alpha = 5\%$ (margen de error)

Paso 3: Regiones de aceptación y rechazo

Según la tabla de t student:

$t(0.95,9) = 1.833$

Si $\mathbf{t_0}$ <= 1.833 entonces H_0 se acepta

Si $\mathbf{t_0}$ > 1.833 entonces H_0 se rechaza

Paso 4: Cálculos

Las fórmulas para calcular el valor del t student y la desviación estándar de la muestra, son las siguientes:

$$S = \sqrt{\frac{\sum_{i=1}^{N} (X_i - \bar{X})^2}{N}}$$

$$t = \frac{\bar{X} - \mu}{S} \sqrt{N-1}$$

Donde:

t : Formula estadística t de Student

S : Desviación estándar

N : Número de elementos

$\bar{X}$: Media obtenida

μ : Media estadística

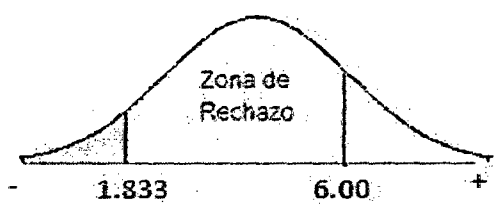
Entonces para:

N= 10 $\bar{X}$= 9,2 μ= 6

Calculamos la desviación estándar **S= 1,60**

Por lo tanto $\mathbf{t_0}$ **= 6,00**

$\mathbf{t_0}$ = 6,00 > 1.833 entonces H_0 se rechaza



Paso 5: Conclusión

Como el resultado no cae en la zona de aceptación ($t_0 > 1.833$) se rechaza la hipótesis nula y se acepta la hipótesis alternativa, por lo tanto podemos decir que ante la hipótesis "El Sistema de Gestión permite mejorar la Seguridad de la Información en la Institución Servicios Industriales de la Marina" el indicador **integridad de la información** es **válido**, ya que está demostrado.

b) **Control de accesos**

Resultado:

Para la aplicación de la Guía de Observación N° 05 se utilizó las preguntas de la tabla (Anexo 05), con la finalidad de establecer un promedio de las preguntas en relación a las respuestas y el tamaño de la muestra.

El resultado se muestra a continuación:

N°	Pregunta	Puntaje
01	Está definido las actividades a realizarse cuando un usuario de servicios informáticos cesa de la Institución	10
02	Existe un registro actualizado de las altas y bajas de usuarios, el cual permita mostrar información de historial de usuarios	10
03	Existe un registro de perfiles y accesos de los usuarios a los servicios informáticos operativos	10
04	Existe una clasificación de perfiles para el acceso a la información en base a las áreas de la Institución	10
05	Los accesos a los sistemas informáticos se han brindado siempre en función a las actividades del usuario solicitante	06
06	Las contraseñas de usuarios para el acceso a los sistemas informáticos son seguras, teniendo en cuenta la información que procesan y almacenan	10
07	Existe algún control que brinde seguridad adecuada a los	10

	documentos (memorándum), que contienen información de acceso a servicios informáticos	
08	La alta de servicios informáticos cuenta con un procedimiento establecido a fin de evitar brindar acceso antes de tener todas las aprobaciones correspondientes	10
09	Los archivos utilizados para almacenar contraseñas de acceso a los diferentes servicios informáticos se encuentran protegidos	10
10	Existe algún procedimiento para controlar el acceso a la red Institucional	10
	TOTAL	**96**

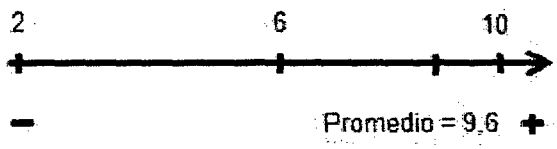
Tabla N° 30: Resultados por pregunta

Fuente: Elaboración propia

Para la obtención del puntaje se utilizó 03 criterios:

- **Si:** 10 puntos
- **Avance:** 6 puntos
- **No:** 2 puntos

El rango de puntuación se muestra a continuación:



Se consideró 2 en el extremo izquierdo, debido a que representa el puntaje mínimo que se puede ponderar a una pregunta, mientras que en el extremo derecho se consideró 10, el cual representa el puntaje óptimo (ideal).

El resultado de la aplicación de la Guía de Observación N° 05 es 9.6, el cual nos indica que el **Control de accesos** es el adecuado y contribuye a mejorar la **integridad de la información.**

Prueba de t student

Adicional a la aplicación de la Guía de Observación, también probaremos si es estadísticamente significativo. Esto lo lograremos a través de la prueba de t student, tal como se muestra a continuación:

Paso 1: Planteamiento de las hipótesis estadísticas

Seleccionamos la hipótesis nula y la hipótesis alternativa

H_0: $\mu = 6$: No se aplica un adecuado control de accesos

Ha: $\mu > 6$: Se aplica un adecuado control de accesos

Paso 2: Nivel de confianza o significancia: (95%)

$\alpha = 5\%$ (margen de error)

Paso 3: Regiones de aceptación y rechazo

Según la tabla de t student:

$t(0.95,9) = 1.833$

Si $\mathbf{t_0} <= 1.833$ entonces H_0 se acepta

Si $\mathbf{t_0} > 1.833$ entonces H_0 se rechaza

Paso 4: Cálculos

Las fórmulas para calcular el valor del t student y la desviación estándar de la muestra, son las siguientes:

$$S = \sqrt{\frac{\sum_{i=1}^{N} (X_i - \bar{X})^2}{N}}$$

$$t = \frac{\bar{X} - \mu}{S} \sqrt{N-1}$$

Donde:

t : Formula estadística t de Student

S : Desviación estándar

N : Número de elementos

$\bar{X}$: Media obtenida

μ : Media estadística

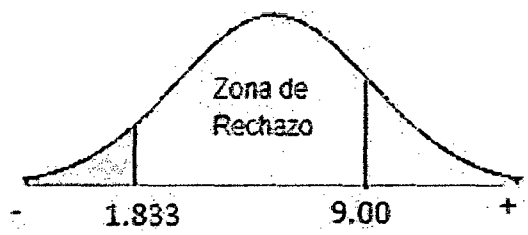
Entonces para:

N= 10 $\bar{X}$= 9,6 μ= 6

Calculamos la desviación estándar **S= 1,20**

Por lo tanto $\mathbf{t_0 = 9{,}00}$

$\mathbf{t_0}$ = 9,00 > 1.833 entonces H_0 se rechaza



Paso 5: Conclusión

Como el resultado no cae en la zona de aceptación ($\mathbf{t_0}$ > 1.833) se rechaza la hipótesis nula y se acepta la hipótesis alternativa, por lo tanto podemos decir que ante la hipótesis "El Sistema de Gestión permite mejorar la Seguridad de la Información en la Institución Servicios Industriales de la Marina" el indicador **integridad de la información** es **válido**, ya que está demostrado.

CAPÍTULO VI

CONCLUSIONES

6.1 Conclusión General

- Se mejoró en 58% la Seguridad de la Información en la Institución Servicios Industriales de la Marina, a través de la implementación de los procesos del Sistema de Gestión de Seguridad de la Información.

6.2 Conclusiones Específicas

- Se utilizó la metodología PDCA, el cual permitió implementar adecuadamente el Sistema de Gestión de Seguridad en los Servicios Industriales de la Marina.

- Se capacitó a todos los usuarios de los servicios informáticos sobre temas relacionadas a la Seguridad de la Información, logrando disminuir la pérdida de información en las diferentes divisiones de los Servicios Industriales de la Marina. (C)

- Se establecieron y supervisaron los niveles de accesibilidad a los sistemas de información, logrando implementar niveles de seguridad desde el acceso a los sistemas hasta su procesamiento. (C)

- Se actualizó el Plan de Contingencias, logrando preparar y capacitar al personal de la DTI frente a algún desastre que pueda interrumpir la continuidad de los servicios informáticos. (D)

- Se establecieron controles de seguridad (entrada, proceso y salida) en todos los sistemas de información operativos, logrando alinear los procesos con la seguridad de la información. (I)

- Se implementaron niveles de seguridad en el uso y creación de las contraseñas de acceso a los diferentes servicios informáticos, logrando brindar una adecuada seguridad a toda la información almacenada en los equipos informáticos. (I)

- Se realizó una clasificación de los activos informáticos (servidores, backup, software y documentación) de acuerdo al nivel de importancia para la Empresa, ya que representa un recurso de gran importancia para la Institución. (I)

- Se estableció el procedimiento para la baja de usuarios de los servicios informáticos, logrando disminuir el tiempo de baja los usuarios que se desvinculan de la Institución. (I)

- Se emplearon normas relacionadas a la seguridad de la información, para lograr una adecuada implementación del Sistema de Gestión de Seguridad en los Servicios Industriales de la Marina.

- Se logró disminuir el número de observaciones en las auditorías que realiza la Oficina de Gestión de Control, gracias a la implementación de las medidas y controles de seguridad de la información en los diferentes procesos de la División de Tecnologías de la Información.

CAPÍTULO VII

RECOMENDACIONES

- Contratar periódicamente la asesoría de consultoras de seguridad de la información, con la finalidad de seguir mejorando los procesos informáticos de los Servicios Industriales de la Marina.

- Planificar reuniones periódicas entre el equipo de la División de Tecnologías de la Información, lideras por el Jefe de la DTI y los Analistas de Seguridad de la Información.

- Continuar con el programa de capacitación a los usuarios de los servicios informáticos, con la finalidad de seguir mejorando la seguridad de la información.

- Investigar e implementar nuevos controles de seguridad en los diferentes procesos de seguridad de la información.

- Incluir partidas presupuestarias por parte del Jefe de la Oficina Estratégica, con la finalidad de mejorar los activos informáticos de la DTI.

- Continuar con la implementación de nuevas medidas de seguridad en el Plan de Contingencias, con la finalidad de evitar pérdidas e interrupciones de los servicios informáticos de la Institución.

- Continuar con la realización de simulacros internos, la cual sirva para brindar una mejor capacitación y entrenamiento al personal de la DTI.

- Brindar todas las facilidades a la Oficina de Control de Gestión en las auditorías que realiza, con la finalidad disminuir las observaciones encontradas y seguir todas las recomendaciones indicadas.

REFERENCIA BIBLIOGRÁFICA

Areitio, J. (2009). "Seguridad de la Información: Redes, Informática y SI". Cengage Learning-Paraninfo.

Areitio, J. (2006). "Análisis en torno a la auditoria de seguridad en tecnologías de la información y las comunicaciones". REE. Nº 625.

Areitio, J. (2009). "Test de penetración y gestión de vulnerabilidades, estrategias clave para evaluar la seguridad de red". REE. Nº 653.

Areitio, J. (2005). "Tipificación de amenazas, identificación de contramedidas de seguridad en el ámbito de gestión de redes y sistemas". REE. Nº 613.

Areitio, J. (2008). Seguridad de la Información. Barcelona. Paraninfo.

Daltabuit, E., Hernández, L., Mallén, G. & V, José. (2007). La Seguridad de la Información. México. Limusa.

Indacochea, A. (2005). Una propuesta para mejorar las prácticas de Gobierno Corporativo en el Perú. Pontificia Universidad Católica del Perú. Recuperado de http://centrum.pucp.edu.pe/docentes/AIndacochea_Libros/documentos_publicados/Gobierno_Corporativo.pdf.

Piattini, M. y Del Peso, E. (2001). Auditoría Informática. Un enfoque práctico, (2ª ed.). México. Alfaomega RA-MA.

H, Enrique. (1996). Auditoría en informática un enfoque metodológico, (1ª ed.). México. McGraw Hill Editorial.

Herzog, P. (2003). Metodología Abierta de Testeo de Seguridad 2.1, Institute for Security and Open Methodologies.

Stuart, Mc (2003). Hacking Exposed: Network Security, 4th edition. McGraw-Hill

Siles, R. (2003). Hacking TCP/IP, EE.UU

Siles, R. (2003). GNU Free Software Foundation, EE.UU

Zwicky, T. (2004). Building Internet Firewalls, EE.UU: O'Relly Media Inc.

Klarp, J. (2000). How to Conduct a Security Audit, PC Network Advisor

Cresson, Ch. (2002). Information Security Police Made Easy, EE.UU, Pentasafe

D, Sullivan. (2004). The Definite Guide to Security Management, Computer Associates

M, Juarez. (2000). La Seguridad de Información, Grupo Ibermática, N° 93

L, Anzola. (2008). IT Governance Regulation – A Latin American Perspective de Information Systems Control Journal

S, Hamaker. (2005). Enterprise Governance and the Role of IT, Information Systems Control Journal

M, Parkinson. (2005). IT and Enterprise Governance, Information Systems Control Journal

A, Servat. (2007). Diseño de un sistema de gestión de seguridad de información, Óptica ISO 27001:2005, Primera edición, México

J, Cano. (2011). El Debido Cuidado en Seguridad de Información. Un ejercicio de virtudes para el responsable de la Seguridad de Información

WEBLOGRAFÍA

NTP-ISO/IEC 17799:2007 (2007). Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la Información.
Disponible en:
http://www.bvindecopi.gob.pe/normas/isoiec17799.pdf
Consultado el 24 de Agosto del 2013.

COBIT 4.1 (2007). Entregar y dar soporte. Garantizar la seguridad de los sistemas.
Disponible en:
http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf
Consultado el 24 de Agosto del 2013.

ONGEI (2005). Auditoria de Sistemas.
Disponible en:
http://www.ongei.gob.pe/publica/metodologias/Lib5002/libro.htm
Consultado el 24 de Agosto del 2013.

ONGEI (2005). Plan de contingencias y seguridad de la Información.
Disponible en:
http://www.ongei.gob.pe/publica/metodologias/Lib5007/libro.htm
Consultado el 24 de Agosto del 2013.

INEI (2007). Recomendaciones técnicas para la seguridad e integridad de la información que se procesa en la Administración Pública.
Disponible en:
http://www.ongei.gob.pe/publica/metodologias/lib5082/cap03.htm
Consultado el 24 de Agosto del 2013.

INEI (2006). Normas técnicas para el almacenamiento y respaldo de la información que se procesan en las Entidades del Estado.
Disponible en:

http://www.ongei.gob.pe/publica/metodologias/lib5082/cap01.htm
Consultado el 24 de Agosto del 2013.

INEI (2006). Normas y procedimientos técnicos para garantizar la seguridad de la información publicadas por las Entidades de la Administración Pública.
Disponible en:
http://www.ongei.gob.pe/publica/metodologias/lib5082/cap01.htm
Consultado el 24 de Agosto del 2013.

J, Miller (2013). Sistema de Gestión de la Seguridad de la Información.
Disponible en:
http://es.wikipedia.org/wiki/Sistema_de_Gesti%C3%B3n_de_la_Seguridad_de_la_Informaci%C3%B3n
Consultado el 24 de Agosto del 2013.

J, Miller (2013). Seguridad de la Información.
Disponible en:
http://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n
Consultado el 24 de Agosto del 2013.

B, Ignacio. (2004). Confidencialidad, Disponibilidad e Integridad de la información.
Disponible en:
http://www.belt.es/expertos/experto.asp?id=2245
Consultado el 24 de Agosto del 2013.

ANEXO 01

GUIA DE OBSERVACIÓN N° 01 – CLASIFICACION Y CONTROL DE ACTIVOS

N°	Pregunta	Si	No	Avance
01	El software operativo se encuentra clasificado en base a algún criterio		X	
02	Sabe la cantidad de software con la que cuenta la Institución		X	
03	Sabe la cantidad de software que se actualizó mediante upgrade	X		
04	Conoce el número de computadoras operativas e inoperativas		X	
05	Conoce el número de impresoras por tipo con los que cuenta la Institución	X		
06	Los servidores se encuentran clasificados de acuerdo a su nivel de importancia frente a algún siniestro			X
07	Para el almacenamiento del backup se utilizó algún criterio de clasificación, el cual asegure su disponibilidad, integridad y confidencialidad		X	
08	La documentación de los sistemas informáticos se controla periódicamente		X	
09	Revisa o recopila información sobre controles de seguridad para respaldar los activos informáticos		X	
10	En caso de producirse algún siniestro sabe qué tipo de documentación tiene que respaldar primeramente		X	

ANEXO 02

GUIA DE OBSERVACIÓN N° 02 – SEGURIDAD LIGADA AL PERSONAL

N°	Pregunta	Si	No	Avance
01	Existe algún acuerdo de confidencialidad de información para personal nuevo dentro del área		X	
02	Se incluyen charlas relacionadas a seguridad de la información en las inducciones a nuevo personal		X	
03	Existe algún control para asegurar que la información no sea comprometida en los trabajos de personal tercero			X
04	Es consciente de las amenazas y riesgos en el ámbito de la seguridad de la información		X	
05	Existe algún procedimiento de entrenamiento al personal sobre la adecuada manipulación de los equipos informáticos		X	
06	Sabe que hacer en caso de presentarse alguna fuga o robo de información en el área		X	
07	El cese de personal incluye actividades de verificación de la seguridad de la información, durante el tiempo de permanencia			X
08	Se analizan y solucionan los errores producidos por mala manipulación de información		X	
09	Existe planificación alguna de como difundir en la Institución las nociones de seguridad de la información		X	
10	Dentro de las sanciones al personal se encuentra incluido aquellas relacionadas con la pérdida o robo de información confidencial		X	

ANEXO 03

GUIA DE OBSERVACIÓN N° 03 – SEGURIDAD FISICA Y DEL ENTORNO

N°	Pregunta	Si	No	Avance
01	El acceso a las instalaciones de la DTI permite el ingreso de personal interno como externo por diferentes situaciones		X	
02	Existen dispositivos de seguridad (cámaras, alarmas, etc.) instalados en puntos estratégicos del área o de la Institución		X	
03	En los meses de producción hay algún resguardo adicional debido a la presencia de una gran cantidad de personal tercero		X	
04	Existe una bitácora con información de fecha, hora y motivo de ingreso de personal externo al área			X
05	La estructura física que contiene los equipos de comunicaciones es la adecuada en relación la información que almacena		X	
06	La DTI tiene señalizaciones adecuadas para diferenciar las diferentes áreas internas (desarrollo, soporte técnico, etc.)		X	
07	El personal de la DTI cuenta con capacitación sobre uso adecuado de extinguidores frente a posibles incendios dentro de las instalaciones			X
08	Dentro de la DTI se diferencia las áreas seguras e inseguras, en caso de producirse algún siniestro		X	
09	El cableado eléctrico implementado para los equipos de comunicaciones es adecuado	X		
10	Los equipos computacionales tienen una adecuado plan de mantenimiento para evitar fallas eléctricas al personal		X	

ANEXO 04

GUIA DE OBSERVACIÓN N° 04 – GESTION DE COMUNICACIONES Y OPERACIONES

N°	Pregunta	Si	No	Avance
01	Existe definido procedimientos necesarios para una correcta operación de los equipos informáticos		X	
02	Se realizan capacitaciones periódicas a los usuarios de los servicios informáticos (sobre diversos temas)			X
03	Existe un procedimiento de comunicación de incidentes relacionados a sistemas o equipos informáticos		X	
04	La información perdida por un falla en el funcionamiento de un sistema o equipo informático es recuperada		X	
05	Existe una adecuada coordinación entre los Analistas de Sistemas y usuarios con respecto al uso de los sistemas informáticos		X	
06	La información se encuentra sincronizada y actualizada en todos los sistemas informáticos de la DTI			X
07	Se ejecutan revisiones a los sistemas después de un mantenimiento finalizado para comprobar que no se ha alterado los controles de seguridad de la información			X
08	Operacionalmente un sistema informático después de un mantenimiento solicitado, sigue manteniendo los mismo objetivos por los cuales fue diseñado	X		
09	Se realizan verificaciones periódicas sobre los equipos de cómputo a fin de evitar el uso o instalación de software no licenciado			X
10	El proceso de desinfección de medios extraíbles de usuarios se realizan en todo momento		X	

ANEXO 05

GUIA DE OBSERVACIÓN N° 05 – CONTROL DE ACCESOS

N°	Pregunta	Si	No	Avance
01	Está definido las actividades a realizarse cuando un usuario de servicios informáticos cesa de la Institución			X
02	Existe un registro actualizado de las altas y bajas de usuarios, el cual permita mostrar información de historial de usuarios		X	
03	Existe un registro de perfiles y accesos de los usuarios a los servicios informáticos operativos		X	
04	Existe una clasificación de perfiles para el acceso a la información en base a las áreas de la Institución		X	
05	Los accesos a los sistemas informáticos se han brindado siempre en función a las actividades del usuario solicitante		X	
06	Las contraseñas de usuarios para el acceso a los sistemas informáticos son seguras, teniendo en cuenta la información que procesan y almacenan			X
07	Existe algún control que brinde seguridad adecuada a los documentos (memorándum), que contienen información de acceso a servicios informáticos		X	
08	La alta de servicios informáticos cuenta con un procedimiento establecido a fin de evitar brindar acceso antes de tener todas las aprobaciones correspondientes			X
09	Los archivos utilizados para almacenar contraseñas de acceso a los diferentes servicios informáticos se encuentran protegidos		X	
10	Existe algún procedimiento para controlar el acceso a la red Institucional		X	

ANEXO 06

GUIA DE OBSERVACIÓN Nº 06 – ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Nº	Pregunta	Si	No	Avance
01	Se utiliza más de un criterio de validación de datos en el procesamiento de la información de los sistemas informáticos			X
02	Todos los sistemas informáticos implementan rutinas de recuperación de datos, a fin de evitar procesamientos erróneos o incompletos de información		X	
03	Existe un registro actualizado de los errores producidos por los sistemas informáticos, en los cuales se haya perdido una gran cantidad información para su posterior revisión y solución		X	
04	Se realizan revisiones periódicas a los sistemas informáticos en producción, a fin de garantizar que cumplen con los objetivos iniciales e implementan los controles de seguridad adecuados		X	
05	Todas las modificaciones solicitadas por los usuarios se realizan en un ambiente de prueba y luego se ejecutan en el ambiente de producción			X
06	Existe una asignación de los sistemas informáticos por cada Analista de Sistemas, para que estos se hagan responsable de su implementación y mantenimiento; en la cual el acceso al código fuente se encuentra restringido		X	
07	Los archivos de datos se encuentran debidamente documentados y almacenados, debido a las migraciones realizadas			X
08	La implantación de código ejecutable en los equipos de cómputo siempre se realiza luego de concluir con todas las pruebas respectivas		X	
09	Se realiza una coordinación adecuada entre el personal de soporte técnico para la configuración de los archivos y software necesario			X
10	Se autoriza el copiado de información en producción a ambientes de prueba o viceversa		X	

ANEXO 07

GUIA DE OBSERVACIÓN Nº 07 – GESTION DE CONTINUIDAD DEL NEGOCIO

Nº	Pregunta	Si	No	Avance
01	Se tiene identificado todos los riesgos a los que está expuesto la DTI			X
02	De los riesgos identificados, se ha elaborada el conjunto de acciones necesarias a realizar para su mitigación		X	
03	Se tiene definido el grupo de trabajo y las actividades a realizar en caso de presentarse algún siniestro en la DTI o en la Institución			X
04	Se planifican entrenamientos del personal a través de simulacros internos del área, con la finalidad de que se pongan en práctica las acciones a realizar en caso de un siniestro		X	
05	Se tiene un presupuesto asignado para una posible recuperación de los activos informáticos de la Institución		X	
06	La Jefatura de la Institución tiene alcance de los riesgos a los que se encuentran expuestos los equipos de informáticos y el impacto que éstos pueden ocasionar		X	
07	Existe una coordinación con las áreas de seguridad y patrimonio para que brinden su apoyo en caso de presentarse un siniestro en la DTI (incendio, corto circuito, explosiones, etc.)			X
08	Existe una coordinación con los proveedores de servicios para que restauren los servicios interrumpidos en un corto plazo		X	
09	Existe una coordinación con la sede de Metal Mecánica en la provisión temporal de los equipos informáticos			X
10	Los lineamientos estratégicos de la Institución incluyen planes de continuidad del negocio y recuperación de los daños ocasionados frente algún siniestro		X	

ANEXO 08

ACUERDO DE CONFIDENCIALIDAD PERSONAL INTERNO

Como parte de la política de seguridad de la información de los Servicios Industriales de la Marina Chimbote, tenemos al Sr. Capitán de Fragata _____, Jefe de Sima Chimbote y por otro lado al Sr (a). _____con PR _____, desempeña el cargo de _____ en la División de _____, se ha acordado celebrar el presente Acuerdo de Confidencialidad que se regirá por las siguientes cláusulas:

CONSIDERACIONES

1. Debido a la naturaleza del trabajo, se hace necesario que se maneje información confidencial y/o información sujeta a derechos de propiedad intelectual, antes, durante y en la etapa posterior.

CLÁUSULAS

PRIMERA

OBJETO. El objeto del presente acuerdo es fijar los términos y condiciones bajo los cuales las partes mantendrán la confidencialidad de los datos e información intercambiados entre ellas, incluyendo información objeto de derecho de autor, patentes, técnicas, modelos, invenciones, procesos, algoritmos, programas, ejecutables, investigaciones, detalles de diseño, información financiera, lista de clientes, inversionistas, empleados, relaciones de negocios y contractuales y cualquier información revelada sobre terceras personas.

SEGUNDA

CONFIDENCIALIDAD. Las partes acuerdan que cualquier información intercambiada, facilitada o creada entre ellas en el tiempo que el personal labore en la Institución, será mantenida en estricta confidencialidad. La parte receptora correspondiente solo podrá revelar información confidencial a quienes la necesiten y estén autorizados previamente por la parte de cuya información confidencial se trata. Se considera también información confidencial: a)

Aquella que como conjunto o por su naturaleza, no sea conocida entre el resto de personal. b) La que no sea de fácil acceso, y c) Aquella información que esté sujeta a medidas de protección razonables, de acuerdo con las circunstancias del caso, a fin de mantener su carácter confidencial.

TERCERA.

EXCEPCIONES. No habrá deber alguno de confidencialidad en los siguientes casos: a) Cuando la parte receptora tenga evidencia de que conoce previamente la información recibida; b) Cuando la información recibida sea de dominio público y, c) Cuando la información deje de ser confidencial por ser revelada al resto de personal.

CUARTA.

DURACION. Este acuerdo regirá durante todo el tiempo que el personal labore en la Institución

QUINTA.

DERECHOS DE PROPIEDAD. Toda información intercambiada es de propiedad exclusiva de la Institución. En consecuencia, ninguna de las partes utilizará información de la otra para su propio uso.

SEXTA.

MODIFICACIÓN. Este acuerdo solo podrá ser modificado por el Jefe de Sima Chimbote, y este se encargará de comunicar al personal responsable para su respectiva difusión y publicación en los medios utilizados actualmente.

Chimbote, ___ de _____ de _____

_____ Jefe Sima Chimbote

_____ Trabajador

ANEXO 09

ACUERDO DE CONFIDENCIALIDAD PERSONAL EXTERNO

Como parte de la política de seguridad de la información de los Servicios Industriales de la Marina Chimbote, tenemos al Sr. Capitán de Fragata _____, Jefe de Sima Chimbote y por otro lado al Sr (a). _____con DNI N° _____, razón social _____ RUC N° _____, se ha acordado celebrar el presente Acuerdo de Confidencialidad que se regirá por las siguientes cláusulas:

CONSIDERACIONES

1. Debido a la naturaleza del trabajo, se hace necesario u opcional que se maneje información confidencial y/o información sujeta a derechos de propiedad intelectual, dependiendo de las actividades a realizar dentro de la Institución.

CLÁUSULAS

PRIMERA

OBJETO. El objeto del presente acuerdo es fijar los términos y condiciones bajo los cuales las partes mantendrán la confidencialidad de los datos e información intercambiados entre ellas, incluyendo información objeto de derecho de autor, patentes, técnicas, modelos, invenciones, procesos, algoritmos, programas, ejecutables, investigaciones, detalles de diseño, información financiera, lista de clientes, inversionistas, empleados, relaciones de negocios y contractuales y cualquier información revelada sobre terceras personas.

SEGUNDA

CONFIDENCIALIDAD. Las partes acuerdan que cualquier información intercambiada, facilitada o creada entre ellas en el tiempo que se labore en la Institución, será mantenida en estricta confidencialidad. Se considera también información confidencial: a) Aquella que como conjunto o por su naturaleza, no sea conocida entre el resto de personal. b) La que no sea de fácil acceso, y c) Aquella información que esté sujeta a medidas de protección

razonables, de acuerdo con las circunstancias del caso, a fin de mantener su carácter confidencial.

TERCERA.

EXCEPCIONES. No habrá deber alguno de confidencialidad en los siguientes casos: a) Cuando la parte receptora tenga evidencia de que conoce previamente la información recibida; b) Cuando la información recibida sea de dominio público y, c) Cuando la información deje de ser confidencial por ser revelada al resto de personal.

CUARTA.

DURACION. Este acuerdo regirá durante todo el tiempo que se realicen labores en la Institución

QUINTA.

DERECHOS DE PROPIEDAD. Toda información intercambiada es de propiedad exclusiva de la Institución. En consecuencia, ninguna de las partes utilizará información de la otra para su propio uso.

SEXTA.

MODIFICACIÓN. Este acuerdo solo podrá ser modificado por el Jefe de Sima Chimbote, y este se encargará de comunicar al personal tercero por el medio utilizado actualmente en la Institución.

Chimbote, ___ de _____ de _____

_____	_____
Jefe Sima Chimbote	Personal Tercero

ANEXO 10

REGISTRO DE CAPACITACION EN SEGURIDAD DE LA INFORMACION

SIMA	FORMATO	Codigo:	F-03-01-01
		Version:	01
	CAPACITACION EN SEGURIDAD DE LA INFORMACION	Fecha:	15-10-11
		Pagina	1 - 1

1. DATOS DE CAPACITACION

Usuario:	
Area/Cargo:	
Fecha	
Capacitador/Cargo:	

2. SERVICIOS INFORMATICOS (Marcar con X lo capacitado)

a. Sistema informático	
b. Correo electrónico	
c. Paginas web	
d. Intranet	
e. Antivirus	
f. Confidencialidad	

3. CONFORMIDAD DE LA CAPACITACION

Capacitador

Trabajador

Jefe DTI

ANEXO 11

REGISTRO DE INGRESO DE PERSONAL EXTERNO A LA DTI

SIMA	REGISTRO
	INGRESO DE PERSONAL EXTERNO A LA DTI

Nº	Nombres/Razón Social	Fecha	Ingreso	Salida	Motivo

ANEXO 12

REGISTRO DE INCIDENTES EN HORARIO ANORMAL

SIMA	REGISTRO
	INCIDENTES EN HORARIO ANORMAL

Nº	Fecha	Hora	Incidente

ANEXO 13

REGISTRO DE CAPACITACION DE PROCESOS INFORMATIVOS OPERATIVOS

SIMA	REGISTRO
	CAPACITACION DE PROCESOS INFORMATICOS OPERATIVOS

OFICINA	
JEFE	
DIVISION	
JEFE	
FECHA	
PROCESOS	

Nº	Apellidos y Nombres	Cargo	PR	Firma

ANEXO 14

REGISTRO DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

SIMA	REGISTRO
	INCIDENTES DE SEGURIDAD DE LA INFORMACION

Nº	Fecha	Hora	Incidente

ANEXO 15

REGISTRO DE BACKUP SEMANAL

SIMA	REGISTRO
	BACKUP SEMANAL

Nº	Fecha	Hora	Correlativo	Responsable	Observación

ANEXO 16

REGISTRO DE INGRESO Y/O SALIDA DE INFORMACION

SIMA	REGISTRO
	INGRESO Y/O SALIDA DE INFORMACION

Nº	Fecha	Tipo	Descripción	Usuario	Observación

ANEXO 17

REGISTRO DE ALTA/BAJA DE USUARIOS

SIMA	REGISTRO
	ALTA/BAJA DE USUARIOS

Nº	Fecha	Tipo	Usuario	PR	Servicios asignados/removidos

ANEXO 18

CLASIFICACIÓN DE SISTEMAS DE INFORMACIÓN POR OFICINAS/DIVISIONES

Estratégica	Financiera	Integrada	Logística	Personal
Backup	Backup	Backup	Backup	Backup
Registro de llamadas	Registro de llamadas	Registro de llamadas	Registro de llamadas	Registro de llamadas
Requerimiento de oficina	Requerimiento de oficina	Calidad	Calidad	Requerimiento de oficina
	Contabilidad de costos	Requerimiento de oficina	Guías de emisión	Personal
	Contabilidad general	Mantenimiento	Control de pañoles	
	Tesorería	Producción	Requerimiento de oficina	
			Mantenimiento	
			Control patrimonial	
			Logístico	
			Producción	
			Comercial	

ANEXO 19

ESQUEMA DE SEGURIDAD PARA CONTRASEÑAS

I. ACCESO A LAS COMPUTADORAS (Nivel I)

a) Áreas que manejan información confidencial

Áreas	Requisitos de contraseña
División de TIC División de Remun. Control División de Contabilidad División de Tesorería	-Longitud: 8 caracteres -Complejidad: las contraseñas deben incluir mayúsculas (3), números (3) y caracteres especiales (2). -No deben contener datos personales -Frecuencia de cambio: 06 meses

b) Áreas que no manejan información confidencial

Áreas	Requisitos de contraseña
Todas las áreas a excepción de las expuestas en el cuadro a)	-Longitud: 8 caracteres -Complejidad: las contraseñas deben incluir mayúsculas (3), números (4) y caracteres especiales (1). -No deben contener datos personales -Frecuencia de cambio: 06 meses

II. ACCESO A LOS SISTEMAS DE INFORMACIÓN (Nivel II)

Criterio	Descripción
Longitud	8 caracteres
Complejidad	Las contraseñas deben incluir mayúsculas (1), minúsculas (2), números (4) y caracteres especiales (1) No deben contener datos personales
Frecuencia de cambio	06 meses

III. ACCESO A LOS SERVIDORES (Nivel III)

Criterio	Descripción
Longitud	14 caracteres
Complejidad	Las contraseñas deben incluir : -mayúsculas (4) -minúsculas (3), -números (4) -caracteres especiales (3)
Frecuencia de cambio	04 meses

ANEXO 20

REGISTRO DE AUTORIZACIÓN DE INGRESO DE EQUIPOS EXTERNOS

SIMA	REGISTRO
	AUTORIZACION DE INGRESO DE EQUIPOS EXTERNOS

N°	Fecha	Empresa/Nombre	Equipos	Jefe solicitante	Jefe DTI

ANEXO 21

REGISTRO DE AUTORIZACIÓN DE ACCESO A LA RED

SIMA	REGISTRO
	AUTORIZACION DE ACCESO A LA RED

N°	Fecha	Empresa/Nombre	Uso de servicio	Jefe solicitante	Jefe DTI

ANEXO 22

DOCUMENTOS REVISADOS DE LA DTI

CONTROL DE ASISTENCIA DE CAPACITACION

SIMA

Oficina de Personal
Dpto. Capacitación

FOC-OP-020
Rev. 1
Fecha: 2004-05-27

CONTROL DE ASISTENCIA DE CAPACITACIÓN

Fecha: ....
Hora de: .... a ....

Actividad: Capacitación uso Modulo de Evaluación Proveedores de Servicio

Institución: SIMACH

Expositor / Instructor: Ing. Milton García Llamosa

El participante deberá escribir su nombre claramente y firmar este documento, para acreditar su asistencia.

Nº	PR/Grado/Otros	Apellidos y Nombres	Área de trabajo/ Dependencia	Firma
1	5902	[illegible]	[illegible]	
2	[illegible]	[illegible]	[illegible]	
3	[illegible]	Torres Alfonso [illegible]	[illegible]	
4	5679	[illegible]	[illegible]	
5	2291	[illegible] Perez [illegible]	[illegible]	
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				

Firma del Instructor

Vº Bº
Departamento de Capacitación

REQUERIMIENTO PARA MANTENIMIENTO DE SISTEMAS

SIMA	FORMATO	Codigo:	F-02-01-01
		Version:	05
	REQUERIMIENTO PARA MANTENIMIENTO DE SISTEMAS	Fecha:	18-01-10
		Pagina:	1 -1

Nº de Requerimiento: 048 - 008 Sistema: GESTION DE CALIDAD

1. **DESCRIPCION DE REQUERIMIENTO:**

Fecha: 12/07/2010 Hora: 9:13 AM Area: JEFE TECNICO (anexo X37

Solicitante: Reinaldo Silva Trujillo Firma:

a. Modificación de datos ☐
b. Creación de nueva funcionalidad ☐
c. Modificación de funcionalidad actual ☐
d. Otros / Detalle ☒

Prioridad: ALTA / MEDIA / BAJA

Modulo: Producción Sub-Modulo: Administrar Registros de Calidad

Descripción / Observación: modificación del Tamaño del Tipo de dato de las Columnas observación 1 y Comentario con el fin de permitir guardar un máximo de 4000 Caracteres de la Tabla Registro de Calidad

2. **OPINION TECNICA (Área de Sistemas):**

La modificación es factible.

Tiempo estimado: ½ hora Tiempo real: 31 minutos

Fecha inicio desarrollo: 12/07/2010 Fecha de termino: 12/07/2010

Analista-Desarrollador: Rómulo Quevedo Ramos Firma:

Aprobación: | Si | No |

Firma: Jefe del Area Desarrollo de Sistemas

3. **RESULTADO DE PRUEBAS:**

Fecha Inicio: 12/07/2010 Fecha Fin: 12/07/2010

realización de pruebas satisfactorias

4. **IMPLEMENTACION DEL CAMBIO:**

Fecha: 12/07/2010

Ejecutado por: Rómulo Quevedo Ramos Firma:

Validado por: Responsable Firma:

Aprobado por: Santos Gabriel Blas Firma:

MEMORANDO DEPARTAMENTO DE PRODUCCIÓN

MEMORANDO Nº JDPAS-SCH-2010-331

Chimbote, 16 agosto del 2010

Al : Jefe Oficina Estratégica
Asunto : Accesos e Sistemas

1. Con relación al asunto, comunico a usted, que a fin de tener acceso a la información, solicito se efectúe los derechos a los Sistemas que se indica, para el personal de la División de Control de Calidad que se detalla a continuación:

P.R. 5928 Carlos Contreras Fajardo
Derechos Acceso Sistema de Calidad
Derechos Acceso correo electrónico
Derechos Acceso al Sistema Control de Naves : (X)Alta ( ) Baja

usar: ccontreras
personal: carlosc

P.R. 6930 Luis Cipriano De la Cruz
Derechos Acceso Sistema de Calidad
Derechos Acceso Correo electrónico
Derechos Acceso al Sistema Control de Naves : (X)Alta ( ) Baja

usar: lcipriano
personal: luisc

Capitán de Navío
Carlos Fernando MARIÑO NUEVO Ojeda
Jefe Departamento de Producción
Astillero

07 JUL 2010

Dpt. Jefe Oficina Estratégica
Copia : JDA-JDCC/
archivo/

CFMO/ECL/nsv.

RECIBIDO
MARINA GUERRA DEL PERU
17 AGO 2010
OFICINA ESTRATÉGICA

Ing. Romulo Quezada
Ing. Marco Retuerto

02-09-2010
08209

ANEXO 23

MEJORA SE SEGURIDAD DE LA INFORMACIÓN POR INDICADOR Y PROCESO

Indicador	Proceso de Seguridad de la Información	Pre test	Post test	Mejora
Confidencialidad	Seguridad física y del entorno	36%	92%	56%
Confidencialidad	Seguridad ligada al personal	28%	96%	68%
Disponibilidad	Adquisición, desarrollo y mantenimiento de sistemas	36%	92%	56%
Disponibilidad	Gestión de comunicaciones y operaciones	44%	96%	52%
Disponibilidad	Gestión de continuidad del negocio	36%	92%	56%
Integridad	Clasificación y control de activos	40%	92%	52%
Integridad	Control de accesos	32%	96%	64%
	Promedio	36%	94%	58%