UNIVERSIDAD NACIONAL AGRARIA DE LA SELVA

FACULTAD DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS

DEPARTAMENTO ACADEMICO DE CIENCIAS EN INFORMATICA Y SISTEMAS

APLICACIÓN DE LA NORMA TECNICA PERUANA ISO 17799 AL DESARROLLO DEL SISTEMA DE INFORMACIÓN DE GESTIÓN ADMINISTRATIVA SIGA MODULO LOGISTICO EN LA DIRECCIÓN SUBREGIONAL DE SALUD ALTO HUALLAGA UNIDAD EJECUTA 403 TOCACHE

TESINA

Para Optar el Titulo de:

INGENIERO EN INFORMÁTICA Y SISTEMAS

Presentado por:

VILLENA ACUÑA, José Luis

Tingo María – Perú

2015

UNIVERSIDAD NACIONAL AGRARIA DE LA SELVA

FACULTAD DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS

DEPARTAMENTO ACADEMICO DE CIENCIAS EN INFORMATICA Y SISTEMAS

APLICACIÓN DE LA NORMA TECNICA PERUANA ISO 17799 AL DESARROLLO DEL SISTEMA DE INFORMACIÓN DE GESTIÓN ADMINISTRATIVA SIGA MODULO LOGISTICO EN LA DIRECCIÓN SUBREGIONAL DE SALUD ALTO HUALLAGA UNIDAD EJECUTA 403 TOCACHE

TESINA

Para Optar el Titulo de:

INGENIERO EN INFORMÁTICA Y SISTEMAS

Presentado por:

VILLENA ACUÑA, José Luis

Tingo María – Perú

2015

T
SIS

VILLENA ACUÑA, José Luís

"Aplicación de la Norma Técnica Peruana ISO 17799 al Desarrollo del Sistema de Información de Gestión Administrativa – en la Dirección Subregional de Salud Alto Huallaga – Unidad Ejecuta 403 Tocache" 2015

66 páginas; 05 Figuras; 12 Cuadros; 05 ref.; 30 cm.
Tesina (Ingeniero en Informática y Sistemas) Universidad Nacional Agraria de la Selva Tingo María (Perú). Facultad de Ingeniería en Informática y Sistemas

1. FUNDAMENTACIÓN TEÓRICA **2. NTP –ISO/IEC 17799-2007**

3. EST. NTP ISO/IEC 17799-2007 **4. DEFINICIONES METODOLÓGICAS**

DEDICATORIA

A Dios, quién me da la vida y
me guía por mi sendero.

A mis padres:

Jesús Villena Tapara y
Máximiliana Acuña Espinoza.

Por su infinito amor, comprensión, su apoyo moral y espiritual, porque siempre anhelan verme salir adelante.

.A mis hermanos:

Gerardo, Vilma, Fredy, Martha, Elmer y Vanesa.

Por contar siempre con su comprensión y apoyo incondicional.

AGRADECIMIENTO

Mis más sinceros agradecimientos a:

Las personas que conforman la Facultad de Ingeniería en Informática y Sistemas de la UNAS, porque cada día ponen su compromiso de formar profesionales en sistemas e informática útiles para la sociedad.

Los docentes del CAPT FIIS que supieron contribuir con sus conocimientos en mi actualización profesional, asimismo al Ing. Pedro C. Trujillo Natividad, por su asesoramiento en el desarrollo de la tesina.

Dr. Rodolfo David Villalobos Valqui, Director Ejecutivo de la UE-403 Dirección Subregional de Salud Alto Huallaga Tocache, por su consideración para la realización de este respectivo trabajo.

A todo familiar, Profesor, colega y amigo, que de alguna u otra forma contribuyeron a la realización de este trabajo.

INDICE GENERAL

Página

CAPITULO III

INDICE DE CUADROS

Página

INDICE DE FIGURAS

Página

INTRODUCCIÓN

La aplicación de la norma técnica peruana ISO 17799 al desarrollo del sistema de información de gestión administrativa - SIGA ML en la Dirección Subregional de Salud Alto Huallaga – Tocache, brindara muchos beneficios por que permitirá tener el plan de contingencia de todo lo relacionado a la seguridad de la información.

La Red de Servicios de Salud Tocache, está enmarcado dentro de los Lineamientos de la Política del Sector salud, Plan Regional, acuerdos de Gestión, que tiene como eje central las actividades de prevención, promoción, recuperación y de rehabilitación de la salud de la población y las capacidades reales del aparato prestador para atender dichas necesidades, con planes y acciones que compromete al sector a establecer estrategias de trabajo suficientemente creativas y racionales que permitan focalizar y priorizar las acciones hacia los sectores de población más pobre o vulnerable, cuyos ejes principales están el logro de la equidad, la eficiencia y la calidad en la atención en salud, promoviendo el desarrollo social.

Los Lineamientos de Política Sectorial 2002-2014 y Fundamentos para el Plan Estratégico Institucional 2007-2014, señala los principios básicos en las cuáles se sustentan las acciones y resultados a alcanzar el 2014; siendo uno de los principales mecanismos para el logro de los objetivos el planeamiento sanitario que mediante las herramientas disponibles se consolidan como instrumento de gestión para reflejar el accionar de salud que realiza la Dirección Ejecutiva de la Red de Servicios de Salud de Tocache.

El Equipo de Gestión de la Dirección Subregional de Salud Tocache, ha formulado el Análisis de la Situación de Salud, sobre la base de las necesidades y problemas de las micro redes Tocache, Uchiza, Progreso y Pólvora, Hospital II-1 Tocache, así como los establecimientos de salud, además como documento de gestión institucional, cuyas acciones conllevará al cumplimiento de las metas del Plan Estratégico Institucional 2007-2014.

CAPITULO I
GENERALIDADES

1.1. ACERCA DE LA INSTITUCION

1.1.1. DESCRIPCION DE LA INSTITUCION

La Red de Servicios de Salud Tocache se crea mediante Resolución Regional N° 695 el 01 de Noviembre del año 2001 bajo la dirección del Psicólogo Roberto López Cahuaza, siendo Director Regional de Salud San Martin el Dr. Pedro Bogarin Vargas; durante la Dirección del Dr. Carlos Alberto del Aguila el 29 de diciembre del 2004 se traslada la sede administrativa con todos los equipos y mobiliarios de los ambientes del Hospital Rural de Tocache a los ambientes remodelados del ex Centro de Salud y que a la actualidad viene funcionando todo el sistema administrativo de la Unidad Ejecutora 403 - Alto Huallaga; se encuentra situada en la zona sur de la Región San Martín del territorio del Perú, ocupa el sector medio del valle formado por el río Huallaga, zona de recursos naturales que conecta la sierra sur con la selva baja, oscilando su altitud entre 300 m.s.n.m. (distrito El Pólvora) y los 2,700 m.s.n.m. (distrito de Shunte).

Actualmente la red de servicios de salud cuenta con 32 establecimientos de salud en la provincia de Tocache- San Martin.

1.1.2. UBICACIÓN GEOGRAFICA

Departamento : San Martin- Perú

Provincia : Tocache

Distrito : Tocache

Dirección : Av. Ricardo Palma N° 550

Institución : “Dirección Subregional de Salud Alto Huallaga Tocache” (DSRSAHT-UE 403).

1.1.3. BASE LEGAL

- Constitución Política del Perú.
- Ley Nº 27657, Ley del Ministerio de Salud y su Reglamento, aprobado por D.S. Nº 013-2002-SA.
- Ley Nº 28411, Ley General del Sistema Nacional de Presupuesto Público.
- Ley Nº 28522; Ley del Sistema Nacional de Planeamiento Estratégico y del Centro Nacional de Planeamiento Estratégico (CEPLAN).
- Ley Nº.27783, Ley de Bases de la Descentralización
- Ley Nº.27867, Ley Orgánica de Gobiernos Regionales, Artículos
- Ley Nº.27658, Ley Marco de la Modernización de la Gestión del Estado.
- Decreto Supremo Nº 014-2002-SA Reglamento de Organización y Funciones del Ministerio de Salud.

- Decreto Supremo N° 163-2004/EF, establece disposiciones para la mejora de la calidad del gasto público y crea el Sistema de Seguimiento y Evaluación del Gasto Público.
- Resolución Suprema N° 014-2002-SA, que aprueba los Lineamientos de Política Sectorial para el período 2002 – 2012 y Principios Fundamentales para el Plan Estratégico Sectorial del Quinquenio agosto 2001 – julio 2006.
- Resolución Directoral Nº 003-2003-EF/68.01 que aprueba la Directiva para la reformulación de los Planes Estratégicos Sectoriales Multianuales para el periodo 2004-2006.
- Resolución Directoral Nº 030-2005-EF/76.01 que aprueba la Directiva para la Programación y Formulación del Presupuesto de los Pliegos del Gobierno Nacional para el año fiscal 2006.
- Resolución Ministerial Nº 665-2004/MINSA que aprueba la directiva para la formulación, seguimiento y evaluación de los planes operativos 2005 de las entidades y dependencias del MINSA.
- Resolución Ministerial Nº 566-2005/MINSA que aprueba los lineamientos para la adecuación de la organización de las Direcciones Regionales de Salud en el marco del proceso de descentralización.
- Resolución Ministerial Nº 729-2003 SA/DM que aprueba el documento La Salud Integral: Compromiso de Todos – El Modelo de Atención Integral de Salud.

1.1.4. FUNCIONES DE LA INSTITUCION:

La Dirección Ejecutiva de la Red Ejecutora de Salud es la unidad orgánica de conducción de la Red de Salud, responsable de su dirección, conducción y gestión. Está encargada de dirigir, coordinar y supervisar su funcionamiento y administrar los recursos (humanos, financieros, y materiales) que se le asigna para el cumplimiento de sus fines; así como organizar y conducir técnica y administrativamente al hospital local y Micro redes a su cargo, así como tener responsabilidad en la gestión de los sistemas administrativos, recursos financieros, bienes, servicios y brindar soporte administrativo a las redes operativas que lo conforman.

Las funciones específicas de la Dirección Ejecutiva de la Red Ejecutora de Salud son las siguientes:

a) Dirigir la elaboración de propuestas, difusión y aplicación de prioridades sanitarias y políticas provinciales sectoriales e intersectoriales que influyen sobre la salud, tomando en consideración las políticas del desarrollo social de la región y las prioridades sanitarias nacionales y regionales.

b) Dirigir la participación de la red en la formulación, difusión, asistencia técnica, implementación, aplicación y control de modelos, metodologías, tecnologías, lineamientos, normativa y procedimientos para los procesos técnicos de organización y funcionamiento de servicios públicos de salud de las personas y servicios de salud ambiental y ocupacional; para la promoción, protección, recuperación y rehabilitación de salud de las personas, salud ambiental y ocupacional, productos farmacéuticos y afines y la atención

farmacéutica, gestión institucional de recursos humanos; suministro de medicamentos e insumos médico quirúrgicos y odontológicos, investigación en salud; gestión y mantenimiento de recursos físicos y logística en el ámbito de la red de salud; proponer adecuaciones a la DIRES.

c) Identificar y promover prioridades sanitarias, de aseguramiento público e investigación en salud en la red de salud.

d) Dirigir la aplicación de metodologías de análisis y participación en la formulación del planeamiento estratégico sectorial e institucional y operativo de salud en la región; conducir, formular, dirigir, controlar y evaluar los planes estratégicos y operativos, programas y proyectos de intervención e inversiones en salud, acuerdos de gestión y anteproyectos de presupuesto para la unidad ejecutora de salud y de su red de salud; apoyar a los gobiernos locales de su jurisdicción en la formulación de su plan estratégico sectorial de salud y elevar propuestas a la DIRES.

e) Conducir la formulación, implementación y control de propuestas de desarrollo organizacional, documentos de organización de la Red y documentos normativos de gestión en los procesos de competencia de la red de salud; dirigir, conducir y controlar la implementación de la estructura, sistemas y procesos organizacionales de las unidades orgánicas de la dirección de red de salud y sus micro redes.

f) Conducir selección de personal y designar al personal responsable de gestión de la red de salud y sus micro redes.

g) Dirigir la elaboración y elevar las solicitudes de autorización sanitaria de apertura, certificados de habilitación y acreditación y licencias de funcionamiento para los establecimientos de salud y de establecimientos farmacéuticos de su responsabilidad en la red de salud; supervisar y mantener las condiciones que las facultan.

h) Dirigir y controlar la programación, almacenamiento, distribución y control de los medicamentos e insumos médico quirúrgicos y odontológicos de su red de salud y micro redes; así como las coordinaciones para su adquisición en el nivel regional y nacional y ejecución de compras de emergencia de la unidad ejecutora de salud.

i) Conducir y controlar la organización, diseño y gestión de la red de salud, sistemas de soporte de red y de laboratorio, acciones intersectoriales y servicios de atención integral, promoción y protección de la salud de las personas, salud ambiental y ocupacional, en coordinación con los gobiernos locales.

j) Dirigir la participación de la red en la formulación de la propuesta de red de servicios, unidades de gestión, carteras de servicios de establecimientos y sistemas de soporte de red y de laboratorio para la atención integral de la salud de las personas, la salud ambiental y ocupacional para el ámbito de la red de salud.

k) Informar a las autoridades competentes sobre el incumplimiento de la permanencia de regentes en establecimientos farmacéuticos públicos y privados de su ámbito, en coordinación con los gobiernos locales.

l) Dirigir la formulación, ejecución y supervisión de planes, estrategias y acciones intersectoriales de promoción, protección y recuperación de la salud de las personas, salud ambiental y ocupacional, uso racional de medicamentos y para la prevención y control de epidemias, emergencias y desastres; proponer al gobierno regional y a los gobiernos locales de su ámbito proyectos y programas de intervención sectorial e institucional y participar en su ejecución.

m) Dirigir y controlar la planificación, programación, obtención, administración, asignación, ejecución y control de los recursos financieros para la unidad ejecutora y en la red de salud según plan y normatividad vigente; definir la disponibilidad de recursos para sus redes y Micro redes y asignar los fondos correspondientes por encargo.

n) Coordinar la identificación de proveedores de servicios de salud para el seguro público de salud, monitorear las atenciones relacionadas al aseguramiento público en salud y dar facilidades para la auditoría en la red de salud.

o) Dirigir la planificación, reclutamiento, selección, contratación, incorporación, control y desarrollo de personal de su red de salud; proponer a la DIRES el nombramiento de personal; efectuar las acciones de protección social de los recursos humanos en los servicios públicos de salud de la red.

p) Dirigir la administración del personal de los programas de internado y segunda especialización asignado a su red de salud, en concordancia con los lineamientos nacionales y regionales.

q) Dirigir la administración de las remuneraciones y pensiones y cese del personal de la red ejecutora de salud.

r) Dirigir la programación de inversiones en servicios públicos; así como la gestión y operación de proyectos de inversión pública en salud de la red de salud, según estándares establecidos; gestionar los recursos humanos requeridos para la operación de los proyectos en la unidad ejecutora.

s) Conducir la participación de la red en la definición de la organización y funcionamiento del sistema de información sanitaria del ámbito regional; así como en la adecuación y definición de su sistema de información en salud complementario al nacional y regional según las necesidades de la red; conducir la aplicación, difusión y supervisión del uso de normas y estándares de gestión de información en salud.

t) Conducir el desarrollo y mantenimiento de la plataforma tecnológica, soporte técnico y mantenimiento operativo los sistemas de información, telecomunicaciones y telemática en la red de salud, en el marco de las políticas, recomendaciones, normas y estándares nacionales y regionales.

u) Conducir la obtención, verificación, registro, ordenamiento, clasificación, consolidación, procesamiento, almacenamiento y análisis de la información para la gestión sanitaria para los procesos de su red de salud; así como la planificación y ejecución de la comunicación y difusión de información en salud para la educación de su público objetivo y gestión de los procesos institucionales de su competencia.

v) Dirigir la formulación, desarrollo, promoción, articulación de alianzas y difusión de resultados de investigación en salud; formular, desarrollar, promover, articular alianzas para los proyectos de investigación en salud.

w) Dirigir y supervisar la difusión, aplicación, promoción, formulación y cumplimiento de planes, estrategias y cumplimiento de normativa de promoción y vigilancia de los derechos y responsabilidades ciudadanos en salud y de la participación ciudadana en su ámbito de competencia de su red de salud.

x) Conducir la planificación, presupuestación y ejecución de la gestión institucional de los recursos físicos y los sistemas logísticos de la unidad ejecutora de salud, asignando en custodia y controlando su uso, identificando sus requerimientos y especificaciones técnicas, programando su distribución y mantenimiento; así como ejecución de procesos de altas, bajas y enajenaciones de sus activos fijos; asignar recursos físicos a las redes y Micro redes de salud de su ámbito de responsabilidad.

y) Dirigir la supervisión, monitoreo y evaluación de los procesos de organización institucional; organización y gestión de servicios públicos de promoción, protección, recuperación y rehabilitación de la salud de las personas; organización y gestión de servicios de salud ambiental y ocupacional, gestión institucional de recursos humanos, gestión de información y desarrollo informático en salud, gestión de la investigación; promoción, protección y garantía de derechos ciudadanos en salud y participación ciudadana en el ámbito de la red de salud.

z) Dirigir la participación de la red en la evaluación de los procesos de emisión de políticas de salud, evaluación del desempeño institucional y del sector, regulación sectorial de salud de las personas, regulación sectorial de salud ambiental y ocupacional, regulación sectorial de medicamentos e insumos, organización y gestión de servicios de salud de promoción, protección, recuperación y rehabilitación de la salud de las personas y de salud ambiental y ocupacional; suministro de medicamentos e insumos médico quirúrgico, odontológicos y de laboratorio; gestión de información y desarrollo informático, gestión de la investigación en salud de la región.

aa) Supervisar la ejecución presupuestaria y controlar la evaluación de resultados de gestión financiera en la unidad ejecutora.

bb) Dirige, conduce, monitorea y evalúa los procesos de selección y adquisición de bienes, servicios y obras en el ámbito de su jurisdicción.

cc) Otras que le sean asignadas en el marco de la normativa vigente.

1.1.5. MISIÓN:[1]

"Somos una Red de Servicios de Salud que brinda atenciones integrales de salud con recursos humanos competitivos, para satisfacer necesidades de salud con calidez y eficiencia; promoviendo la integración intercultural y estilos de vida saludables según niveles de atención, liderando actividades preventivo promocionales de salud en concertación con las instituciones representativas, priorizando a las comunidades de difícil accesibilidad a los servicios de salud de acuerdo a su perfil epidemiológico".

[1] **FUENTE**: ROF INSTITUCIONAL APROBADO CON RESOLUCIÓN DE GOBIERNO REGIONAL DE SAN MARTIN

1.1.6. VISIÓN: [2]

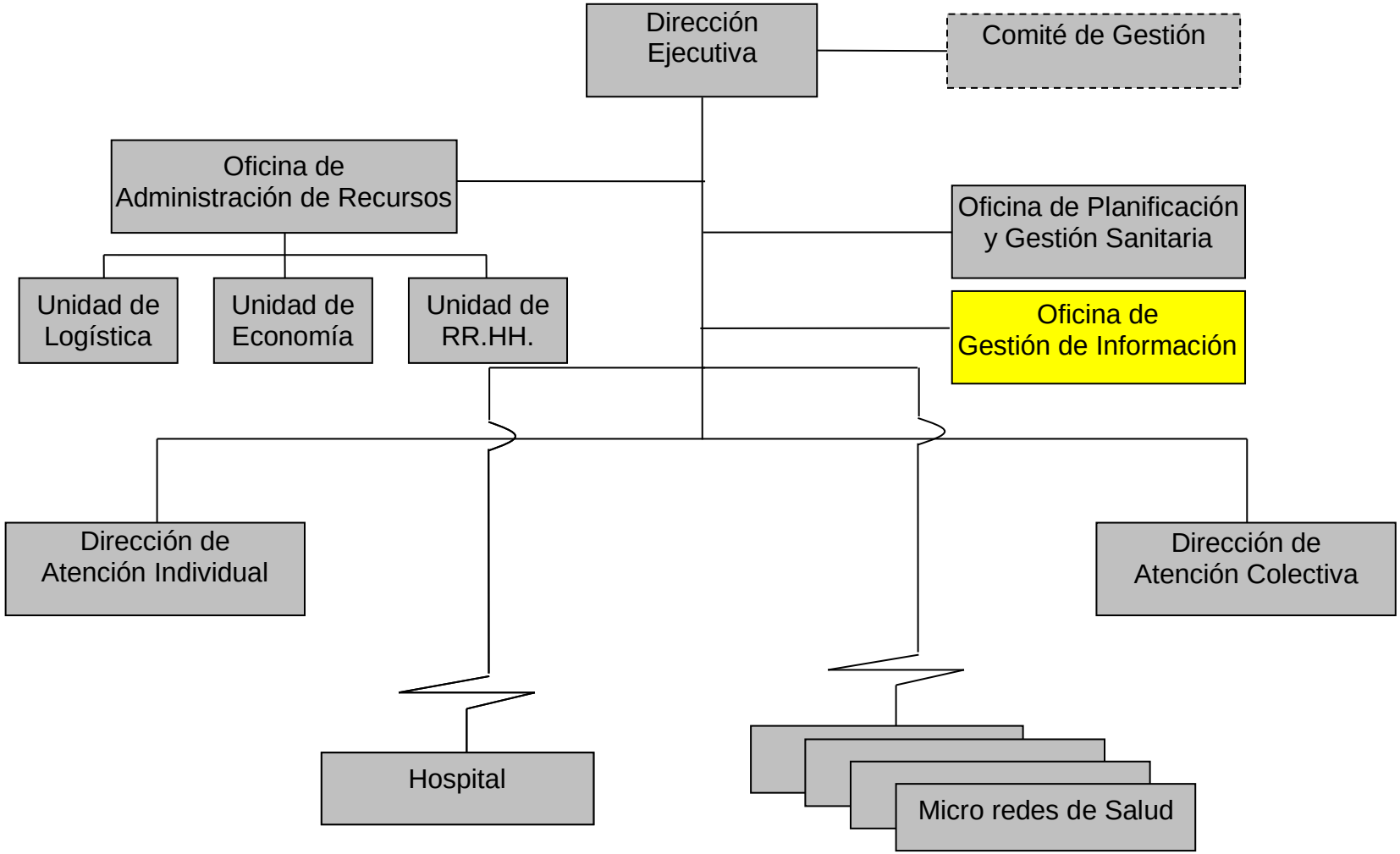
"Al 2014 la Red de Servicios de Salud Tocache será una Institución descentralizada y desconcentrada de la DIRES SM, brindando atención integral con calidad, calidez y equidad; con un nivel altamente competitivo y capacidad resolutiva, con accesibilidad a una población organizada que se compromete y participa en las acciones de salud a través de sus Micro redes eficientemente articuladas".

1.1.7. ORGANIZACIÓN INSTITUCIONAL.

Para el cumplimiento de las funciones, la Dirección Subregional de Salud Alto Huallaga - Unidad Ejecutora 403, cuenta con la siguiente estructura orgánica.

[2] **FUENTE**: ROF INSTITUCIONAL APROBADO CON RESOLUCIÓN DE GOBIERNO REGIONAL DE SAN MARTIN

ORGANIGRAMA DE LA DIRECCION SUBREGIONAL DE SALUD ALTO HUALLAGA TOCACHE[3]



[3] **FUENTE**: ROF INSTITUCIONAL APROBADO CON RESOLUCIÓN DE GOBIERNO REGIONAL DE SAN MARTIN

CAPITULO II
DESCRIPCION DEL PROBLEMA

2.1 SITUACION ACTUAL

Las Entidades de la Administración Pública enfrentan constantes ataques internos y externos a la Seguridad de la Información, y puesto que cuentan con presupuestos limitados, es difícil determinar la prioridad con la que una vulnerabilidad de Seguridad debe ser atendida, a fin de cubrir las vulnerabilidades primarias, sin embargo esto puede implicar una inversión significativa.

Son, por ejemplo, los trámites documentarios, las transferencias electrónicas de dinero o de documentos, la mensajería electrónica, los diversos servicios.

Actualmente la Dirección Subregional de Salud Alto Huallaga - Unidad Ejecutora 403, cuenta con la implementación del sistema de información de gestión administrativa SIGA, lo cual cuenta con tres módulos que son: SIGA-ML (Modulo Logístico), SIGA-PPR (Modulo Presupuesto por Resultados), SIGA-MP (Modulo Patrimonio).

El SIGA-ML sirve para la elaboración de órdenes de compra así como órdenes de servicio la Institución, entre otros.

El SIGA-PPR sirve para la programación de presupuesto de los diferentes programas estratégicos como son: Programa Articulado Nutricional, Materno Neonatal, TBC/VIH, Metaxenicas y Zoonosis, Enfermedades no transmisibles, Control y Prevención del Cáncer.

SIGA-MP sirve para la el control de los bienes patrimoniales de la Institución, entre otros.

El SIGA que actualmente se utiliza en la Dirección Subregional de Salud Alto Huallaga - Unidad Ejecutora 403 es de uso para los trabajadores, permitiéndoles solo el acceso a las personas que cuentan con su respectivo usuario y contraseña.

Debido a que no cuenta con una documentación que sea referente a la aplicación de la NTP peruana ISO 17799, se ha visto la necesidad de implementar una documentación con la Aplicación de este Estándar para tener mayor seguridad de la información.

2.2 OBJETIVOS:

GENERAL

Desarrollar la documentación utilizando la norma técnica peruana ISO 17799 en el desarrollo del Sistema de Información de Gestión Administrativa en la Dirección Subregional de Salud Alto Huallaga Tocache.

ESPECIFICOS

- Desarrollar la documentación con la norma técnica peruana ISO 17799 en el Sistema de Información de Gestión Administrativa, que permita administrar de manera centralizada las información del Siga.
- Implantar la documentación con la norma técnica peruana ISO 17799.
- Implementar de controles para la seguridad de la información.

2.3 JUSTIFICACIÓN

En la actualidad las entidades de la Administración pública se encuentran obligadas por la regulación peruana a cumplir con la norma técnica peruana NTP/ISO-IEC 17799, la cual está basada en el estándar ISO 27002. Sin embargo, puesto que esta norma técnica solamente hace referencia a la implementación de controles, debe ser completada con un sistema de análisis de riesgo que permita priorizar los controles y determinar las áreas de la organización sobre las cuales deben implementarse, a fin de optimizar la inversión económica y garantizar que solamente se implementen aquellos controles cuya inversión sea menor que la pérdidas por vulnerabilidades de seguridad.

El análisis de riesgo basado en los estándares ISO 27001:2005 e ISO 27005:2008, para las entidades de la Administración Pública, a fin de permitir recomendar los controles de seguridad que deben implementarse desde la formación de estos sistemas, estos controles estarán basados en el ISO 27002 e ITIL v3.

El presente trabajo sobre la aplicación de la norma técnica ISO 17799 en el desarrollo del Sistema de Información de Gestión Administrativa - SIGA ML en la Dirección Subregional de Salud Alto Huallaga Tocache, tiene por finalidad socializar al personal administrativo referente a la seguridad de la información de la institución.

CAPITULO III
FUNDAMENTACIÓN TEORICA

3.1 ANTECEDENTES

Actualmente la Dirección Subregional de Salud Alto Huallaga Tocache no Cuenta con un trabajo realizado sobre seguridad de la información, es decir aplicando la norma técnica peruana ISO 17799 al desarrollo del sistema de información de gestión administrativa SIGA- ML.

A nivel de la región San Martín existe poca información desarrollada con la aplicación de la norma técnica peruana.

A nivel nacional existen diferentes entidades que si han aplicado la mencionada norma como es por ejemplo el ministerio de educación, la RENIEC, universidades y otros.

3.2 BASES TEORICAS

3.2.1 Norma Técnica Peruana NTP-ISO/IEC 17799:2007

La presente Norma Técnica Peruana ha sido elaborada por el Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos (EDI), durante los meses de junio a julio del 2006, utilizando como antecedente a la Norma ISO/IEC 17799:2005.

El Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos (EDI) presentó a la Comisión de Reglamentos Técnico y Comerciales CRT, con fecha 2006-07-21, el PNTP-ISO/IEC 17799:2006 para su revisión y aprobación; siendo sometido a la etapa de Discusión Pública el 2006-11-25.

No habiéndose presentado observaciones fue oficializada como Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información, 2ª Edición, el 22 de enero del 2007.

Esta Norma Técnica Peruana es una adopción de la Norma ISO/IEC 17799:2005. La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español a sido estructurada de acuerdo a las Guías Peruanas GP 001:1995 y GP 002:1995.

3.2.2 Estructura de la NTP-ISO/IEC 17799:2007

Este estándar contiene 11 cláusulas de control de seguridad que contienen colectivamente un total de 39 categorías principales de seguridad y una cláusula introductoria conteniendo temas de evaluación y tratamiento del riesgo.

Cláusulas

Cada cláusula contiene un número de categorías principales de seguridad. Las 11 cláusulas (acompañadas por el número de categorías principales de seguridad incluidas en cada cláusula) son:

1) Política de seguridad (1);
2) Organizando la seguridad de información (2);
3) Gestión de activos (2);
4) Seguridad en recursos humanos (3);
5) Seguridad física y ambiental (2);

6) Gestión de comunicaciones y operaciones (10);
7) Control de acceso (7);
8) Adquisición, desarrollo y mantenimiento de sistemas de información(6);
9) Gestión de incidentes de los sistemas de información (2);
10) Gestión de la continuidad del negocio (1);
11) Cumplimiento (3)

El orden de las cláusulas en este estándar no implica su importancia. Dependen de las circunstancias, todas las cláusulas pueden ser importantes, por lo tanto cada organización que aplica este estándar debe identificar cláusulas aplicables, que tan importantes son y sus aplicaciones para procesos de negocios individuales. Igualmente, todas las listas de este estándar no se encuentran en orden de prioridad a menos que se notifique lo contrario.

3.2.3 ¿Qué es la 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 está 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 protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocios.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, 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.

3.2.4 ¿Por qué es necesaria la seguridad de la información?

La información y los procesos que la apoyan, los sistemas y redes son importantes activos de la organización. Definir, realizar, mantener y mejorar la seguridad de información, puede ser esencial para mantener la competitividad, flujo de liquidez, rentabilidad, cumplimiento de la legalidad e imagen comercial.

Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus

informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

La seguridad de información es importante en negocios tanto del sector público como del privado y para proteger las infraestructuras críticas. En ambos sectores, la seguridad de información permitirá, por ejemplo lograr el gobierno electrónico o el comercio electrónico, evitando y reduciendo los riesgos relevantes. La interconexión de las redes públicas y privadas y el compartir los recursos de información aumentan la dificultad de lograr el control de los accesos. La tendencia hacia la informática distribuida debilita la eficacia de un control central y especializado.

Muchos sistemas de información no se han diseñado para ser seguros. La seguridad que puede lograrse a través de los medios técnicos es limitada, y debería apoyarse en una gestión y procedimientos adecuados. La identificación de los controles que deberían instalarse requiere una planificación cuidadosa y una atención al detalle. La gestión de la seguridad de la información necesita, como mínimo, la participación de todos los empleados de la organización. También puede requerir la participación de los proveedores, clientes o accionistas. La asesoría especializada de organizaciones externas también puede ser necesaria.

3.2.5 ¿Cómo establecer los requisitos de seguridad?

Es esencial que la organización identifique sus requisitos de seguridad. Existen tres fuentes principales.

a) La primera fuente procede de la valoración de los riesgos de la organización, tomando en cuenta los objetivos y estrategias generales del negocio. Con ella se identifican las amenazas a los activos, se evalúa la vulnerabilidad y la probabilidad de su ocurrencia y se estima su posible impacto.

b) La segunda fuente es el conjunto de requisitos legales, estatutos, regulaciones y contratos que debería satisfacer la organización, sus socios comerciales, los contratistas y los proveedores de servicios.

c) La tercera fuente está formada por los principios, objetivos y requisitos que forman parte del tratamiento de la información que la organización ha desarrollado para apoyar sus operaciones.

3.2.6 Evaluación de los riesgos de seguridad

Los requisitos de seguridad se identifican mediante una evaluación metódica de los riesgos. El gasto en controles debería equilibrarse con el posible impacto económico, resultante de los fallos de seguridad.

Los resultados de ésta evaluación ayudarán a encauzar y determinar una adecuada acción gerencial y las prioridades para gestionar los riesgos de seguridad de la información, y la implantación de los controles seleccionados para protegerse contra dichos riesgos.

Las evaluaciones de riesgos deben repetirse periódicamente para tener en cuenta cualquier cambio que pueda influir en los resultados de la evaluación.

3.2.7 Selección de controles

Una vez que los requisitos de seguridad han sido identificados y las decisiones para el tratamiento de riesgos han sido realizadas, deberían elegirse e implantarse los controles que aseguren la reducción de los riesgos a un nivel aceptable. Pueden elegirse los controles partiendo de este documento, de otros conjuntos de controles o de nuevos controles que pueden diseñarse para cubrir adecuadamente las necesidades específicas. La selección de los controles de seguridad depende de las decisiones organizacionales basadas en el criterio para la identificación y clasificación de riesgos, las opciones para el tratamiento de estos y la gestión general de riesgos aplicable a la organización. Así mismo, debe ser sujeto a toda regulación y legislación nacional e internacional.

Ciertos controles expuestos en este documento, pueden considerarse como principios que guían la gestión de la seguridad de la información, aplicables a la mayoría de las organizaciones. Estos se explican en más detalle en el siguiente inciso denominado “Punto de partida de la seguridad de la información”.

3.2.8 Punto de partida de seguridad de la información

Cierto número de controles se consideran principios orientativos que proporcionan un punto de partida adecuado para implantar la seguridad de la información. Se apoyan en requisitos legislativos esenciales o se considera la mejor práctica habitual para conseguir dicha seguridad.

Los controles que se consideran esenciales para una organización desde un punto de vista legislativo comprenden:

a) La protección de los datos de carácter personal y la intimidad de las personas;

b) La salvaguarda de los registros de la organización;

c) Los derechos de la propiedad intelectual.

Los controles que se consideran la mejor práctica habitual para conseguir la seguridad de la información comprenden:

a) La documentación de la política de seguridad de la información;

b) La asignación de responsabilidades de seguridad;

c) La formación y capacitación para la seguridad de la información;

d) El procedimiento correcto en las aplicaciones;

e) La gestión de la vulnerabilidad técnica;

f) La gestión de la continuidad del negocio;

g) El registro de las incidencias de seguridad y las mejoras.

Estos controles pueden aplicarse a la mayoría de las organizaciones y los entornos.

Es conveniente señalar que pese a la importancia dada a los controles en este documento, la importancia de cualquier control debería determinarse a la luz de los riesgos específicos que afronta la organización. Por tanto y aunque el enfoque anterior se considere un buen punto de partida, no sustituye a la selección de controles basada en una evaluación del riesgo.

3.3 DEFINICIONES OPERACIONALES

3.3.1 Base de Datos[4]

Una base de datos se puede definir como un conjunto de información relacionada que se encuentra agrupada o estructurada.

Desde el punto de vista de la informático, la base de datos es un sistema formado por un conjunto de datos almacenados en discos que permiten el acceso directo a ellos y un conjunto de programas que manipulen ese conjunto de datos.

Una base de datos tiene mucha importancia en el ritmo de vida que llevamos en los actuales momentos, ya que, está acelera el ritmo en el momento realizar una búsqueda de información.

3.3.2 Administración

Es una disciplina que tiene por finalidad dar una explicación acerca del comportamiento de las organizaciones, además de referirse al proceso de conducción de las mismas.

Es ciencia fáctica, tiene un objeto real del mundo de la cultura (las organizaciones). Es técnica porque implica aceptar la existencia de medios específicos utilizables en la búsqueda del funcionamiento eficaz y eficiente de las organizaciones. Es técnica con su bagaje de principios, normas y procedimientos para la conducción racional de las organizaciones.

3.3.3 Activo[5]

Algo que tenga valor para lo organización.

[4] http://www.itlp.edu.mx/publica/tutoriales/basedat1/tema1_1.htm
[5] Fuente: norma técnica peruana NTP-ISO/IEC 17799

3.3.4 Control[6]

Herramienta de la gestión del riesgo, incluidas políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal. Control es también usado como sinónimo de salvaguardia o contramedida.

3.3.5 Pauta

Descripción que aclara que es lo que se debe hacer y cómo se hace, con el fin de alcanzar los objetivos planteados en las políticas.

3.3.6 Instalaciones de proceso de información

Sistemas de información, servicio o infraestructura, o locaciones físicas que los almacena.

3.3.7 Seguridad de la información[7]

Preservación de la confidencialidad, integridad y disponibilidad de la información, así mismo, otras propiedades como la autenticidad, no rechazo, contabilidad y confiabilidad también pueden ser consideradas.

3.3.8 Evento de seguridad de información

Es una ocurrencia identificada de un sistema, servicio, o red el cual indica una posible brecha de la política de seguridad de información o fallas de las salvaguardias o una situación desconocida que puede ser relevante para la seguridad.

[6] Fuente: norma técnica peruana NTP-ISO/IEC 17799
[7] Fuente: norma técnica peruana NTP-ISO/IEC 17799

3.3.9 Incidente de seguridad de información

Es indicado por una o varias series de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de negocios y de amenazar la seguridad de información.

3.3.10 Política[8]

Dirección general y formal expresada por la gerencia.

3.3.11 Riesgo[9]

Combinación de la probabilidad de un evento y sus consecuencias.

3.3.12 Análisis del riesgo[10]

Uso sistemático de la información para identificar fuentes y estimar el riesgo.

3.3.13 Evaluación del riesgo

Proceso general de análisis y evaluación del riesgo.

3.3.14 Valoración del riesgo

Proceso de comparación del riesgo estimado contra el criterio del riesgo dado para determinar el significado de este.

3.3.15 Gestión del riesgo[11]

Actividades coordinadas para dirigir y controlar una organización considerando el riesgo. Gestión del riesgo incluye típicamente evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo y comunicación del riesgo.

[8] Fuente: norma técnica peruana NTP-ISO/IEC 17799
[9] Fuente: norma técnica peruana NTP-ISO/IEC 17799
[10] Fuente: norma técnica peruana NTP-ISO/IEC 17799
[11] Fuente: norma técnica peruana NTP-ISO/IEC 17799

3.3.16 Tratamiento del riesgo

Proceso de selección e implementación de medidas para modificar el riesgo.

3.3.17 Terceros

Persona que es reconocida por ser independiente de las partes involucradas concerniente al tema en cuestión.

3.3.18 Amenaza

Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización.

3.3.19 Vulnerabilidad

Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas.

3.4 DEFINICIONES METODOLOGICAS

El alcance del presente documento está limitado a establecer los controles requeridos por la NTP-ISO 17799:2004 y el dominio 9 de la norma NTP-ISO 17799:2007 llamado “Administración de Incidentes”. Dichos controles se detallan a continuación:

1. Políticas de Seguridad

#	Objetivo de Control	#	Actividad de Control
1.1	Políticas de Seguridad de la Información	1.1.1	Documento de política de seguridad de la información y revisión de la evaluación.

Cuadro 01: Dominio 01 de la NTP ISO 17799.

2. Aspectos Organizativos para la Seguridad

#	Objetivo de Control	#	Actividad de Control
2.1	Estructura para la seguridad de la información	2.1.1	Comité de gestión de seguridad de la información
		2.1.2	Coordinación de la seguridad de la información
		2.1.3	Asignación de responsabilidades sobre seguridad de la información
		2.1.4	Proceso de autorización de recursos para el tratamiento de la información
		2.1.5	Asesoramiento de especialistas en seguridad de la información
		2.1.6	Cooperación entre organizaciones
		2.1.7	Revisión independiente de la seguridad de la información
2.2	Seguridad en los accesos de	2.2.1	Identificación de riesgos por el acceso de terceros

#	Objetivo de Control	#	Actividad de Control
	terceras partes	2.2.2	Requisitos de seguridad en contratos con terceros
2.3	Outsourcing	2.3.1	Requisitos de seguridad en contratos de Outsourcing

Cuadro 02: Dominio 02 de la NTP ISO 17799.

3. Clasificación y Control de Activos

#	Objetivo de Control	#	Actividad de Control
3.1	Responsabilidad sobre los activos	3.1.1	Inventario de activos
3.2	Clasificación de la información	3.2.1	Guías de Clasificación
		3.2.2	Marcado y tratamiento de la información

Cuadro 03: Dominio 03 de la NTP ISO 17799.

4. Seguridad Ligado al Personal

#	Objetivo de Control	#	Actividad de Control
4.1	Seguridad en la definición del trabajo y los recursos	4.1.1	Inclusión de la seguridad en las responsabilidades laborales
		4.1.2	Selección y política de personal
		4.1.3	Acuerdos de confidencialidad
		4.1.4	Términos y condiciones de la relación laboral
4.2	Formación de usuarios	4.2.1	Formación y capacitación en seguridad de la información
4.3	Respuesta ante incidencias y	4.3.1	Comunicación de las incidencias de seguridad

#	Objetivo de Control	#	Actividad de Control
	malos funcionamientos de la seguridad	4.3.2	Comunicación de las debilidades de seguridad
		4.3.3	Comunicación de los fallos del software.
		4.3.4	Aprendiendo de las incidencias
		4.3.5	Procedimiento disciplinario

Cuadro 04: Dominio 04 de la NTP ISO 17799.

5. Seguridad Física y Del Entorno

#	Objetivo de Control	#	Actividad de Control
5.1	Áreas seguras	5.1.1	Perímetro de seguridad física
		5.1.2	Controles físicos de entradas
		5.1.3	Seguridad de oficinas, despachos y recursos
		5.1.4	El trabajo en las áreas seguras
		5.1.5	Áreas aisladas de carga y descarga
5.2	Seguridad de los equipos	5.2.1	Instalación y protección de equipos
		5.2.2	Suministro eléctrico
		5.2.3	Seguridad del cableado
		5.2.4	Mantenimiento de equipos
		5.2.5	Seguridad de equipos fuera de los locales de la organización
		5.2.6	Seguridad en el re-uso o eliminación de equipos
5.3	Controles Generales	5.3.1	Política de puesto de trabajo despejado y bloqueo de pantalla

Cuadro 05: Dominio 05 de la NTP ISO 17799.

6. Gestión de Comunicaciones y Operaciones

#	Objetivo de Control	#	Actividad de Control
6.1	Procedimientos y responsabilidades de operación	6.1.1	Documentación de procedimientos operativos
		6.1.2	Control de cambios operacionales
		6.1.3	Procedimientos de gestión de incidencias
		6.1.4	Segregación de tareas
		6.1.5	Separación de los recursos para desarrollo y para producción
		6.1.6	Gestión de servicios externos
6.2	Planificación y aceptación del sistema	6.2.1	Planificación de la capacidad
		6.2.2	Aceptación del sistema
6.3	Protección contra software malicioso	6.3.1	Medidas y controles contra software malicioso
6.4	Gestión interna de respaldo y recuperación	6.4.1	Recuperación de la información
		6.4.2	Diarios de operación
		6.4.3	Registro de fallos
6.5	Gestión de redes	6.5.1	Controles de red
6.6	Utilización y seguridad de los medios de información	6.6.1	Gestión de medios removibles
		6.6.2	Eliminación de medios
		6.6.3	Procedimientos de manipulación de la información
		6.6.4	Seguridad de la documentación de sistemas
6.7	Intercambio de información y software	6.7.1	Acuerdos para intercambio de información y software
		6.7.2	Seguridad de medios en tránsito
		6.7.3	Seguridad en comercio electrónico
		6.7.4	Seguridad del correo electrónico
		6.7.5	Seguridad de los sistemas ofimáticos
		6.7.6	Sistemas públicamente disponibles

Cuadro 06: Dominio 06 de la NTP ISO 17799.

7. Control de Accesos

#	Objetivo de Control	#	Actividad de Control
7.1	Requisitos de negocio para el control de accesos	7.1.1	Política de control de accesos
7.2	Gestión de acceso de usuarios	7.2.1	Registro de usuarios
		7.2.2	Gestión de privilegios
		7.2.3	Gestión de contraseñas de usuario
		7.2.4	Revisión de los derechos de acceso de los usuarios
7.3	Responsabilidades de usuarios	7.3.1	Uso de contraseñas
		7.3.2	Equipo informático de usuario desatendido
7.4	Control de acceso a la red	7.4.1	Política de uso de los servicios de la red
		7.4.2	Ruta forzosa
		7.4.3	Autenticación de usuarios para conexiones externas
		7.4.4	Autenticación de nodos de la red
		7.4.5	Protección a puertos de diagnóstico remoto
		7.4.6	Segregación en las redes
		7.4.7	Control de conexión a las redes
		7.4.8	Control de enrutamiento en la red
7.5	Control de acceso al sistema operativo	7.5.1	Identificación automática de terminales
		7.5.2	Procedimientos de conexión de terminales
		7.5.3	Identificación y autenticación del usuario
		7.5.4	Sistema de gestión de contraseñas
		7.5.5	Utilización de las facilidades del sistema
		7.5.6	Protección del usuario frente a coacciones
		7.5.7	Desconexión automática de terminales

#	Objetivo de Control	#	Actividad de Control
		7.5.8	Limitación del tiempo de conexión
7.6	Control de acceso a las aplicaciones	7.6.1	Restricción de acceso a la información
		7.6.2	Aislamiento de sistemas sensibles
7.7	Seguimiento de accesos y uso del sistema	7.7.1	Registro de incidencias
		7.7.2	Seguimiento del uso de los sistemas
		7.7.3	Sincronización de relojes

Cuadro 07: Dominio 07 de la NTP ISO 17799.

8. Desarrollo y Mantenimiento de Sistemas

#	Objetivo de Control	#	Actividad de Control
8.1	Requisitos de seguridad de los sistemas	8.1.1	Análisis y especificación de los requisitos de seguridad
8.2	Seguridad de las aplicaciones del sistema	8.2.1	Validación de los datos de entrada
		8.2.2	Control del proceso interno
		8.2.3	Autenticación de mensajes
		8.2.4	Validación de los datos de salida
8.3	Controles criptográficos	8.3.1	Política de uso de los controles criptográficos
		8.3.2	Cifrado
		8.3.3	Firmas digitales
		8.3.4	Servicios de no repudio
		8.3.5	Gestión de claves
8.4	Seguridad de los archivos del sistema	8.4.1	Control del software en producción
		8.4.2	Protección de los datos de prueba del sistema
		8.4.3	Control de acceso a la librería de programas fuente
8.5	Seguridad en los procesos de	8.5.1	Procedimientos de control de cambios
		8.5.2	Revisión técnica de los cambios en el

#	Objetivo de Control	#	Actividad de Control
	desarrollo y soporte		sistema operativo
		8.5.3	Restricciones en los cambios a los paquetes de software
		8.5.4	Canales encubiertos y código Troyano
		8.5.5	Desarrollo externo del software

Cuadro 08: Dominio 08 de la NTP ISO 17799.

9. Gestión de Continuidad del Negocio

#	Objetivo de Control	#	Actividad de Control
9.1	Aspectos de la gestión de continuidad del negocio	9.1.1	Proceso de gestión de la continuidad del negocio
		9.1.2	Continuidad del negocio y análisis de impactos
		9.1.3	Redacción e implantación de planes de continuidad
		9.1.4	Marco de planificación para la continuidad del negocio
		9.1.5	Prueba, mantenimiento y reevaluación de los planes de continuidad

Cuadro 09: Dominio 09 de la NTP ISO 17799.

10. Cumplimiento

#	Objetivo de Control	#	Actividad de Control
10.1	Cumplimiento con los requisitos legales	10.1.1	Identificación de la legislación aplicable
		10.1.2	Derechos de propiedad intelectual (DPI)
		10.1.3	Salvaguarda de los registros de la

#	Objetivo de Control	#	Actividad de Control
			organización
		10.1.4	Evitar el mal uso de los recursos de tratamiento de la información
10.2	Revisiones de la política de seguridad y de la conformidad técnica	10.2.1	Conformidad con la política de seguridad
10.3	Consideraciones sobre la auditoria de sistemas	10.3.1	Controles de auditoria de sistemas
		10.3.2	Protección de las herramientas de auditoria de sistemas

Cuadro 10: Dominio 10 de la NTP ISO 17799.

Controles definidos en la NTP ISO 17799:2007

#	Objetivo de Control	#	Actividad de Control
9.1	Reportando eventos y debilidades de la seguridad de información	9.1.1	Reportando los eventos en la seguridad de información
		9.1.2	Reportando debilidades en la seguridad de información
9.2	Gestión de las mejoras e incidentes en la seguridad de información	9.2.1	Responsabilidades y procedimientos
		9.2.2	Aprendiendo de los incidentes en la seguridad de información
		9.2.3	Recolección de evidencia

CAPITULO IV
DESARROLLO DE LA APLICACIÓN DEL ESTÁNDAR

Los controles de seguridad desarrollados en el presente documento permitirán establecer mejoras a la gestión de la seguridad del Centro de Datos y facilitar el proceso de implementación de los mismos. Por otro lado, las narrativas de cada uno de los controles permitirán establecer una base común para el establecimiento de normas, políticas y procedimientos de seguridad de la información.

A continuación se muestran los principales conceptos relacionados a los controles desarrollados.

4.1 DEFINICIÓN DE TERMINOS

Para identificar adecuadamente a cada responsable que forma parte de la descripción del control se han definido los siguientes términos:

- **COSI:** Comité Operativo de Seguridad de Información.
- **CESI:** Comité Ejecutivo de Seguridad de Información.
- **JOFIN:** Jefe de la Oficina de Informática.
- **OSEG:** Oficial de seguridad de la información.
- **JAIT:** Jefe del Área de Infraestructura Tecnológica.
- **ETIC:** Especialista en Tecnologías de Información y Comunicación.
- **SEC:** Secretaria del Área de Infraestructura Tecnológica.
- **PIES:** Proveedor Interno o Externo del Servicio.

- **USIE:** Usuario Interno o Externo.
- **ASER:** Administrador de Servidores.

4.2 CLASIFICACIÓN DE CONTROLES DE SEGURIDAD

Para una mejor comprensión se explica a continuación el significado de cada uno de los tipos de los controles de seguridad:

De acuerdo al objetivo con el cual está desarrollado cada control, se puede clasificar como:

- **Preventivo:** Permite prevenir que se origine un riesgo.
- **Detectivo:** Permite identificar una incidencia de seguridad de información.
- **Correctivo:** Permite corregir una incidencia de seguridad de información, con el objetivo de minimizar el daño o pérdida que pueda ocasionar la misma.

De acuerdo a como se ejecuta el control, se puede clasificar como:

- **Manual:** Control realizado por una serie de actividades ejecutadas por seres humanos.
- **Automático:** Control apoyado por tecnologías de información, las cuales permiten automatizar el proceso de ejecución del mismo.

4.3 NARRATIVAS DE LOS OBJETIVOS Y ACTIVIDADES DE CONTROL

Los objetivos y controles de seguridad se identificaron como resultado del análisis de la situación actual de la seguridad de información de la Dirección Subregional de Salud Alto Huallaga Tocache y el nivel de cumplimiento requerido por las principales normas de seguridad.

Para una mejor comprensión, los resultados se presentan agrupados por dominio de control dentro de la norma NTP-ISO 17799:2004 y 2007.

El significado de cada columna de la tabla de Objetivos de Control, se muestran a continuación:

#OC: Es el código que permite identificar un Objetivo de Control.

Objetivo de Control: se refiere el nombre del Objetivo de Control de la norma.

Descripción: Se refiere a la descripción de cada Objetivo de Control de la norma.

El significado de cada columna de la tabla de Actividades de control, se muestran a continuación:

#AC: Es el código que permite identificar a una Actividad de Control de la norma.

Actividad de Control: Es la descripción general de cada control definido en la norma.

Tipo de Control: Se refiere a la clasificación asignada a la actividad de control (preventivo, detectivo, correctivo; manual y/o automático).

Responsable de ejecutar el control: Se refiere a los encargados de ejecutar la actividad de control.

Narrativa de la actividad de control: Se refiere a la descripción de las actividades que se requieren establecer para implementar la actividad de control.

Documentación relacionada: Se refiere a la descripción de la documentación (Políticas, Normas, Procedimientos y Estándares) requeridos para cubrir la narrativa de la actividad de control.

Estándar relacionado: Contiene la descripción de los estándares relacionados (NTP-IO/IEC 17799:2004, COBIT e ITIL) a la actividad de control establecida.

Figura 01: Pantalla Inicial del SIGA

Figura 02: Autenticación al SIGA

Figura 03: Módulos del SIGA

Figura 04: Modulo Logística del SIGA

Figura 05: Generación de un pedido de Compra de B/S en el SIGA

A continuación se muestra el detalle del objetivo y control de seguridad desarrollado:

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

# OC	Objetivo de Control	Descripción
8.1	Requisitos de seguridad de los sistemas	OBJETIVO: Asegurar que la seguridad esté imbuida dentro de los sistemas de información. Esto incluirá la infraestructura, las aplicaciones de negocio y las aplicaciones desarrolladas por usuarios. El diseño y la implantación de los procesos de negocio que soportan las aplicaciones o el servicio, pueden ser cruciales para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados antes de desarrollar los sistemas de información.

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.1.1	La Unidad Ejecutora 403 deberá establecer una norma en la que se formalice como necesarias las especificaciones de seguridad que deben ser	• Preventivo Manual	• Responsable de sistemas de información	1. Verificar que se cuente con una norma en la cual se incluya cláusulas en las que se consideren como necesaria la especificación de requisitos de seguridad para los sistemas a ser adquiridos o desarrollados a la medida. 2. Verificar que se cuenta con un procedimiento de gestión de cambios en los que se considere la evaluación de requerimientos considerando aspectos de seguridad, disponibilidad, confidencialidad, integridad e impacto. 3. Verificar que el documento de registro de control de requerimientos de	Normas: Norma de administración de cambios de sistemas de información Procedimiento: Gestión para el cambio en los sistemas de información	NTP-IO/IEC 17799:2004 Análisis y especificación de los requisitos de seguridad COBIT PO2.1, PO9.5, AI1.8, AI1.9, DS5.8 ITIL 7.3, 7.3, 7.2,

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
	analizadas en un desarrollo o mantenimiento a un sistema de información. Frecuencia: Anual			cambio a los sistemas de aplicación se encuentre actualizado.	Documento Estándar: Registro de control de requerimientos	2.6, 7.3, 4.2

# OC	Objetivo de Control	Descripción
8.2	Seguridad de las aplicaciones del sistema	OBJETIVO: Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones. Se deberían diseñar dentro de las aplicaciones (incluidas las aplicaciones escritas por los usuarios) las medidas de control y las evidencias de auditoría o los registros de actividad. Éstos deberían incluir la validación de los datos de entrada, el tratamiento interno y los datos de salida.

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.2.1	La Unidad Ejecutora 403 deberá establecer controles para validar datos de entrada a las aplicaciones de los sistemas para garantizar que estas sean correctas y apropiadas. Frecuencia: Permanente	• Preventivo Manual	• Responsable de sistemas de información	1. Verificar que se cuente con una norma en la cual se incluya cláusulas en el que se indique el uso de controles para los datos de entrada de las aplicaciones, tales como: ▪ Valores fuera de rango ▪ Caracteres inválidos en los campos de datos ▪ Datos que faltan o que están incompletos 2. Verificar que los sistemas de información cuenten con los controles especificados en la Norma de seguridad de las aplicaciones del sistema.	Norma: Norma de seguridad de las aplicaciones del sistema.	NTP-IO/IEC 17799:2004 Validación de los datos de entrada COBIT AI1.8, 2.6.1, AI1.9, AI1.10, AI2.7, AI2.8, AI2.10, AI2.11, AI2.12, AI2.14, DS5.15, DS11.6, DS11.7, DS11.8, DS11.9, DS11.10, DS11.11, DS11.14, DS11.15, DS11.28, DS11.29 ITIL 7.2, 7.3, 5.2, 5.3, 4.3, 5.2,

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
						7, 4.2
8.2.2	La Unidad Ejecutora 403 deberá implementar comprobaciones periódicas para garantizar la integridad de los datos. Frecuencia: Semestral	• Preventivo Manual	• Responsable de sistemas de información	1. Verificar que se cuente con una norma en la cual se incluya una cláusula en la que se especifique la necesidad de realizar pruebas para garantizar la integridad de datos y comprobar que los programas de las aplicaciones se ejecutan en el momento adecuado. 2. Verificar que se realicen comprobaciones periódicas de la integridad de los datos de acuerdo a lo definido en la Norma de seguridad de las aplicaciones del sistema.	Norma: Norma de seguridad de las aplicaciones del sistema.	NTP-IO/IEC 17799:2004 Control del proceso interno COBIT AI1.8, 2.6.1, AI1.9, AI1.10, AI2.7, AI2.8, AI2.10, AI2.11, AI2.12, AI2.14, DS5.15, DS11.6, DS11.7, DS11.8, DS11.9, DS11.10, DS11.11, DS11.14, DS11.15, DS11.28, DS11.29

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
						ITIL 7.2, 7.3, 5.2, 5.3, 4.3, 5.2, 7, 4.2
8.2.3	La Unidad Ejecutora 403 deberá implementar autenticación de mensajes en aplicaciones que requieran protección de la integridad del contenido del mensaje. Frecuencia: Permanente	• Preventivo Manual	• Responsable de sistemas de información	1. Verificar que se cuente con una norma en la cual se incluya cláusulas para el uso de controles de autenticación de mensajes para el caso de las aplicaciones críticas donde se transmite información sensible. 2. Verificar que se han implementado controles de autenticación de mensajes en las aplicaciones críticas donde se transmite información sensible, de acuerdo a la Norma de seguridad de las aplicaciones del sistema.	Norma: Norma de seguridad de las aplicaciones del sistema.	NTP-IO/IEC 17799:2004 Autenticación de mensajes COBIT AI1.8, 2.6.1, AI1.9, AI1.10, AI2.7, AI2.8, AI2.10, AI2.11, AI2.12, AI2.14, DS5.15, DS11.6, DS11.7, DS11.8, DS11.9, DS11.10, DS11.11, DS11.14, DS11.15, DS11.28,

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
						DS11.29 <u>ITIL</u> 7.2, 7.3, 5.2, 5.3, 4.3, 5.2, 7, 4.2
8.2.4	La Unidad Ejecutora 403 deberá validar los datos de salida de un sistema de aplicación para garantizar que el proceso de la información ha sido el correcto. <u>Frecuencia:</u> Semestral	• Preventivo Manual	• Responsable de sistemas de información	1. Verificar que se cuente con una norma en la cual se incluya cláusulas de validaciones de datos de salida para el caso de sistemas críticos. 2. Verificar que se hayan implementado controles de validación de datos de salida para el caso de sistemas críticos de acuerdo a la Norma de seguridad de las aplicaciones del sistema.	<u>Norma:</u> Norma de seguridad de las aplicaciones del sistema.	<u>NTP-IO/IEC 17799:2004</u> Validación de los datos de salida <u>COBIT</u> AI1.8, 2.6.1, AI1.9, AI1.10, AI2.7, AI2.8, AI2.10, AI2.11, AI2.12, AI2.14, DS5.15, DS11.6, DS11.7, DS11.8, DS11.9, DS11.10, DS11.11, DS11.14,

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
						DS11.15, DS11.28, DS11.29 ITIL 7.2., 7.3, 5.2, 5.3, 4.3, 5.2, 7, 4.2

# OC	Objetivo de Control	Descripción
8.3	Controles criptográficos	OBJETIVO: Proteger la confidencialidad, autenticidad o integridad de la información. Se deberían usar sistemas y técnicas criptográficas para proteger la información sometida a riesgo, cuando otras medidas y controles no proporcionen la protección adecuada.

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.3.1	La Unidad Ejecutora 403 deberá desarrollar una política para	• Preventivo • Manual	• Responsable de sistemas de información	1. Verificar que se cuente con una norma en la cual se incluya el uso de controles criptográficos.	Norma: Norma de controles criptográficos.	NTP-IO/IEC 17799:2004 Política de uso de los controles criptográficos

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
	criptografía. Frecuencia: Anual					COBIT PO8.4, PO9.3, DS2.7, DS5.1, DS5.14, DS5.15, DS5.16, DS5.17, DS5.18, DS11.27, DS11.28 ITIL 4.1, 2.3, 4.2
8.3.2	La Unidad Ejecutora 403 deberá implementar la técnica criptográfica de cifrado para proteger la informació	• Preventivo Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma en la cual se incluya el uso de la técnica criptográfica de cifrado para proteger la información crítica o sensible para la organización. 2. Verificar la implementación de controles criptográficos en las aplicaciones que manejan información sensible de acuerdo a lo definido en la	Norma: Norma de controles criptográficos.	NTP-IO/IEC 17799:2004 Cifrado COBIT PO8.4, PO9.3, DS2.7, DS5.1, DS5.14,

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
	n considerada como sensible para la organización. Frecuencia: Permanente			Norma de controles criptográficos.		DS5.15, DS5.16, DS5.17, DS5.18, DS11.27, DS11.28 ITIL 4.1, 2.3, 4.2
8.3.3	La Unidad Ejecutora 403 deberá implementar el uso de firmas digitales para proteger la autenticidad e integridad de los documentos electrónicos.	• Preventivo • Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma en la cual se incluya el uso de firmas digitales para proteger la integridad de documentos electrónicos considerados críticos para organización y para aplicaciones de red interna que manejen información sensible. 2. Verificar que se haya implementado el uso de firmas digitales de acuerdo a la Norma de Controles Criptográficos.	Norma: Norma de controles criptográficos.	NTP-IO/IEC 17799:2004 Firmas digitales COBIT PO8.4, PO9.3, DS2.7, DS5.1, DS5.14, DS5.15, DS5.16, DS5.17, DS5.18,

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
	Frecuencia: Permanente					DS11.27, DS11.28 ITIL 4.1, 2.3, 4.2
8.3.4	La Unidad Ejecutora 403 deberá implementar servicios de no repudio. Frecuencia: Anual	• Preventivo Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma en la cual se incluya el uso de servicios de no repudio para resolver posibles disputas sobre la ocurrencia o no de un evento o acción electrónica. 2. Verificar que se hayan implementado controles de no repudio en los sistemas de información.	Normas: Norma de controles criptográficos.	NTP-IO/IEC 17799:2004 Servicios de no repudio COBIT PO8.4, PO9.3, DS2.7, DS5.1, DS5.14, DS5.15, DS5.16, DS5.17, DS5.18, DS11.27, DS11.28 ITIL 4.1, 2.3, 4.2

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.3.5	La Unidad Ejecutora 403 deberá implementar un sistema de gestión para dar soporte a las técnicas criptográficas (Claves privadas y públicas) Frecuencia: Anual	• Preventivo Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma que establezca el empleo de un sistema para la gestión para dar soporte y proteger todos los tipos de claves (privada y pública) de su modificación o destrucción. 2. Verificar que se ha implementado un sistema de gestión de criptografía de acuerdo a la Norma de controles criptográfico.	Normas: Norma de controles criptográficos.	NTP-IO/IEC 17799:2004 Gestión de claves COBIT PO8.4, PO9.3, DS2.7, DS5.1, DS5.14, DS5.15, DS5.16, DS5.17, DS5.18, DS11.27, DS11.28 ITIL 4.1, 2.3, 4.2

# OC	Objetivo de Control	Descripción
8.4	Seguridad de los archivos del sistema	OBJETIVO: Para asegurar que los proyectos de Tecnología de la Información (TI) y las actividades complementarias sean llevadas a cabo de una forma segura. El acceso a los archivos del sistema debería ser controlado. El mantenimiento de la integridad del sistema debería ser responsabilidad del grupo de desarrollo o de la función del usuario a quien pertenezcan las aplicaciones del sistema o el software.

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.4.1	La Unidad Ejecutora 403 deberá establecer controles para restringir la instalación y mantenimiento de los sistemas operativos. Frecuencia: Permanente	• Preventivo Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma en la cual se incluya las siguientes cláusulas: Las actualizaciones de las librerías de programas y las instalaciones del software de producción estén restringido al personal autorizado. Actualización de parches al software para eliminar o reducir vulnerabilidades. Registro de auditoría de todas las actualizaciones a las librerías de los programas en producción. 2. Verificar que en la política de seguridad del controlador de dominio de red se haya configurado para prevenir la instalación y/o modificación	Normas: Norma de control del software en producción.	NTP-IO/IEC 17799:2004 Control del software en producción COBIT AI2.15, AI3.3, AI3.4, AI3.5, AI3.6, DS5.4, DS5.7, DS9.6, DS9.7, DS9.8 ITIL 7.2, 5.4, 3.5, 4, 3.3, 4.2

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
				del sistema operativo.		
8.4.2	La Unidad Ejecutora 403 deberá implementar controles de acceso a los datos de pruebas. Frecuencia: Permanente	• Preventivo Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma en la que se incluya el uso de banco de prueba diferente a los datos de prueba con el cual se pueda cubrir la totalidad de escenarios de pruebas 2. Verificar que se cuenta con controles de accesos a proteger los datos de pruebas, los cuales deben ser accesados solo por el personal autorizado.	Normas: Norma de creación de datos de prueba.	NTP-IO/IEC 17799:2004 Protección de los datos de prueba del sistema COBIT AI2.15, AI3.3, AI3.4, AI3.5, AI3.6, DS5.4, DS5.7, DS9.6, DS9.7, DS9.8 ITIL 7.2, 5.4, 3.5, 4, 3.3, 4.2
8.4.3	La Unidad Ejecutora 403 deberá establecer un adecuado control en el acceso a	• Preventivo Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma en la cual se incluya cláusulas en la que se describa los controles que se requieren establecer para restringir el acceso del personal no autorizado a las fuentes de cada aplicativo. 2. Verificar que se cuenta con controles	Norma: Norma de control de acceso a las librerías de programas fuente.	NTP-IO/IEC 17799:2004 COBIT AI2.15, AI3.3, AI3.4, AI3.5, AI3.6, DS5.4,

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
	las librerías de programas fuentes. <u>Frecuencia:</u> Permanente			de acceso sobre las librerías de programas fuentes, de acuerdo a las Norma de control de acceso a las librerías de programas fuente.		DS5.7, DS9.6, DS9.7, DS9.8 <u>ITIL</u> 7.2, 5.4, 3.5, 4, 3.3, 4.2

# OC	Objetivo de Control	Descripción
8.5	Seguridad en los procesos de desarrollo y soporte	OBJETIVO: Mantener la seguridad del software de aplicación y la información. Se deberían controlar estrictamente los entornos del proyecto y de soporte. Los directivos responsables de los sistemas de aplicaciones también lo deberían ser de la seguridad del entorno del proyecto o su soporte. Se deberían asegurar de la revisión de todo cambio propuesto al sistema para comprobar que no debilite su seguridad o la del sistema operativo.

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.5.1	La Unidad Ejecutora	• Preventivo Manual	• Responsable de	1. Verificar que se cuenta con una norma de administración de cambios de	<u>Norma:</u>	<u>NTP-IO/IEC</u>

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
	403 deberá contar con estrictos controles sobre la implementación de cambios. Frecuencia: Permanente		sistemas de información.	sistema de información en los que se describe los controles requeridos para minimizar la corrupción de los sistemas de información. 2. Verificar que se cuenta con un procedimiento para el cambio en las operaciones en el que se establece una actividad de autorización del cambio por parte del responsable de sistemas. 3. Verificar la existencia de un formato en el cual se registran los cambios a los sistemas de información. 4. Verificar que los cambios a los sistemas de información son revisados por el área de calidad de software antes de realizar el pase a producción.	Norma de administración de cambios de sistemas de información. Procedimiento: Gestión para el cambio en los sistemas de información Documento Estándar: Registro de control de requerimientos	17799:2004 Procedimientos de control de cambios COBIT PO6.9, PO11.10, AI1.4, AI1.15, AI1.16, AI2.4, AI2.10, AI3.6, AI5.12, AI6.1, AI6.2, AI6.3, AI6.4, AI6.5, AI6.7, AI6.8, DS2.5, DS2.6, DS2.7, DS2.8 ITIL 5.6, 5.2, 5.2, 5.3, 3.3, 9.6, 3.5, 8.3, 8.5, 7.9, 8.2, 2.2, 9.5, 9.3, 9.3, 7.1, 7.4

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.5.2	La Unidad Ejecutora 403 deberá efectuar cambios en el sistema operativo, por ejemplo, para instalar una nueva versión o un parche de software. Frecuencia: Permanente	• Preventivo Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma que incluya la documentación de los cambios efectuados en los sistemas operativos y la autorización de los cambios por parte del responsable de sistemas.	Norma: Norma de administración de cambios de sistemas de información.	NTP-IO/IEC 17799:2004 Revisión técnica de los cambios en el sistema operativo COBIT PO6.9, PO11.10, AI1.4, AI1.15, AI1.16, AI2.4, AI2.10, AI3.6, AI5.12, AI6.1, AI6.2, AI6.3, AI6.4, AI6.5, AI6.7, AI6.8, DS2.5, DS2.6, DS2.7, DS2.8 ITIL 5.6, 5.2, 5.2, 5.3, 3.3, 9.6, 3.5, 8.3, 8.5, 7.9, 8.2, 2.2, 9.5, 9.3, 9.3, 7.1, 7.4

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.5.3	La Unidad Ejecutora 403 deberá limitar los cambios necesarios a los paquetes de software. Frecuencia: Permanente	• Preventivo Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma en la cual se incluya cláusulas en donde solo se realicen cambios autorizados por parte del responsable de sistemas de información.	Norma: Norma de administración de cambios de sistemas de información.	NTP-IO/IEC 17799:2004 Restricciones en los cambios a los paquetes de software COBIT PO6.9, PO11.10, AI1.4, AI1.15, AI1.16, AI2.4, AI2.10, AI3.6, AI5.12, AI6.1, AI6.2, AI6.3, AI6.4, AI6.5, AI6.7, AI6.8, DS2.5, DS2.6, DS2.7, DS2.8 ITIL 5.6, 5.2, 5.2, 5.3, 3.3, 9.6, 3.5, 8.3, 8.5, 7.9, 8.2, 2.2, 9.5, 9.3, 9.3, 7.1, 7.4

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.5.4	La Unidad Ejecutora 403 deberá establecer cláusulas que protejan a la institución respecto al monitoreo de canales encubiertos o código troyanos en el software adquirido o en el mantenimiento del mismo. Frecuencia: Anual	• Preventivo Manual	• Responsable de sistemas de información.	1. Verificar que la Política General de Seguridad de la Información contenga cláusulas que protejan a la institución respecto a los canales encubiertos o código troyano. 2. Verificar que se cuente con una norma que incluya cláusulas para el uso de antivirus.	Política Política General de Seguridad de Información. Norma: Norma de seguridad de los equipos informáticos.	NTP-IO/IEC 17799:2004 Canales encubiertos y código Troyano COBIT PO6.9, PO11.10, AI1.4, AI1.15, AI1.16, AI2.4, AI2.10, AI3.6, AI5.12, AI6.1, AI6.2, AI6.3, AI6.4, AI6.5, AI6.7, AI6.8, DS2.5, DS2.6, DS2.7, DS2.8 ITIL 5.6, 5.2, 5.2, 5.3, 3.3, 9.6, 3.5, 8.3, 8.5, 7.9, 8.2, 2.2, 9.5, 9.3, 9.3, 7.1, 7.4

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.5.5	La Unidad Ejecutora 403 deberá establecer acuerdos bajo licencia, propiedad del código y derechos de propiedad intelectual, derechos de acceso para auditar la calidad y exactitud del trabajo realizado, requisitos contractuales sobre la calidad del código, pruebas	• Preventivo • Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma en la cual se indique las cláusulas en las cuales se detallan la propiedad intelectual, garantías entre otros.	Norma: Norma de desarrollo externo de software.	NTP-IO/IEC 17799:2004 Desarrollo externo del software COBIT PO6.9, PO11.10, AI1.4, AI1.15, AI1.16, AI2.4, AI2.10, AI3.6, AI5.12, AI6.1, AI6.2, AI6.3, AI6.4, AI6.5, AI6.7, AI6.8, DS2.5, DS2.6, DS2.7, DS2.8 ITIL 5.6, 5.2, 5.2, 5.3, 3.3, 9.6, 3.5, 8.3, 8.5, 7.9, 8.2, 2.2, 9.5, 9.3, 9.3, 7.1, 7.4

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
	antes de la implantación para detectar el código Troyano. Frecuencia: Anual					

Cuadro 11: Adquisición, Desarrollo y Mantenimiento de Sistemas NTP ISO 17799.

4.4 COSTO DE LA APLICACION DE LA NTP ISO 17799

El costo de la aplicación de la Norma técnica Peruana ISO 17799 para la propuesta planteada en el presente trabajo es el costo de recurso humano, en el presente Cuadro se resume el costo de las tecnologías a usar. En tal sentido que el licenciamiento y costo de la mano de obra para la aplicación de NTP ISO 17799 es como se detalla a continuación.

TECNOLOGÍAS	**COSTO (S/.)**
Lic. Windows Server Standard 2008 R2 / SP1 X 64 idioma español lic. 5 CAL 1 server.	3,000.00
Lic. SQL SERVER 2008 R2 Standard	2,000.00
TOTAL TECNOLOGIAS	5,000.00
RECURSO HUMANO	1,500.00
TOTAL RR. HH.	**1,500.00**
TOTAL	**6,500.00**

Cuadro 12: Costo de aplicación de la NTP ISO 117799

Fuente: Elaboración Propia.

En este Capítulo, se plantea como propuesta para resguardar la integridad de la información de la Dirección Subregional de salud Alto Huallaga Tocache – UE 403.

CONCLUSIONES

- Se propuso la utilización de la Norma Técnica Peruana ISO 17799 en el desarrollo del Sistema de Información de Gestión Administrativa en la Dirección Subregional de Salud Alto Huallaga Tocache.

- Se desarrolló la documentación con la norma técnica peruana ISO 17799 en el Sistema de Información de Gestión Administrativa, que permitirá administrar de manera centralizada las información del Siga.

- Se implanto la documentación con la norma técnica peruana ISO 17799, para tener como una guía de buenas prácticas para la gestión de la seguridad de la información de la Dirección Subregional de Salud Alto Huallaga - Unidad Ejecutora 403 Tocache.

- Se implementó de controles para la seguridad de la información, para poder una buena gestión de la seguridad de la información de la Dirección Subregional de Salud Alto Huallaga - Unidad Ejecutora 403 Tocache.

RECOMENDACIONES

- Se recomienda que exista un buen uso y manejo de los equipos terminales que tienen acceso al servidor del Sistema de Información de Gestión Administrativa.
- Realizar los Back Up del Sistema de Información de Gestión Administrativa en línea y que tenga una frecuencia diaria en discos externos.
- Realizar el mantenimiento correctivo y preventivo de los equipos (Switch y router) de la red de datos una vez por año, para su mejor funcionamiento evitando cualquier deterioro provocado por el medio ambiente.
- Por la demanda de usuarios se recomienda hacer un mantenimiento y afinamiento de base de datos Siga.

REFERENCIAS BIBLIOGRAFÍCAS

- JAMES PETERS, JONATHAN DAVIDSON. 2001. Fundamentos de seguridad de la información. Trad. Maribel Martínez Moyano. 1ed. Madrid, Pearson educación. 344 p.

- ISO/IEC 17799 Segunda Edición, Tecnología de la Información – Técnicas de Seguridad – Código para la Práctica de la Gestión de la Seguridad de la Información. Pág. 170. Año 2005-06-15.

- ECHENIQUE GARCIA, JOSE ANTONIO. (2004). Auditoría en Informática. México, México D.F. McGraw-Hill Interamericana Editores S.A.

- CASTILLO SOTO, WILSON; ESTEBAN CHURAMPI, EFRAÍN. (2001). Normas Técnicas para Redacción y Presentación de Documentos Científicos. Perú, Tingo María, UNAS (CIUNAS), Imprenta La Florida.

- UNMSM (2003). AUDITORÍA A LA GESTIÓN DE LAS TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN [En Línea]: unmsm.edu.pe (http://sisbib.unmsm.edu.pe/bibvirtualdata/publicaciones/indata/Vol6_n1/pdf/auditoria.pdf, 10 Ago. 2011).

ANEXOS

GLOSARIO DE TERMINOS

ISO: International Organization for Standardization

IEC: International Electrotechnical Commission

SGSI: Sistema de Gestión de Seguridad de la información

BSI: British Standards Institution

COBIT: Control Objectives for Information and Related Technologies

ISACA:

ITIL: Information Technology Infrastructure Library

ANEXO 01: CODIGO SQL PARA AFINAMIENTO DE BASE DE DATOS Y EXTORNO DE ORDENES DE COMPRA Y DE SERVICIOS.

AFINAMIENTO DE BASE DE DATOS

sp_dboption 'siga', 'single user', 'true' – AFINAMIENTO DE BASE

go

DBCC checkalloc ('siga') -- REVISA EL CATALOGO DEL SISTEMA

GO

DBCC CHECKDB ('siga', repair_rebuild)

GO

DBCC CHECKDB ('siga', REPAIR_ALLOW_DATA_LOSS) -- REPARA LOS OBJETOS DE MANERA LOGICA

GO

sp_dboption 'siga', 'single user', 'false'

go

EXEC sp_MSforeachtable @command1="print '?' DBCC DBREINDEX ('?')" -- REINDEXADO LOGICO

go

sp_dboption 'siga', 'single user', 'false' --MULTIUSUARIO

EXTORNO DE ORDEN COMPRA 104

USE SIGA

UPDATE SIG_ORDEN_PRESUPUESTO **SET** SECUENCIAL = NULL, EXP_SIAF = NULL, SECU_SIAF = '', CORR_SIAF = '', FECHA_SIAF = NULL, ESTADO_EXP = ''

WHERE ANO_EJE = 2014 **and** SEC_EJEC = 1060 **and** NRO_ORDEN = 104 **and** TIPO_BIEN = 'B' **and** TIPO_PPTO = 1 **and** SEC_ORDEN = 1;

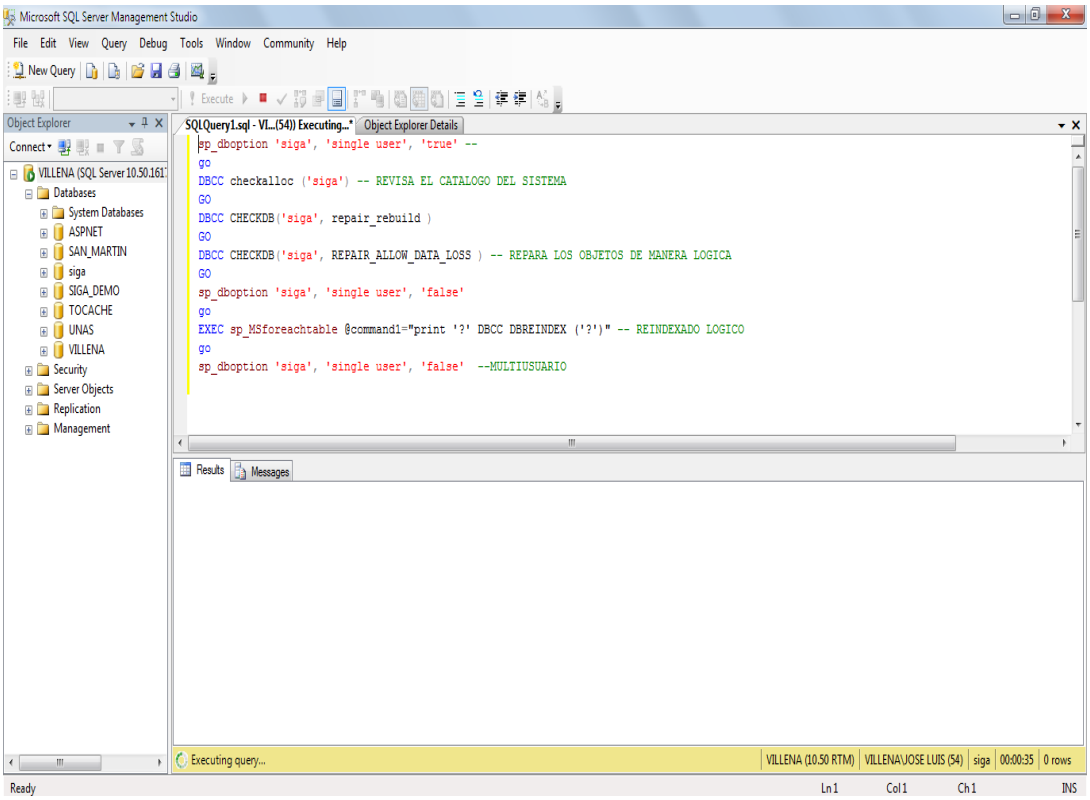
UPDATE SIG_ORDEN_SECUENCIA **SET** ESTADO_FASE = '0'

WHERE ANO_EJE = 2014 **and** SEC_EJEC = 1060 **and** NRO_ORDEN = 104 **and** TIPO_BIEN = 'B' **and** TIPO_PPTO = 1 **and** SEC_ORDEN = 1;

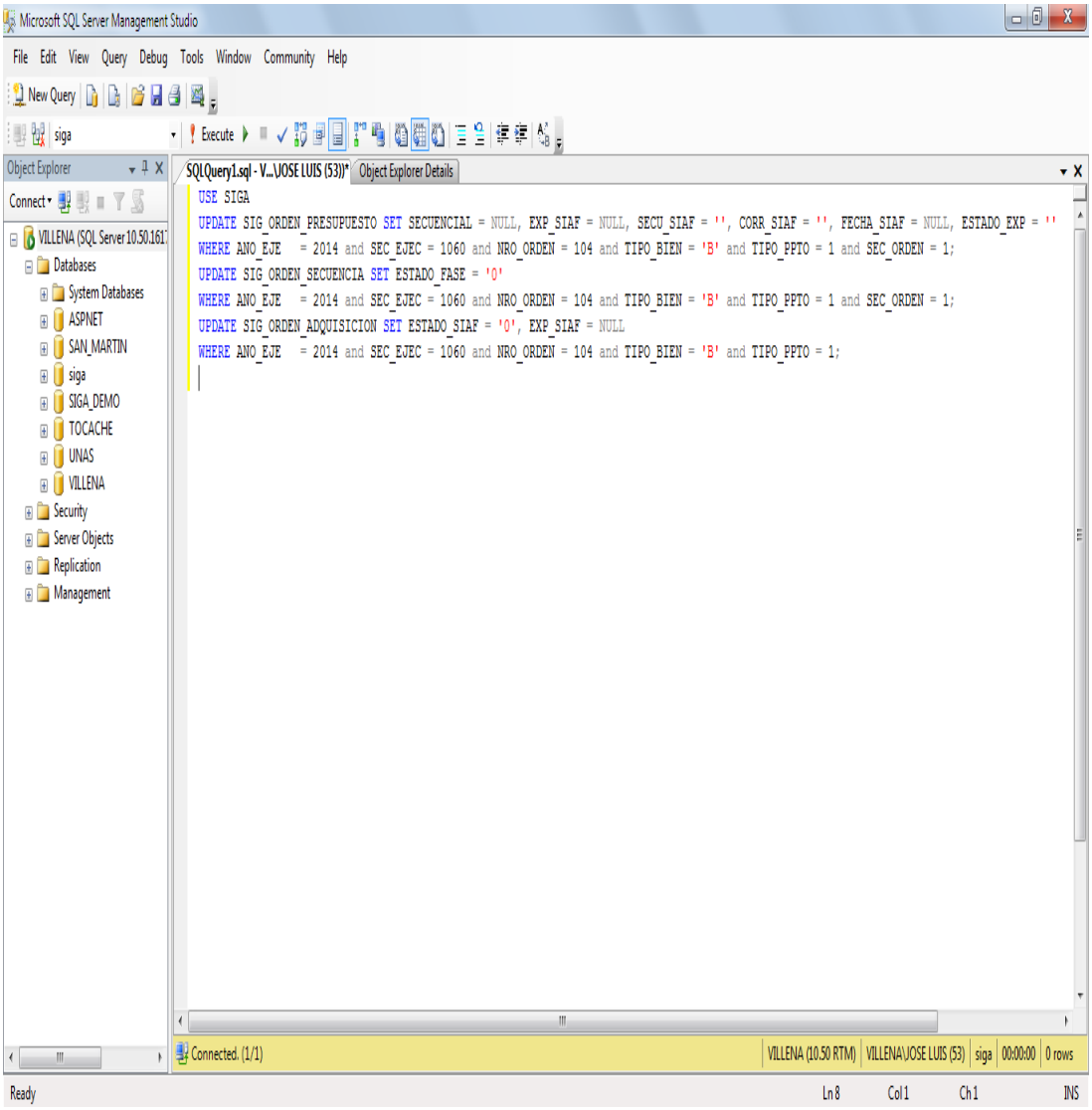
UPDATE SIG_ORDEN_ADQUISICION **SET** ESTADO_SIAF = '0', EXP_SIAF = NULL

WHERE ANO_EJE = 2014 **and** SEC_EJEC = 1060 **and** NRO_ORDEN = 104 **and** TIPO_BIEN = 'B' **and** TIPO_PPTO = 1;

MANTENIMIENTO Y AFINAMIENTO DE LA BASE DE DATOS SIGA



EXTORNO DE UNA ORDEN DE COMPRA 104 EN EL SIGA



ANEXO 02: INFORMES DE SITUACION DEL DATA CENTER Y SERVIDORES DE DATOS

DIRECCION REGIONAL DE SALUD SAN MARTIN
DIRECCION DE LA OFICINA DE OPERACIONES - SALUD
ALTO HUALLAGA TOCACHE

"Año de la Inversión para el Desarrollo Rural y la Seguridad Alimentaria"

INFORME Nº 004 -13-JLVA/O.O.S. –A.H.T.

Señor : **G.P. GEOVANNI W. CONDEZO SALVATIERRA**
DIRECTOR DE LA OFICINA DE OPERACIONES SALUD ALTO HUALLAGA – TOCACHE

De : **Bach. JOSE LUIS VILLENA ACUÑA**
INFORMATICO DE LA OFICINA DE OPERACIONES SALUD ALTO HUALLAGA – TOCACHE

REFERENCIA: ORDEN DE COMPRA N° 0261.

ASUNTO : MEJORAS TECNICAS DE EQUIPOS COMPUTACIONALES.

FECHA : 20 DE NOVIEMBRE DEL 2013

Me dirijo a Ud. a fin de informarle que se ha tomado conocimiento del documento de la referencia Orden de Compra Nº 0261, dentro de las cuales se mencionan los siguientes equipos:

- SERVIDOR DE DATOS SIGA.
- COMPUTADORA DE ESCRITORIO.
- PANTALLA.

El cuanto a la Estación de Trabajo con el Servidor la mejor opción es el **Servidor** con Procesador **Xeón E3-1220 V2** marca **HP**; mientras que la

Estación de Trabajo marca **HP** tiene un Procesador **Xeón E3-1240 V2**, Computadora de Escritorio con procesador AMD A10-5800B 3.80 GHZ con el procesador INTEL CORE i5-3470 3.20 GHZ la mejor opción es la computadora de Escritorio con **procesador INTEL CORE i5-3470 3.20 GHZ**; y con respecto al **PANTALLA** si está conforme**.**

Se recomienda adquirir el servidor con Procesador **Xeon E3-1220 V2** marca HP, Computadora de Escritorio con **procesador INTEL CORE i5-3470 3.20 GHZ.**

Es cuanto informo a Ud. para su conocimiento y fin.

Atentamente.,

Bach. JOSE LUIS VILLENA ACUÑA

"Año de la Promoción de la Industria Responsable y del Compromiso Climático"

INFORME Nº 003 -14-JLVA/O.O.S. –A.H.T.

Señor : C.P.C. Mg. AGUSTIN CORONEL ALARCÓN.
Director de la Oficina de Operaciones S.A.H.T.

De : Bach. JOSE LUIS VILLENA ACUÑA.
Informático Oficina de Operaciones S.A.H.T.

Asunto : Data Center e Internet y Propuesta de la NTP ISO 17799.

Fecha : 10 DE MARZO DEL 2014

Es grato dirigirme a Usted para saludarle muy cordialmente y a la vez informarle que los equipos de cómputo del área de Estadística e Informática se detallan a continuación:

El Data Center donde se ubican los servidores de datos tanto del SISTEMA DE INFORMACIÓN DE GESTIÓN ADMINISTRATIVA – SIGA ML y del SISTEMA INTEGRADO DE ADMINISTRACIÓN FINANCIERA – SIAF SP tiene problemas con respecto al acceso de personas no autorizadas por no contar con un ambiente adecuado y con sistema de aire acondicionado, reinicia constantemente, por tener programas de digitación como son: HIS, SEM, SIEN, NOTI-SP, REHIS y otros programas; el Equipo de cómputo en mención está sin los UPS para evitar el corte de energía eléctrica.

Además el área de estadística e informática no cuenta con red de datos e internet para él envió de información oportuna; por falta de una red estructurada de CAT 6.

Se recomienda para la adquisición de UPS para los servidores de datos y una nueva red de cableado estructurado CAT 6.

Adquirir un sistema de aire acondicionado de 24 BTU para mantener los servidores en condiciones normales sabiendo que a temperatura ambiente es elevada y los servidores están encendidos todos los días de la semana, como también adquirir antivirus con licencia corporativos que trabajen en sistemas cliente servidor.

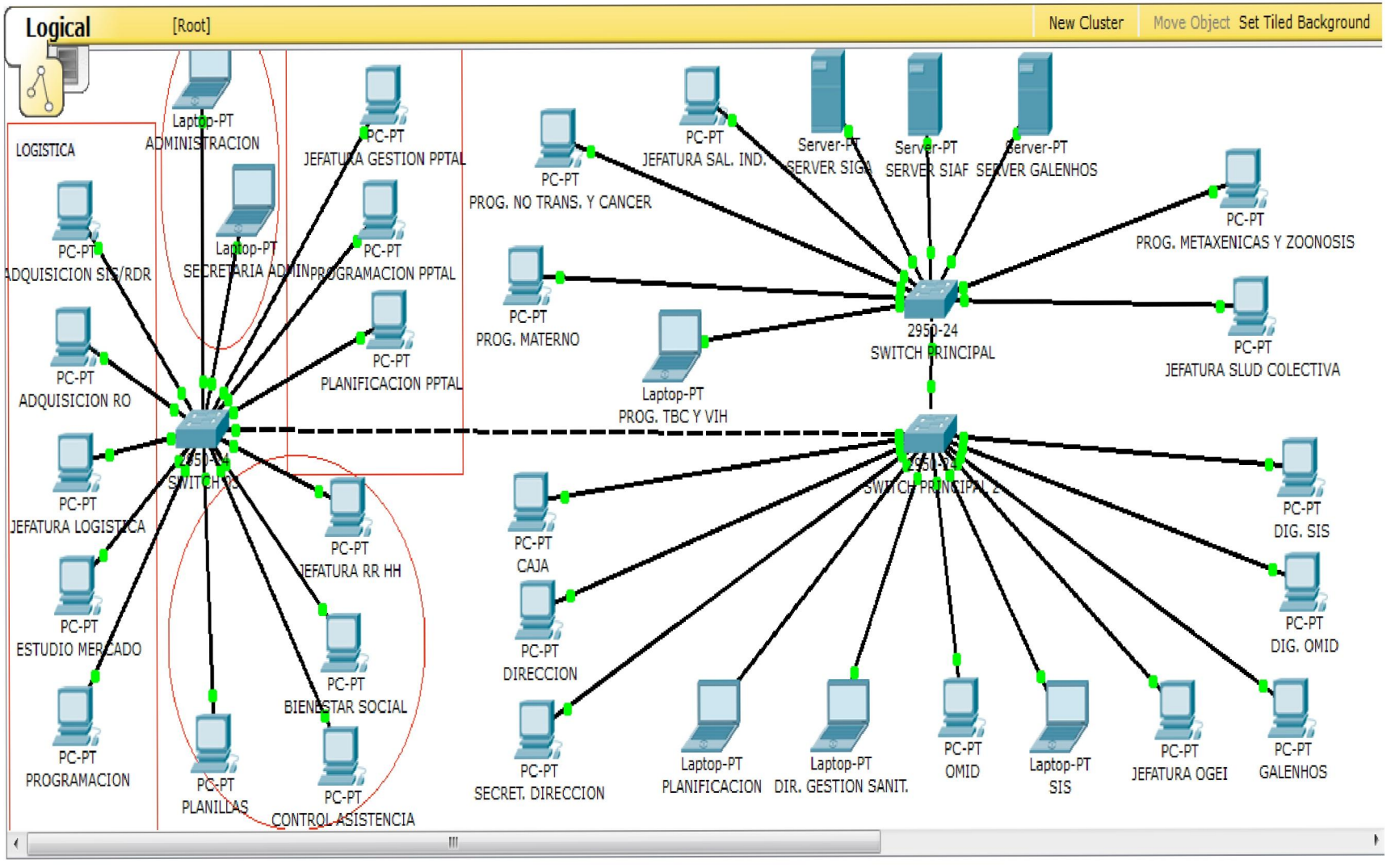
Además le hago llegar la propuesta de la implementación de la NTP ISO 17799 en la Oficina de Operaciones Salud Alto Huallaga Tocache Unidad Ejecutora 403.

Es cuanto informo a Ud. para su conocimiento y fin.

Atentamente.,

Bach. JOSE LUIS VILLENA ACUÑA

ANEXO 03: IINFRAESTRUCTURA ACTUAL DE LA RED INTERNA



UNIVERSIDAD NACIONAL AGRARIA DE LA SELVA

FACULTAD DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS

DEPARTAMENTO ACADEMICO DE CIENCIAS EN INFORMATICA Y SISTEMAS

APLICACIÓN DE LA NORMA TECNICA PERUANA ISO 17799 AL DESARROLLO DEL SISTEMA DE INFORMACIÓN DE GESTIÓN ADMINISTRATIVA SIGA MODULO LOGISTICO EN LA DIRECCIÓN SUBREGIONAL DE SALUD ALTO HUALLAGA UNIDAD EJECUTA 403 TOCACHE

TESINA

Para Optar el Titulo de:

INGENIERO EN INFORMÁTICA Y SISTEMAS

Presentado por:

VILLENA ACUÑA, José Luis

Tingo María – Perú

2015

UNIVERSIDAD NACIONAL AGRARIA DE LA SELVA

FACULTAD DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS

DEPARTAMENTO ACADEMICO DE CIENCIAS EN INFORMATICA Y SISTEMAS

APLICACIÓN DE LA NORMA TECNICA PERUANA ISO 17799 AL DESARROLLO DEL SISTEMA DE INFORMACIÓN DE GESTIÓN ADMINISTRATIVA SIGA MODULO LOGISTICO EN LA DIRECCIÓN SUBREGIONAL DE SALUD ALTO HUALLAGA UNIDAD EJECUTA 403 TOCACHE

TESINA

Para Optar el Titulo de:

INGENIERO EN INFORMÁTICA Y SISTEMAS

Presentado por:

VILLENA ACUÑA, José Luis

Tingo María – Perú

2015

T
SIS

VILLENA ACUÑA, José Luís

"Aplicación de la Norma Técnica Peruana ISO 17799 al Desarrollo del Sistema de Información de Gestión Administrativa – en la Dirección Subregional de Salud Alto Huallaga – Unidad Ejecuta 403 Tocache" 2015

66 páginas; 05 Figuras; 12 Cuadros; 05 ref.; 30 cm.
Tesina (Ingeniero en Informática y Sistemas) Universidad Nacional Agraria de la Selva Tingo María (Perú). Facultad de Ingeniería en Informática y Sistemas

1. FUNDAMENTACIÓN TEÓRICA **2. NTP –ISO/IEC 17799-2007**

3. EST. NTP ISO/IEC 17799-2007 **4. DEFINICIONES METODOLÓGICAS**

DEDICATORIA

A Dios, quién me da la vida y
me guía por mi sendero.

A mis padres:

Jesús Villena Tapara y
Máximiliana Acuña Espinoza.

Por su infinito amor, comprensión, su apoyo moral y espiritual, porque siempre anhelan verme salir adelante.

.A mis hermanos:

Gerardo, Vilma, Fredy, Martha, Elmer y Vanesa.

Por contar siempre con su comprensión y apoyo incondicional.

AGRADECIMIENTO

Mis más sinceros agradecimientos a:

Las personas que conforman la Facultad de Ingeniería en Informática y Sistemas de la UNAS, porque cada día ponen su compromiso de formar profesionales en sistemas e informática útiles para la sociedad.

Los docentes del CAPT FIIS que supieron contribuir con sus conocimientos en mi actualización profesional, asimismo al Ing. Pedro C. Trujillo Natividad, por su asesoramiento en el desarrollo de la tesina.

Dr. Rodolfo David Villalobos Valqui, Director Ejecutivo de la UE-403 Dirección Subregional de Salud Alto Huallaga Tocache, por su consideración para la realización de este respectivo trabajo.

A todo familiar, Profesor, colega y amigo, que de alguna u otra forma contribuyeron a la realización de este trabajo.

INDICE GENERAL

Página

CAPITULO III

INDICE DE CUADROS

Página

INDICE DE FIGURAS

Página

INTRODUCCIÓN

La aplicación de la norma técnica peruana ISO 17799 al desarrollo del sistema de información de gestión administrativa - SIGA ML en la Dirección Subregional de Salud Alto Huallaga – Tocache, brindara muchos beneficios por que permitirá tener el plan de contingencia de todo lo relacionado a la seguridad de la información.

La Red de Servicios de Salud Tocache, está enmarcado dentro de los Lineamientos de la Política del Sector salud, Plan Regional, acuerdos de Gestión, que tiene como eje central las actividades de prevención, promoción, recuperación y de rehabilitación de la salud de la población y las capacidades reales del aparato prestador para atender dichas necesidades, con planes y acciones que compromete al sector a establecer estrategias de trabajo suficientemente creativas y racionales que permitan focalizar y priorizar las acciones hacia los sectores de población más pobre o vulnerable, cuyos ejes principales están el logro de la equidad, la eficiencia y la calidad en la atención en salud, promoviendo el desarrollo social.

Los Lineamientos de Política Sectorial 2002-2014 y Fundamentos para el Plan Estratégico Institucional 2007-2014, señala los principios básicos en las cuáles se sustentan las acciones y resultados a alcanzar el 2014; siendo uno de los principales mecanismos para el logro de los objetivos el planeamiento sanitario que mediante las herramientas disponibles se consolidan como instrumento de gestión para reflejar el accionar de salud que realiza la Dirección Ejecutiva de la Red de Servicios de Salud de Tocache.

El Equipo de Gestión de la Dirección Subregional de Salud Tocache, ha formulado el Análisis de la Situación de Salud, sobre la base de las necesidades y problemas de las micro redes Tocache, Uchiza, Progreso y Pólvora, Hospital II-1 Tocache, así como los establecimientos de salud, además como documento de gestión institucional, cuyas acciones conllevará al cumplimiento de las metas del Plan Estratégico Institucional 2007-2014.

CAPITULO I
GENERALIDADES

1.1. ACERCA DE LA INSTITUCION

1.1.1. DESCRIPCION DE LA INSTITUCION

La Red de Servicios de Salud Tocache se crea mediante Resolución Regional N° 695 el 01 de Noviembre del año 2001 bajo la dirección del Psicólogo Roberto López Cahuaza, siendo Director Regional de Salud San Martin el Dr. Pedro Bogarin Vargas; durante la Dirección del Dr. Carlos Alberto del Aguila el 29 de diciembre del 2004 se traslada la sede administrativa con todos los equipos y mobiliarios de los ambientes del Hospital Rural de Tocache a los ambientes remodelados del ex Centro de Salud y que a la actualidad viene funcionando todo el sistema administrativo de la Unidad Ejecutora 403 - Alto Huallaga; se encuentra situada en la zona sur de la Región San Martín del territorio del Perú, ocupa el sector medio del valle formado por el río Huallaga, zona de recursos naturales que conecta la sierra sur con la selva baja, oscilando su altitud entre 300 m.s.n.m. (distrito El Pólvora) y los 2,700 m.s.n.m. (distrito de Shunte).

Actualmente la red de servicios de salud cuenta con 32 establecimientos de salud en la provincia de Tocache- San Martin.

1.1.2. UBICACIÓN GEOGRAFICA

Departamento : San Martin- Perú

Provincia : Tocache

Distrito : Tocache

Dirección : Av. Ricardo Palma N° 550

Institución : “Dirección Subregional de Salud Alto Huallaga Tocache” (DSRSAHT-UE 403).

1.1.3. BASE LEGAL

- Constitución Política del Perú.
- Ley Nº 27657, Ley del Ministerio de Salud y su Reglamento, aprobado por D.S. Nº 013-2002-SA.
- Ley Nº 28411, Ley General del Sistema Nacional de Presupuesto Público.
- Ley Nº 28522; Ley del Sistema Nacional de Planeamiento Estratégico y del Centro Nacional de Planeamiento Estratégico (CEPLAN).
- Ley Nº.27783, Ley de Bases de la Descentralización
- Ley Nº.27867, Ley Orgánica de Gobiernos Regionales, Artículos
- Ley Nº.27658, Ley Marco de la Modernización de la Gestión del Estado.
- Decreto Supremo Nº 014-2002-SA Reglamento de Organización y Funciones del Ministerio de Salud.

- Decreto Supremo N° 163-2004/EF, establece disposiciones para la mejora de la calidad del gasto público y crea el Sistema de Seguimiento y Evaluación del Gasto Público.
- Resolución Suprema N° 014-2002-SA, que aprueba los Lineamientos de Política Sectorial para el período 2002 – 2012 y Principios Fundamentales para el Plan Estratégico Sectorial del Quinquenio agosto 2001 – julio 2006.
- Resolución Directoral Nº 003-2003-EF/68.01 que aprueba la Directiva para la reformulación de los Planes Estratégicos Sectoriales Multianuales para el periodo 2004-2006.
- Resolución Directoral Nº 030-2005-EF/76.01 que aprueba la Directiva para la Programación y Formulación del Presupuesto de los Pliegos del Gobierno Nacional para el año fiscal 2006.
- Resolución Ministerial Nº 665-2004/MINSA que aprueba la directiva para la formulación, seguimiento y evaluación de los planes operativos 2005 de las entidades y dependencias del MINSA.
- Resolución Ministerial Nº 566-2005/MINSA que aprueba los lineamientos para la adecuación de la organización de las Direcciones Regionales de Salud en el marco del proceso de descentralización.
- Resolución Ministerial Nº 729-2003 SA/DM que aprueba el documento La Salud Integral: Compromiso de Todos – El Modelo de Atención Integral de Salud.

1.1.4. FUNCIONES DE LA INSTITUCION:

La Dirección Ejecutiva de la Red Ejecutora de Salud es la unidad orgánica de conducción de la Red de Salud, responsable de su dirección, conducción y gestión. Está encargada de dirigir, coordinar y supervisar su funcionamiento y administrar los recursos (humanos, financieros, y materiales) que se le asigna para el cumplimiento de sus fines; así como organizar y conducir técnica y administrativamente al hospital local y Micro redes a su cargo, así como tener responsabilidad en la gestión de los sistemas administrativos, recursos financieros, bienes, servicios y brindar soporte administrativo a las redes operativas que lo conforman.

Las funciones específicas de la Dirección Ejecutiva de la Red Ejecutora de Salud son las siguientes:

a) Dirigir la elaboración de propuestas, difusión y aplicación de prioridades sanitarias y políticas provinciales sectoriales e intersectoriales que influyen sobre la salud, tomando en consideración las políticas del desarrollo social de la región y las prioridades sanitarias nacionales y regionales.

b) Dirigir la participación de la red en la formulación, difusión, asistencia técnica, implementación, aplicación y control de modelos, metodologías, tecnologías, lineamientos, normativa y procedimientos para los procesos técnicos de organización y funcionamiento de servicios públicos de salud de las personas y servicios de salud ambiental y ocupacional; para la promoción, protección, recuperación y rehabilitación de salud de las personas, salud ambiental y ocupacional, productos farmacéuticos y afines y la atención

farmacéutica, gestión institucional de recursos humanos; suministro de medicamentos e insumos médico quirúrgicos y odontológicos, investigación en salud; gestión y mantenimiento de recursos físicos y logística en el ámbito de la red de salud; proponer adecuaciones a la DIRES.

c) Identificar y promover prioridades sanitarias, de aseguramiento público e investigación en salud en la red de salud.

d) Dirigir la aplicación de metodologías de análisis y participación en la formulación del planeamiento estratégico sectorial e institucional y operativo de salud en la región; conducir, formular, dirigir, controlar y evaluar los planes estratégicos y operativos, programas y proyectos de intervención e inversiones en salud, acuerdos de gestión y anteproyectos de presupuesto para la unidad ejecutora de salud y de su red de salud; apoyar a los gobiernos locales de su jurisdicción en la formulación de su plan estratégico sectorial de salud y elevar propuestas a la DIRES.

e) Conducir la formulación, implementación y control de propuestas de desarrollo organizacional, documentos de organización de la Red y documentos normativos de gestión en los procesos de competencia de la red de salud; dirigir, conducir y controlar la implementación de la estructura, sistemas y procesos organizacionales de las unidades orgánicas de la dirección de red de salud y sus micro redes.

f) Conducir selección de personal y designar al personal responsable de gestión de la red de salud y sus micro redes.

g) Dirigir la elaboración y elevar las solicitudes de autorización sanitaria de apertura, certificados de habilitación y acreditación y licencias de funcionamiento para los establecimientos de salud y de establecimientos farmacéuticos de su responsabilidad en la red de salud; supervisar y mantener las condiciones que las facultan.

h) Dirigir y controlar la programación, almacenamiento, distribución y control de los medicamentos e insumos médico quirúrgicos y odontológicos de su red de salud y micro redes; así como las coordinaciones para su adquisición en el nivel regional y nacional y ejecución de compras de emergencia de la unidad ejecutora de salud.

i) Conducir y controlar la organización, diseño y gestión de la red de salud, sistemas de soporte de red y de laboratorio, acciones intersectoriales y servicios de atención integral, promoción y protección de la salud de las personas, salud ambiental y ocupacional, en coordinación con los gobiernos locales.

j) Dirigir la participación de la red en la formulación de la propuesta de red de servicios, unidades de gestión, carteras de servicios de establecimientos y sistemas de soporte de red y de laboratorio para la atención integral de la salud de las personas, la salud ambiental y ocupacional para el ámbito de la red de salud.

k) Informar a las autoridades competentes sobre el incumplimiento de la permanencia de regentes en establecimientos farmacéuticos públicos y privados de su ámbito, en coordinación con los gobiernos locales.

l) Dirigir la formulación, ejecución y supervisión de planes, estrategias y acciones intersectoriales de promoción, protección y recuperación de la salud de las personas, salud ambiental y ocupacional, uso racional de medicamentos y para la prevención y control de epidemias, emergencias y desastres; proponer al gobierno regional y a los gobiernos locales de su ámbito proyectos y programas de intervención sectorial e institucional y participar en su ejecución.

m) Dirigir y controlar la planificación, programación, obtención, administración, asignación, ejecución y control de los recursos financieros para la unidad ejecutora y en la red de salud según plan y normatividad vigente; definir la disponibilidad de recursos para sus redes y Micro redes y asignar los fondos correspondientes por encargo.

n) Coordinar la identificación de proveedores de servicios de salud para el seguro público de salud, monitorear las atenciones relacionadas al aseguramiento público en salud y dar facilidades para la auditoría en la red de salud.

o) Dirigir la planificación, reclutamiento, selección, contratación, incorporación, control y desarrollo de personal de su red de salud; proponer a la DIRES el nombramiento de personal; efectuar las acciones de protección social de los recursos humanos en los servicios públicos de salud de la red.

p) Dirigir la administración del personal de los programas de internado y segunda especialización asignado a su red de salud, en concordancia con los lineamientos nacionales y regionales.

q) Dirigir la administración de las remuneraciones y pensiones y cese del personal de la red ejecutora de salud.

r) Dirigir la programación de inversiones en servicios públicos; así como la gestión y operación de proyectos de inversión pública en salud de la red de salud, según estándares establecidos; gestionar los recursos humanos requeridos para la operación de los proyectos en la unidad ejecutora.

s) Conducir la participación de la red en la definición de la organización y funcionamiento del sistema de información sanitaria del ámbito regional; así como en la adecuación y definición de su sistema de información en salud complementario al nacional y regional según las necesidades de la red; conducir la aplicación, difusión y supervisión del uso de normas y estándares de gestión de información en salud.

t) Conducir el desarrollo y mantenimiento de la plataforma tecnológica, soporte técnico y mantenimiento operativo los sistemas de información, telecomunicaciones y telemática en la red de salud, en el marco de las políticas, recomendaciones, normas y estándares nacionales y regionales.

u) Conducir la obtención, verificación, registro, ordenamiento, clasificación, consolidación, procesamiento, almacenamiento y análisis de la información para la gestión sanitaria para los procesos de su red de salud; así como la planificación y ejecución de la comunicación y difusión de información en salud para la educación de su público objetivo y gestión de los procesos institucionales de su competencia.

v) Dirigir la formulación, desarrollo, promoción, articulación de alianzas y difusión de resultados de investigación en salud; formular, desarrollar, promover, articular alianzas para los proyectos de investigación en salud.

w) Dirigir y supervisar la difusión, aplicación, promoción, formulación y cumplimiento de planes, estrategias y cumplimiento de normativa de promoción y vigilancia de los derechos y responsabilidades ciudadanos en salud y de la participación ciudadana en su ámbito de competencia de su red de salud.

x) Conducir la planificación, presupuestación y ejecución de la gestión institucional de los recursos físicos y los sistemas logísticos de la unidad ejecutora de salud, asignando en custodia y controlando su uso, identificando sus requerimientos y especificaciones técnicas, programando su distribución y mantenimiento; así como ejecución de procesos de altas, bajas y enajenaciones de sus activos fijos; asignar recursos físicos a las redes y Micro redes de salud de su ámbito de responsabilidad.

y) Dirigir la supervisión, monitoreo y evaluación de los procesos de organización institucional; organización y gestión de servicios públicos de promoción, protección, recuperación y rehabilitación de la salud de las personas; organización y gestión de servicios de salud ambiental y ocupacional, gestión institucional de recursos humanos, gestión de información y desarrollo informático en salud, gestión de la investigación; promoción, protección y garantía de derechos ciudadanos en salud y participación ciudadana en el ámbito de la red de salud.

z) Dirigir la participación de la red en la evaluación de los procesos de emisión de políticas de salud, evaluación del desempeño institucional y del sector, regulación sectorial de salud de las personas, regulación sectorial de salud ambiental y ocupacional, regulación sectorial de medicamentos e insumos, organización y gestión de servicios de salud de promoción, protección, recuperación y rehabilitación de la salud de las personas y de salud ambiental y ocupacional; suministro de medicamentos e insumos médico quirúrgico, odontológicos y de laboratorio; gestión de información y desarrollo informático, gestión de la investigación en salud de la región.

aa) Supervisar la ejecución presupuestaria y controlar la evaluación de resultados de gestión financiera en la unidad ejecutora.

bb) Dirige, conduce, monitorea y evalúa los procesos de selección y adquisición de bienes, servicios y obras en el ámbito de su jurisdicción.

cc) Otras que le sean asignadas en el marco de la normativa vigente.

1.1.5. MISIÓN:[1]

"Somos una Red de Servicios de Salud que brinda atenciones integrales de salud con recursos humanos competitivos, para satisfacer necesidades de salud con calidez y eficiencia; promoviendo la integración intercultural y estilos de vida saludables según niveles de atención, liderando actividades preventivo promocionales de salud en concertación con las instituciones representativas, priorizando a las comunidades de difícil accesibilidad a los servicios de salud de acuerdo a su perfil epidemiológico".

[1] **FUENTE**: ROF INSTITUCIONAL APROBADO CON RESOLUCIÓN DE GOBIERNO REGIONAL DE SAN MARTIN

1.1.6. VISIÓN: [2]

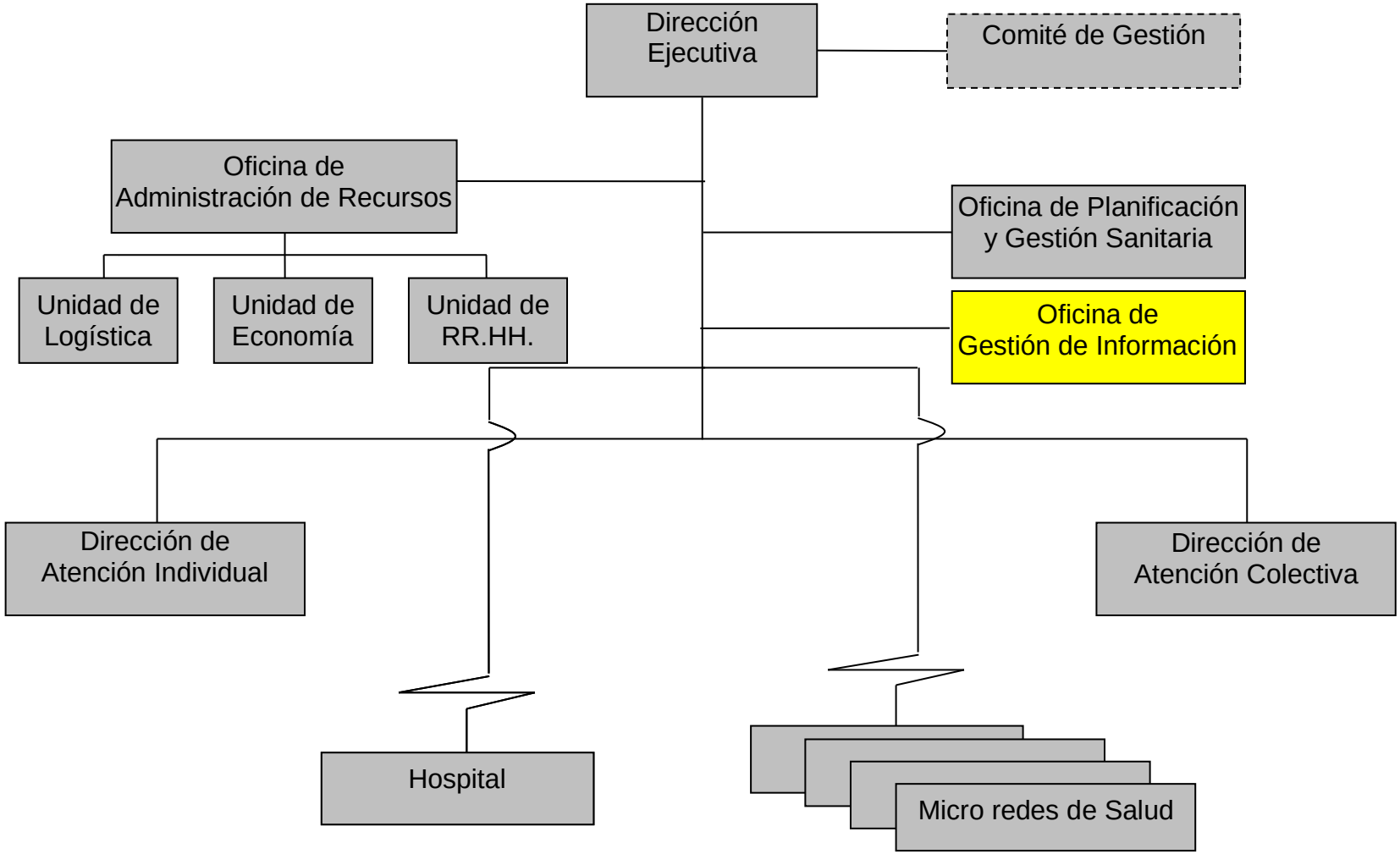
"Al 2014 la Red de Servicios de Salud Tocache será una Institución descentralizada y desconcentrada de la DIRES SM, brindando atención integral con calidad, calidez y equidad; con un nivel altamente competitivo y capacidad resolutiva, con accesibilidad a una población organizada que se compromete y participa en las acciones de salud a través de sus Micro redes eficientemente articuladas".

1.1.7. ORGANIZACIÓN INSTITUCIONAL.

Para el cumplimiento de las funciones, la Dirección Subregional de Salud Alto Huallaga - Unidad Ejecutora 403, cuenta con la siguiente estructura orgánica.

[2] **FUENTE**: ROF INSTITUCIONAL APROBADO CON RESOLUCIÓN DE GOBIERNO REGIONAL DE SAN MARTIN

ORGANIGRAMA DE LA DIRECCION SUBREGIONAL DE SALUD ALTO HUALLAGA TOCACHE[3]



[3] **FUENTE**: ROF INSTITUCIONAL APROBADO CON RESOLUCIÓN DE GOBIERNO REGIONAL DE SAN MARTIN

CAPITULO II
DESCRIPCION DEL PROBLEMA

2.1 SITUACION ACTUAL

Las Entidades de la Administración Pública enfrentan constantes ataques internos y externos a la Seguridad de la Información, y puesto que cuentan con presupuestos limitados, es difícil determinar la prioridad con la que una vulnerabilidad de Seguridad debe ser atendida, a fin de cubrir las vulnerabilidades primarias, sin embargo esto puede implicar una inversión significativa.

Son, por ejemplo, los trámites documentarios, las transferencias electrónicas de dinero o de documentos, la mensajería electrónica, los diversos servicios.

Actualmente la Dirección Subregional de Salud Alto Huallaga - Unidad Ejecutora 403, cuenta con la implementación del sistema de información de gestión administrativa SIGA, lo cual cuenta con tres módulos que son: SIGA-ML (Modulo Logístico), SIGA-PPR (Modulo Presupuesto por Resultados), SIGA-MP (Modulo Patrimonio).

El SIGA-ML sirve para la elaboración de órdenes de compra así como órdenes de servicio la Institución, entre otros.

El SIGA-PPR sirve para la programación de presupuesto de los diferentes programas estratégicos como son: Programa Articulado Nutricional, Materno Neonatal, TBC/VIH, Metaxenicas y Zoonosis, Enfermedades no transmisibles, Control y Prevención del Cáncer.

SIGA-MP sirve para la el control de los bienes patrimoniales de la Institución, entre otros.

El SIGA que actualmente se utiliza en la Dirección Subregional de Salud Alto Huallaga - Unidad Ejecutora 403 es de uso para los trabajadores, permitiéndoles solo el acceso a las personas que cuentan con su respectivo usuario y contraseña.

Debido a que no cuenta con una documentación que sea referente a la aplicación de la NTP peruana ISO 17799, se ha visto la necesidad de implementar una documentación con la Aplicación de este Estándar para tener mayor seguridad de la información.

2.2 OBJETIVOS:

GENERAL

Desarrollar la documentación utilizando la norma técnica peruana ISO 17799 en el desarrollo del Sistema de Información de Gestión Administrativa en la Dirección Subregional de Salud Alto Huallaga Tocache.

ESPECIFICOS

- Desarrollar la documentación con la norma técnica peruana ISO 17799 en el Sistema de Información de Gestión Administrativa, que permita administrar de manera centralizada las información del Siga.
- Implantar la documentación con la norma técnica peruana ISO 17799.
- Implementar de controles para la seguridad de la información.

2.3 JUSTIFICACIÓN

En la actualidad las entidades de la Administración pública se encuentran obligadas por la regulación peruana a cumplir con la norma técnica peruana NTP/ISO-IEC 17799, la cual está basada en el estándar ISO 27002. Sin embargo, puesto que esta norma técnica solamente hace referencia a la implementación de controles, debe ser completada con un sistema de análisis de riesgo que permita priorizar los controles y determinar las áreas de la organización sobre las cuales deben implementarse, a fin de optimizar la inversión económica y garantizar que solamente se implementen aquellos controles cuya inversión sea menor que la pérdidas por vulnerabilidades de seguridad.

El análisis de riesgo basado en los estándares ISO 27001:2005 e ISO 27005:2008, para las entidades de la Administración Pública, a fin de permitir recomendar los controles de seguridad que deben implementarse desde la formación de estos sistemas, estos controles estarán basados en el ISO 27002 e ITIL v3.

El presente trabajo sobre la aplicación de la norma técnica ISO 17799 en el desarrollo del Sistema de Información de Gestión Administrativa - SIGA ML en la Dirección Subregional de Salud Alto Huallaga Tocache, tiene por finalidad socializar al personal administrativo referente a la seguridad de la información de la institución.

CAPITULO III
FUNDAMENTACIÓN TEORICA

3.1 ANTECEDENTES

Actualmente la Dirección Subregional de Salud Alto Huallaga Tocache no Cuenta con un trabajo realizado sobre seguridad de la información, es decir aplicando la norma técnica peruana ISO 17799 al desarrollo del sistema de información de gestión administrativa SIGA- ML.

A nivel de la región San Martín existe poca información desarrollada con la aplicación de la norma técnica peruana.

A nivel nacional existen diferentes entidades que si han aplicado la mencionada norma como es por ejemplo el ministerio de educación, la RENIEC, universidades y otros.

3.2 BASES TEORICAS

3.2.1 Norma Técnica Peruana NTP-ISO/IEC 17799:2007

La presente Norma Técnica Peruana ha sido elaborada por el Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos (EDI), durante los meses de junio a julio del 2006, utilizando como antecedente a la Norma ISO/IEC 17799:2005.

El Comité Técnico de Normalización de Codificación e Intercambio Electrónico de Datos (EDI) presentó a la Comisión de Reglamentos Técnico y Comerciales CRT, con fecha 2006-07-21, el PNTP-ISO/IEC 17799:2006 para su revisión y aprobación; siendo sometido a la etapa de Discusión Pública el 2006-11-25.

No habiéndose presentado observaciones fue oficializada como Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información, 2ª Edición, el 22 de enero del 2007.

Esta Norma Técnica Peruana es una adopción de la Norma ISO/IEC 17799:2005. La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español a sido estructurada de acuerdo a las Guías Peruanas GP 001:1995 y GP 002:1995.

3.2.2 Estructura de la NTP-ISO/IEC 17799:2007

Este estándar contiene 11 cláusulas de control de seguridad que contienen colectivamente un total de 39 categorías principales de seguridad y una cláusula introductoria conteniendo temas de evaluación y tratamiento del riesgo.

Cláusulas

Cada cláusula contiene un número de categorías principales de seguridad. Las 11 cláusulas (acompañadas por el número de categorías principales de seguridad incluidas en cada cláusula) son:

1) Política de seguridad (1);
2) Organizando la seguridad de información (2);
3) Gestión de activos (2);
4) Seguridad en recursos humanos (3);
5) Seguridad física y ambiental (2);

6) Gestión de comunicaciones y operaciones (10);
7) Control de acceso (7);
8) Adquisición, desarrollo y mantenimiento de sistemas de información(6);
9) Gestión de incidentes de los sistemas de información (2);
10) Gestión de la continuidad del negocio (1);
11) Cumplimiento (3)

El orden de las cláusulas en este estándar no implica su importancia. Dependen de las circunstancias, todas las cláusulas pueden ser importantes, por lo tanto cada organización que aplica este estándar debe identificar cláusulas aplicables, que tan importantes son y sus aplicaciones para procesos de negocios individuales. Igualmente, todas las listas de este estándar no se encuentran en orden de prioridad a menos que se notifique lo contrario.

3.2.3 ¿Qué es la 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 está 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 protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocios.

La seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, 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.

3.2.4 ¿Por qué es necesaria la seguridad de la información?

La información y los procesos que la apoyan, los sistemas y redes son importantes activos de la organización. Definir, realizar, mantener y mejorar la seguridad de información, puede ser esencial para mantener la competitividad, flujo de liquidez, rentabilidad, cumplimiento de la legalidad e imagen comercial.

Las organizaciones y sus sistemas de información se enfrentan, cada vez más, con riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, espionaje, sabotaje, vandalismo, incendios o inundaciones. Ciertas fuentes de daños como virus

informáticos y ataques de intrusión o de negación de servicios se están volviendo cada vez más comunes, ambiciosos y sofisticados.

La seguridad de información es importante en negocios tanto del sector público como del privado y para proteger las infraestructuras críticas. En ambos sectores, la seguridad de información permitirá, por ejemplo lograr el gobierno electrónico o el comercio electrónico, evitando y reduciendo los riesgos relevantes. La interconexión de las redes públicas y privadas y el compartir los recursos de información aumentan la dificultad de lograr el control de los accesos. La tendencia hacia la informática distribuida debilita la eficacia de un control central y especializado.

Muchos sistemas de información no se han diseñado para ser seguros. La seguridad que puede lograrse a través de los medios técnicos es limitada, y debería apoyarse en una gestión y procedimientos adecuados. La identificación de los controles que deberían instalarse requiere una planificación cuidadosa y una atención al detalle. La gestión de la seguridad de la información necesita, como mínimo, la participación de todos los empleados de la organización. También puede requerir la participación de los proveedores, clientes o accionistas. La asesoría especializada de organizaciones externas también puede ser necesaria.

3.2.5 ¿Cómo establecer los requisitos de seguridad?

Es esencial que la organización identifique sus requisitos de seguridad. Existen tres fuentes principales.

a) La primera fuente procede de la valoración de los riesgos de la organización, tomando en cuenta los objetivos y estrategias generales del negocio. Con ella se identifican las amenazas a los activos, se evalúa la vulnerabilidad y la probabilidad de su ocurrencia y se estima su posible impacto.

b) La segunda fuente es el conjunto de requisitos legales, estatutos, regulaciones y contratos que debería satisfacer la organización, sus socios comerciales, los contratistas y los proveedores de servicios.

c) La tercera fuente está formada por los principios, objetivos y requisitos que forman parte del tratamiento de la información que la organización ha desarrollado para apoyar sus operaciones.

3.2.6 Evaluación de los riesgos de seguridad

Los requisitos de seguridad se identifican mediante una evaluación metódica de los riesgos. El gasto en controles debería equilibrarse con el posible impacto económico, resultante de los fallos de seguridad.

Los resultados de ésta evaluación ayudarán a encauzar y determinar una adecuada acción gerencial y las prioridades para gestionar los riesgos de seguridad de la información, y la implantación de los controles seleccionados para protegerse contra dichos riesgos.

Las evaluaciones de riesgos deben repetirse periódicamente para tener en cuenta cualquier cambio que pueda influir en los resultados de la evaluación.

3.2.7 Selección de controles

Una vez que los requisitos de seguridad han sido identificados y las decisiones para el tratamiento de riesgos han sido realizadas, deberían elegirse e implantarse los controles que aseguren la reducción de los riesgos a un nivel aceptable. Pueden elegirse los controles partiendo de este documento, de otros conjuntos de controles o de nuevos controles que pueden diseñarse para cubrir adecuadamente las necesidades específicas. La selección de los controles de seguridad depende de las decisiones organizacionales basadas en el criterio para la identificación y clasificación de riesgos, las opciones para el tratamiento de estos y la gestión general de riesgos aplicable a la organización. Así mismo, debe ser sujeto a toda regulación y legislación nacional e internacional.

Ciertos controles expuestos en este documento, pueden considerarse como principios que guían la gestión de la seguridad de la información, aplicables a la mayoría de las organizaciones. Estos se explican en más detalle en el siguiente inciso denominado “Punto de partida de la seguridad de la información”.

3.2.8 Punto de partida de seguridad de la información

Cierto número de controles se consideran principios orientativos que proporcionan un punto de partida adecuado para implantar la seguridad de la información. Se apoyan en requisitos legislativos esenciales o se considera la mejor práctica habitual para conseguir dicha seguridad.

Los controles que se consideran esenciales para una organización desde un punto de vista legislativo comprenden:

a) La protección de los datos de carácter personal y la intimidad de las personas;

b) La salvaguarda de los registros de la organización;

c) Los derechos de la propiedad intelectual.

Los controles que se consideran la mejor práctica habitual para conseguir la seguridad de la información comprenden:

a) La documentación de la política de seguridad de la información;

b) La asignación de responsabilidades de seguridad;

c) La formación y capacitación para la seguridad de la información;

d) El procedimiento correcto en las aplicaciones;

e) La gestión de la vulnerabilidad técnica;

f) La gestión de la continuidad del negocio;

g) El registro de las incidencias de seguridad y las mejoras.

Estos controles pueden aplicarse a la mayoría de las organizaciones y los entornos.

Es conveniente señalar que pese a la importancia dada a los controles en este documento, la importancia de cualquier control debería determinarse a la luz de los riesgos específicos que afronta la organización. Por tanto y aunque el enfoque anterior se considere un buen punto de partida, no sustituye a la selección de controles basada en una evaluación del riesgo.

3.3 DEFINICIONES OPERACIONALES

3.3.1 Base de Datos[4]

Una base de datos se puede definir como un conjunto de información relacionada que se encuentra agrupada o estructurada.

Desde el punto de vista de la informático, la base de datos es un sistema formado por un conjunto de datos almacenados en discos que permiten el acceso directo a ellos y un conjunto de programas que manipulen ese conjunto de datos.

Una base de datos tiene mucha importancia en el ritmo de vida que llevamos en los actuales momentos, ya que, está acelera el ritmo en el momento realizar una búsqueda de información.

3.3.2 Administración

Es una disciplina que tiene por finalidad dar una explicación acerca del comportamiento de las organizaciones, además de referirse al proceso de conducción de las mismas.

Es ciencia fáctica, tiene un objeto real del mundo de la cultura (las organizaciones). Es técnica porque implica aceptar la existencia de medios específicos utilizables en la búsqueda del funcionamiento eficaz y eficiente de las organizaciones. Es técnica con su bagaje de principios, normas y procedimientos para la conducción racional de las organizaciones.

3.3.3 Activo[5]

Algo que tenga valor para lo organización.

[4] http://www.itlp.edu.mx/publica/tutoriales/basedat1/tema1_1.htm
[5] Fuente: norma técnica peruana NTP-ISO/IEC 17799

3.3.4 Control[6]

Herramienta de la gestión del riesgo, incluidas políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal. Control es también usado como sinónimo de salvaguardia o contramedida.

3.3.5 Pauta

Descripción que aclara que es lo que se debe hacer y cómo se hace, con el fin de alcanzar los objetivos planteados en las políticas.

3.3.6 Instalaciones de proceso de información

Sistemas de información, servicio o infraestructura, o locaciones físicas que los almacena.

3.3.7 Seguridad de la información[7]

Preservación de la confidencialidad, integridad y disponibilidad de la información, así mismo, otras propiedades como la autenticidad, no rechazo, contabilidad y confiabilidad también pueden ser consideradas.

3.3.8 Evento de seguridad de información

Es una ocurrencia identificada de un sistema, servicio, o red el cual indica una posible brecha de la política de seguridad de información o fallas de las salvaguardias o una situación desconocida que puede ser relevante para la seguridad.

[6] Fuente: norma técnica peruana NTP-ISO/IEC 17799
[7] Fuente: norma técnica peruana NTP-ISO/IEC 17799

3.3.9 Incidente de seguridad de información

Es indicado por una o varias series de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de negocios y de amenazar la seguridad de información.

3.3.10 Política[8]

Dirección general y formal expresada por la gerencia.

3.3.11 Riesgo[9]

Combinación de la probabilidad de un evento y sus consecuencias.

3.3.12 Análisis del riesgo[10]

Uso sistemático de la información para identificar fuentes y estimar el riesgo.

3.3.13 Evaluación del riesgo

Proceso general de análisis y evaluación del riesgo.

3.3.14 Valoración del riesgo

Proceso de comparación del riesgo estimado contra el criterio del riesgo dado para determinar el significado de este.

3.3.15 Gestión del riesgo[11]

Actividades coordinadas para dirigir y controlar una organización considerando el riesgo. Gestión del riesgo incluye típicamente evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo y comunicación del riesgo.

[8] Fuente: norma técnica peruana NTP-ISO/IEC 17799
[9] Fuente: norma técnica peruana NTP-ISO/IEC 17799
[10] Fuente: norma técnica peruana NTP-ISO/IEC 17799
[11] Fuente: norma técnica peruana NTP-ISO/IEC 17799

3.3.16 Tratamiento del riesgo

Proceso de selección e implementación de medidas para modificar el riesgo.

3.3.17 Terceros

Persona que es reconocida por ser independiente de las partes involucradas concerniente al tema en cuestión.

3.3.18 Amenaza

Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización.

3.3.19 Vulnerabilidad

Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas.

3.4 DEFINICIONES METODOLOGICAS

El alcance del presente documento está limitado a establecer los controles requeridos por la NTP-ISO 17799:2004 y el dominio 9 de la norma NTP-ISO 17799:2007 llamado “Administración de Incidentes”. Dichos controles se detallan a continuación:

1. Políticas de Seguridad

#	Objetivo de Control	#	Actividad de Control
1.1	Políticas de Seguridad de la Información	1.1.1	Documento de política de seguridad de la información y revisión de la evaluación.

Cuadro 01: Dominio 01 de la NTP ISO 17799.

2. Aspectos Organizativos para la Seguridad

#	Objetivo de Control	#	Actividad de Control
2.1	Estructura para la seguridad de la información	2.1.1	Comité de gestión de seguridad de la información
		2.1.2	Coordinación de la seguridad de la información
		2.1.3	Asignación de responsabilidades sobre seguridad de la información
		2.1.4	Proceso de autorización de recursos para el tratamiento de la información
		2.1.5	Asesoramiento de especialistas en seguridad de la información
		2.1.6	Cooperación entre organizaciones
		2.1.7	Revisión independiente de la seguridad de la información
2.2	Seguridad en los accesos de	2.2.1	Identificación de riesgos por el acceso de terceros

#	Objetivo de Control	#	Actividad de Control
	terceras partes	2.2.2	Requisitos de seguridad en contratos con terceros
2.3	Outsourcing	2.3.1	Requisitos de seguridad en contratos de Outsourcing

Cuadro 02: Dominio 02 de la NTP ISO 17799.

3. Clasificación y Control de Activos

#	Objetivo de Control	#	Actividad de Control
3.1	Responsabilidad sobre los activos	3.1.1	Inventario de activos
3.2	Clasificación de la información	3.2.1	Guías de Clasificación
		3.2.2	Marcado y tratamiento de la información

Cuadro 03: Dominio 03 de la NTP ISO 17799.

4. Seguridad Ligado al Personal

#	Objetivo de Control	#	Actividad de Control
4.1	Seguridad en la definición del trabajo y los recursos	4.1.1	Inclusión de la seguridad en las responsabilidades laborales
		4.1.2	Selección y política de personal
		4.1.3	Acuerdos de confidencialidad
		4.1.4	Términos y condiciones de la relación laboral
4.2	Formación de usuarios	4.2.1	Formación y capacitación en seguridad de la información
4.3	Respuesta ante incidencias y	4.3.1	Comunicación de las incidencias de seguridad

#	Objetivo de Control	#	Actividad de Control
	malos funcionamientos de la seguridad	4.3.2	Comunicación de las debilidades de seguridad
		4.3.3	Comunicación de los fallos del software.
		4.3.4	Aprendiendo de las incidencias
		4.3.5	Procedimiento disciplinario

Cuadro 04: Dominio 04 de la NTP ISO 17799.

5. Seguridad Física y Del Entorno

#	Objetivo de Control	#	Actividad de Control
5.1	Áreas seguras	5.1.1	Perímetro de seguridad física
		5.1.2	Controles físicos de entradas
		5.1.3	Seguridad de oficinas, despachos y recursos
		5.1.4	El trabajo en las áreas seguras
		5.1.5	Áreas aisladas de carga y descarga
5.2	Seguridad de los equipos	5.2.1	Instalación y protección de equipos
		5.2.2	Suministro eléctrico
		5.2.3	Seguridad del cableado
		5.2.4	Mantenimiento de equipos
		5.2.5	Seguridad de equipos fuera de los locales de la organización
		5.2.6	Seguridad en el re-uso o eliminación de equipos
5.3	Controles Generales	5.3.1	Política de puesto de trabajo despejado y bloqueo de pantalla

Cuadro 05: Dominio 05 de la NTP ISO 17799.

6. Gestión de Comunicaciones y Operaciones

#	Objetivo de Control	#	Actividad de Control
6.1	Procedimientos y responsabilidades de operación	6.1.1	Documentación de procedimientos operativos
		6.1.2	Control de cambios operacionales
		6.1.3	Procedimientos de gestión de incidencias
		6.1.4	Segregación de tareas
		6.1.5	Separación de los recursos para desarrollo y para producción
		6.1.6	Gestión de servicios externos
6.2	Planificación y aceptación del sistema	6.2.1	Planificación de la capacidad
		6.2.2	Aceptación del sistema
6.3	Protección contra software malicioso	6.3.1	Medidas y controles contra software malicioso
6.4	Gestión interna de respaldo y recuperación	6.4.1	Recuperación de la información
		6.4.2	Diarios de operación
		6.4.3	Registro de fallos
6.5	Gestión de redes	6.5.1	Controles de red
6.6	Utilización y seguridad de los medios de información	6.6.1	Gestión de medios removibles
		6.6.2	Eliminación de medios
		6.6.3	Procedimientos de manipulación de la información
		6.6.4	Seguridad de la documentación de sistemas
6.7	Intercambio de información y software	6.7.1	Acuerdos para intercambio de información y software
		6.7.2	Seguridad de medios en tránsito
		6.7.3	Seguridad en comercio electrónico
		6.7.4	Seguridad del correo electrónico
		6.7.5	Seguridad de los sistemas ofimáticos
		6.7.6	Sistemas públicamente disponibles

Cuadro 06: Dominio 06 de la NTP ISO 17799.

7. Control de Accesos

#	Objetivo de Control	#	Actividad de Control
7.1	Requisitos de negocio para el control de accesos	7.1.1	Política de control de accesos
7.2	Gestión de acceso de usuarios	7.2.1	Registro de usuarios
		7.2.2	Gestión de privilegios
		7.2.3	Gestión de contraseñas de usuario
		7.2.4	Revisión de los derechos de acceso de los usuarios
7.3	Responsabilidades de usuarios	7.3.1	Uso de contraseñas
		7.3.2	Equipo informático de usuario desatendido
7.4	Control de acceso a la red	7.4.1	Política de uso de los servicios de la red
		7.4.2	Ruta forzosa
		7.4.3	Autenticación de usuarios para conexiones externas
		7.4.4	Autenticación de nodos de la red
		7.4.5	Protección a puertos de diagnóstico remoto
		7.4.6	Segregación en las redes
		7.4.7	Control de conexión a las redes
		7.4.8	Control de enrutamiento en la red
7.5	Control de acceso al sistema operativo	7.5.1	Identificación automática de terminales
		7.5.2	Procedimientos de conexión de terminales
		7.5.3	Identificación y autenticación del usuario
		7.5.4	Sistema de gestión de contraseñas
		7.5.5	Utilización de las facilidades del sistema
		7.5.6	Protección del usuario frente a coacciones
		7.5.7	Desconexión automática de terminales

#	Objetivo de Control	#	Actividad de Control
		7.5.8	Limitación del tiempo de conexión
7.6	Control de acceso a las aplicaciones	7.6.1	Restricción de acceso a la información
		7.6.2	Aislamiento de sistemas sensibles
7.7	Seguimiento de accesos y uso del sistema	7.7.1	Registro de incidencias
		7.7.2	Seguimiento del uso de los sistemas
		7.7.3	Sincronización de relojes

Cuadro 07: Dominio 07 de la NTP ISO 17799.

8. Desarrollo y Mantenimiento de Sistemas

#	Objetivo de Control	#	Actividad de Control
8.1	Requisitos de seguridad de los sistemas	8.1.1	Análisis y especificación de los requisitos de seguridad
8.2	Seguridad de las aplicaciones del sistema	8.2.1	Validación de los datos de entrada
		8.2.2	Control del proceso interno
		8.2.3	Autenticación de mensajes
		8.2.4	Validación de los datos de salida
8.3	Controles criptográficos	8.3.1	Política de uso de los controles criptográficos
		8.3.2	Cifrado
		8.3.3	Firmas digitales
		8.3.4	Servicios de no repudio
		8.3.5	Gestión de claves
8.4	Seguridad de los archivos del sistema	8.4.1	Control del software en producción
		8.4.2	Protección de los datos de prueba del sistema
		8.4.3	Control de acceso a la librería de programas fuente
8.5	Seguridad en los procesos de	8.5.1	Procedimientos de control de cambios
		8.5.2	Revisión técnica de los cambios en el

#	Objetivo de Control	#	Actividad de Control
	desarrollo y soporte		sistema operativo
		8.5.3	Restricciones en los cambios a los paquetes de software
		8.5.4	Canales encubiertos y código Troyano
		8.5.5	Desarrollo externo del software

Cuadro 08: Dominio 08 de la NTP ISO 17799.

9. Gestión de Continuidad del Negocio

#	Objetivo de Control	#	Actividad de Control
9.1	Aspectos de la gestión de continuidad del negocio	9.1.1	Proceso de gestión de la continuidad del negocio
		9.1.2	Continuidad del negocio y análisis de impactos
		9.1.3	Redacción e implantación de planes de continuidad
		9.1.4	Marco de planificación para la continuidad del negocio
		9.1.5	Prueba, mantenimiento y reevaluación de los planes de continuidad

Cuadro 09: Dominio 09 de la NTP ISO 17799.

10. Cumplimiento

#	Objetivo de Control	#	Actividad de Control
10.1	Cumplimiento con los requisitos legales	10.1.1	Identificación de la legislación aplicable
		10.1.2	Derechos de propiedad intelectual (DPI)
		10.1.3	Salvaguarda de los registros de la

#	Objetivo de Control	#	Actividad de Control
			organización
		10.1.4	Evitar el mal uso de los recursos de tratamiento de la información
10.2	Revisiones de la política de seguridad y de la conformidad técnica	10.2.1	Conformidad con la política de seguridad
10.3	Consideraciones sobre la auditoria de sistemas	10.3.1	Controles de auditoria de sistemas
		10.3.2	Protección de las herramientas de auditoria de sistemas

Cuadro 10: Dominio 10 de la NTP ISO 17799.

Controles definidos en la NTP ISO 17799:2007

#	Objetivo de Control	#	Actividad de Control
9.1	Reportando eventos y debilidades de la seguridad de información	9.1.1	Reportando los eventos en la seguridad de información
		9.1.2	Reportando debilidades en la seguridad de información
9.2	Gestión de las mejoras e incidentes en la seguridad de información	9.2.1	Responsabilidades y procedimientos
		9.2.2	Aprendiendo de los incidentes en la seguridad de información
		9.2.3	Recolección de evidencia

CAPITULO IV
DESARROLLO DE LA APLICACIÓN DEL ESTÁNDAR

Los controles de seguridad desarrollados en el presente documento permitirán establecer mejoras a la gestión de la seguridad del Centro de Datos y facilitar el proceso de implementación de los mismos. Por otro lado, las narrativas de cada uno de los controles permitirán establecer una base común para el establecimiento de normas, políticas y procedimientos de seguridad de la información.

A continuación se muestran los principales conceptos relacionados a los controles desarrollados.

4.1 DEFINICIÓN DE TERMINOS

Para identificar adecuadamente a cada responsable que forma parte de la descripción del control se han definido los siguientes términos:

- **COSI:** Comité Operativo de Seguridad de Información.
- **CESI:** Comité Ejecutivo de Seguridad de Información.
- **JOFIN:** Jefe de la Oficina de Informática.
- **OSEG:** Oficial de seguridad de la información.
- **JAIT:** Jefe del Área de Infraestructura Tecnológica.
- **ETIC:** Especialista en Tecnologías de Información y Comunicación.
- **SEC:** Secretaria del Área de Infraestructura Tecnológica.
- **PIES:** Proveedor Interno o Externo del Servicio.

- **USIE:** Usuario Interno o Externo.
- **ASER:** Administrador de Servidores.

4.2 CLASIFICACIÓN DE CONTROLES DE SEGURIDAD

Para una mejor comprensión se explica a continuación el significado de cada uno de los tipos de los controles de seguridad:

De acuerdo al objetivo con el cual está desarrollado cada control, se puede clasificar como:

- **Preventivo:** Permite prevenir que se origine un riesgo.
- **Detectivo:** Permite identificar una incidencia de seguridad de información.
- **Correctivo:** Permite corregir una incidencia de seguridad de información, con el objetivo de minimizar el daño o pérdida que pueda ocasionar la misma.

De acuerdo a como se ejecuta el control, se puede clasificar como:

- **Manual:** Control realizado por una serie de actividades ejecutadas por seres humanos.
- **Automático:** Control apoyado por tecnologías de información, las cuales permiten automatizar el proceso de ejecución del mismo.

4.3 NARRATIVAS DE LOS OBJETIVOS Y ACTIVIDADES DE CONTROL

Los objetivos y controles de seguridad se identificaron como resultado del análisis de la situación actual de la seguridad de información de la Dirección Subregional de Salud Alto Huallaga Tocache y el nivel de cumplimiento requerido por las principales normas de seguridad.

Para una mejor comprensión, los resultados se presentan agrupados por dominio de control dentro de la norma NTP-ISO 17799:2004 y 2007.

El significado de cada columna de la tabla de Objetivos de Control, se muestran a continuación:

#OC: Es el código que permite identificar un Objetivo de Control.

Objetivo de Control: se refiere el nombre del Objetivo de Control de la norma.

Descripción: Se refiere a la descripción de cada Objetivo de Control de la norma.

El significado de cada columna de la tabla de Actividades de control, se muestran a continuación:

#AC: Es el código que permite identificar a una Actividad de Control de la norma.

Actividad de Control: Es la descripción general de cada control definido en la norma.

Tipo de Control: Se refiere a la clasificación asignada a la actividad de control (preventivo, detectivo, correctivo; manual y/o automático).

Responsable de ejecutar el control: Se refiere a los encargados de ejecutar la actividad de control.

Narrativa de la actividad de control: Se refiere a la descripción de las actividades que se requieren establecer para implementar la actividad de control.

Documentación relacionada: Se refiere a la descripción de la documentación (Políticas, Normas, Procedimientos y Estándares) requeridos para cubrir la narrativa de la actividad de control.

Estándar relacionado: Contiene la descripción de los estándares relacionados (NTP-IO/IEC 17799:2004, COBIT e ITIL) a la actividad de control establecida.

Figura 01: Pantalla Inicial del SIGA

Figura 02: Autenticación al SIGA

Figura 03: Módulos del SIGA

Figura 04: Modulo Logística del SIGA

Figura 05: Generación de un pedido de Compra de B/S en el SIGA

A continuación se muestra el detalle del objetivo y control de seguridad desarrollado:

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

# OC	Objetivo de Control	Descripción
8.1	Requisitos de seguridad de los sistemas	OBJETIVO: Asegurar que la seguridad esté imbuida dentro de los sistemas de información. Esto incluirá la infraestructura, las aplicaciones de negocio y las aplicaciones desarrolladas por usuarios. El diseño y la implantación de los procesos de negocio que soportan las aplicaciones o el servicio, pueden ser cruciales para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados antes de desarrollar los sistemas de información.

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.1.1	La Unidad Ejecutora 403 deberá establecer una norma en la que se formalice como necesarias las especificaciones de seguridad que deben ser	• Preventivo Manual	• Responsable de sistemas de información	1. Verificar que se cuente con una norma en la cual se incluya cláusulas en las que se consideren como necesaria la especificación de requisitos de seguridad para los sistemas a ser adquiridos o desarrollados a la medida. 2. Verificar que se cuenta con un procedimiento de gestión de cambios en los que se considere la evaluación de requerimientos considerando aspectos de seguridad, disponibilidad, confidencialidad, integridad e impacto. 3. Verificar que el documento de registro de control de requerimientos de	Normas: Norma de administración de cambios de sistemas de información Procedimiento: Gestión para el cambio en los sistemas de información	NTP-IO/IEC 17799:2004 Análisis y especificación de los requisitos de seguridad COBIT PO2.1, PO9.5, AI1.8, AI1.9, DS5.8 ITIL 7.3, 7.3, 7.2,

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
	analizadas en un desarrollo o mantenimiento a un sistema de información. Frecuencia: Anual			cambio a los sistemas de aplicación se encuentre actualizado.	Documento Estándar: Registro de control de requerimientos	2.6, 7.3, 4.2

# OC	Objetivo de Control	Descripción
8.2	Seguridad de las aplicaciones del sistema	OBJETIVO: Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones. Se deberían diseñar dentro de las aplicaciones (incluidas las aplicaciones escritas por los usuarios) las medidas de control y las evidencias de auditoría o los registros de actividad. Éstos deberían incluir la validación de los datos de entrada, el tratamiento interno y los datos de salida.

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.2.1	La Unidad Ejecutora 403 deberá establecer controles para validar datos de entrada a las aplicaciones de los sistemas para garantizar que estas sean correctas y apropiadas. Frecuencia: Permanente	• Preventivo Manual	• Responsable de sistemas de información	1. Verificar que se cuente con una norma en la cual se incluya cláusulas en el que se indique el uso de controles para los datos de entrada de las aplicaciones, tales como: ▪ Valores fuera de rango ▪ Caracteres inválidos en los campos de datos ▪ Datos que faltan o que están incompletos 2. Verificar que los sistemas de información cuenten con los controles especificados en la Norma de seguridad de las aplicaciones del sistema.	Norma: Norma de seguridad de las aplicaciones del sistema.	NTP-IO/IEC 17799:2004 Validación de los datos de entrada COBIT AI1.8, 2.6.1, AI1.9, AI1.10, AI2.7, AI2.8, AI2.10, AI2.11, AI2.12, AI2.14, DS5.15, DS11.6, DS11.7, DS11.8, DS11.9, DS11.10, DS11.11, DS11.14, DS11.15, DS11.28, DS11.29 ITIL 7.2, 7.3, 5.2, 5.3, 4.3, 5.2,

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
						7, 4.2
8.2.2	La Unidad Ejecutora 403 deberá implementar comprobaciones periódicas para garantizar la integridad de los datos. Frecuencia: Semestral	• Preventivo Manual	• Responsable de sistemas de información	1. Verificar que se cuente con una norma en la cual se incluya una cláusula en la que se especifique la necesidad de realizar pruebas para garantizar la integridad de datos y comprobar que los programas de las aplicaciones se ejecutan en el momento adecuado. 2. Verificar que se realicen comprobaciones periódicas de la integridad de los datos de acuerdo a lo definido en la Norma de seguridad de las aplicaciones del sistema.	Norma: Norma de seguridad de las aplicaciones del sistema.	NTP-IO/IEC 17799:2004 Control del proceso interno COBIT AI1.8, 2.6.1, AI1.9, AI1.10, AI2.7, AI2.8, AI2.10, AI2.11, AI2.12, AI2.14, DS5.15, DS11.6, DS11.7, DS11.8, DS11.9, DS11.10, DS11.11, DS11.14, DS11.15, DS11.28, DS11.29

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
						ITIL 7.2, 7.3, 5.2, 5.3, 4.3, 5.2, 7, 4.2
8.2.3	La Unidad Ejecutora 403 deberá implementar autenticación de mensajes en aplicaciones que requieran protección de la integridad del contenido del mensaje. Frecuencia: Permanente	• Preventivo Manual	• Responsable de sistemas de información	1. Verificar que se cuente con una norma en la cual se incluya cláusulas para el uso de controles de autenticación de mensajes para el caso de las aplicaciones críticas donde se transmite información sensible. 2. Verificar que se han implementado controles de autenticación de mensajes en las aplicaciones críticas donde se transmite información sensible, de acuerdo a la Norma de seguridad de las aplicaciones del sistema.	Norma: Norma de seguridad de las aplicaciones del sistema.	NTP-IO/IEC 17799:2004 Autenticación de mensajes COBIT AI1.8, 2.6.1, AI1.9, AI1.10, AI2.7, AI2.8, AI2.10, AI2.11, AI2.12, AI2.14, DS5.15, DS11.6, DS11.7, DS11.8, DS11.9, DS11.10, DS11.11, DS11.14, DS11.15, DS11.28,

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
						DS11.29 <u>ITIL</u> 7.2, 7.3, 5.2, 5.3, 4.3, 5.2, 7, 4.2
8.2.4	La Unidad Ejecutora 403 deberá validar los datos de salida de un sistema de aplicación para garantizar que el proceso de la información ha sido el correcto. <u>Frecuencia:</u> Semestral	• Preventivo Manual	• Responsable de sistemas de información	1. Verificar que se cuente con una norma en la cual se incluya cláusulas de validaciones de datos de salida para el caso de sistemas críticos. 2. Verificar que se hayan implementado controles de validación de datos de salida para el caso de sistemas críticos de acuerdo a la Norma de seguridad de las aplicaciones del sistema.	<u>Norma:</u> Norma de seguridad de las aplicaciones del sistema.	<u>NTP-IO/IEC 17799:2004</u> Validación de los datos de salida <u>COBIT</u> AI1.8, 2.6.1, AI1.9, AI1.10, AI2.7, AI2.8, AI2.10, AI2.11, AI2.12, AI2.14, DS5.15, DS11.6, DS11.7, DS11.8, DS11.9, DS11.10, DS11.11, DS11.14,

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
						DS11.15, DS11.28, DS11.29 ITIL 7.2., 7.3, 5.2, 5.3, 4.3, 5.2, 7, 4.2

# OC	Objetivo de Control	Descripción
8.3	Controles criptográficos	OBJETIVO: Proteger la confidencialidad, autenticidad o integridad de la información. Se deberían usar sistemas y técnicas criptográficas para proteger la información sometida a riesgo, cuando otras medidas y controles no proporcionen la protección adecuada.

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.3.1	La Unidad Ejecutora 403 deberá desarrollar una política para	• Preventivo • Manual	• Responsable de sistemas de información	1. Verificar que se cuente con una norma en la cual se incluya el uso de controles criptográficos.	Norma: Norma de controles criptográficos.	NTP-IO/IEC 17799:2004 Política de uso de los controles criptográficos

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
	criptografía. Frecuencia: Anual					COBIT PO8.4, PO9.3, DS2.7, DS5.1, DS5.14, DS5.15, DS5.16, DS5.17, DS5.18, DS11.27, DS11.28 ITIL 4.1, 2.3, 4.2
8.3.2	La Unidad Ejecutora 403 deberá implementar la técnica criptográfica de cifrado para proteger la informació	• Preventivo Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma en la cual se incluya el uso de la técnica criptográfica de cifrado para proteger la información crítica o sensible para la organización. 2. Verificar la implementación de controles criptográficos en las aplicaciones que manejan información sensible de acuerdo a lo definido en la	Norma: Norma de controles criptográficos.	NTP-IO/IEC 17799:2004 Cifrado COBIT PO8.4, PO9.3, DS2.7, DS5.1, DS5.14,

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
	n considerada como sensible para la organización. Frecuencia: Permanente			Norma de controles criptográficos.		DS5.15, DS5.16, DS5.17, DS5.18, DS11.27, DS11.28 ITIL 4.1, 2.3, 4.2
8.3.3	La Unidad Ejecutora 403 deberá implementar el uso de firmas digitales para proteger la autenticidad e integridad de los documentos electrónicos.	• Preventivo • Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma en la cual se incluya el uso de firmas digitales para proteger la integridad de documentos electrónicos considerados críticos para organización y para aplicaciones de red interna que manejen información sensible. 2. Verificar que se haya implementado el uso de firmas digitales de acuerdo a la Norma de Controles Criptográficos.	Norma: Norma de controles criptográficos.	NTP-IO/IEC 17799:2004 Firmas digitales COBIT PO8.4, PO9.3, DS2.7, DS5.1, DS5.14, DS5.15, DS5.16, DS5.17, DS5.18,

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
	Frecuencia: Permanente					DS11.27, DS11.28 ITIL 4.1, 2.3, 4.2
8.3.4	La Unidad Ejecutora 403 deberá implementar servicios de no repudio. Frecuencia: Anual	• Preventivo Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma en la cual se incluya el uso de servicios de no repudio para resolver posibles disputas sobre la ocurrencia o no de un evento o acción electrónica. 2. Verificar que se hayan implementado controles de no repudio en los sistemas de información.	Normas: Norma de controles criptográficos.	NTP-IO/IEC 17799:2004 Servicios de no repudio COBIT PO8.4, PO9.3, DS2.7, DS5.1, DS5.14, DS5.15, DS5.16, DS5.17, DS5.18, DS11.27, DS11.28 ITIL 4.1, 2.3, 4.2

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.3.5	La Unidad Ejecutora 403 deberá implementar un sistema de gestión para dar soporte a las técnicas criptográficas (Claves privadas y públicas) Frecuencia: Anual	• Preventivo Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma que establezca el empleo de un sistema para la gestión para dar soporte y proteger todos los tipos de claves (privada y pública) de su modificación o destrucción. 2. Verificar que se ha implementado un sistema de gestión de criptografía de acuerdo a la Norma de controles criptográfico.	Normas: Norma de controles criptográficos.	NTP-IO/IEC 17799:2004 Gestión de claves COBIT PO8.4, PO9.3, DS2.7, DS5.1, DS5.14, DS5.15, DS5.16, DS5.17, DS5.18, DS11.27, DS11.28 ITIL 4.1, 2.3, 4.2

# OC	Objetivo de Control	Descripción
8.4	Seguridad de los archivos del sistema	OBJETIVO: Para asegurar que los proyectos de Tecnología de la Información (TI) y las actividades complementarias sean llevadas a cabo de una forma segura. El acceso a los archivos del sistema debería ser controlado. El mantenimiento de la integridad del sistema debería ser responsabilidad del grupo de desarrollo o de la función del usuario a quien pertenezcan las aplicaciones del sistema o el software.

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.4.1	La Unidad Ejecutora 403 deberá establecer controles para restringir la instalación y mantenimiento de los sistemas operativos. Frecuencia: Permanente	• Preventivo Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma en la cual se incluya las siguientes cláusulas: Las actualizaciones de las librerías de programas y las instalaciones del software de producción estén restringido al personal autorizado. Actualización de parches al software para eliminar o reducir vulnerabilidades. Registro de auditoría de todas las actualizaciones a las librerías de los programas en producción. 2. Verificar que en la política de seguridad del controlador de dominio de red se haya configurado para prevenir la instalación y/o modificación	Normas: Norma de control del software en producción.	NTP-IO/IEC 17799:2004 Control del software en producción COBIT AI2.15, AI3.3, AI3.4, AI3.5, AI3.6, DS5.4, DS5.7, DS9.6, DS9.7, DS9.8 ITIL 7.2, 5.4, 3.5, 4, 3.3, 4.2

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
				del sistema operativo.		
8.4.2	La Unidad Ejecutora 403 deberá implementar controles de acceso a los datos de pruebas. Frecuencia: Permanente	• Preventivo Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma en la que se incluya el uso de banco de prueba diferente a los datos de prueba con el cual se pueda cubrir la totalidad de escenarios de pruebas 2. Verificar que se cuenta con controles de accesos a proteger los datos de pruebas, los cuales deben ser accesados solo por el personal autorizado.	Normas: Norma de creación de datos de prueba.	NTP-IO/IEC 17799:2004 Protección de los datos de prueba del sistema COBIT AI2.15, AI3.3, AI3.4, AI3.5, AI3.6, DS5.4, DS5.7, DS9.6, DS9.7, DS9.8 ITIL 7.2, 5.4, 3.5, 4, 3.3, 4.2
8.4.3	La Unidad Ejecutora 403 deberá establecer un adecuado control en el acceso a	• Preventivo Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma en la cual se incluya cláusulas en la que se describa los controles que se requieren establecer para restringir el acceso del personal no autorizado a las fuentes de cada aplicativo. 2. Verificar que se cuenta con controles	Norma: Norma de control de acceso a las librerías de programas fuente.	NTP-IO/IEC 17799:2004 COBIT AI2.15, AI3.3, AI3.4, AI3.5, AI3.6, DS5.4,

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
	las librerías de programas fuentes. <u>Frecuencia:</u> Permanente			de acceso sobre las librerías de programas fuentes, de acuerdo a las Norma de control de acceso a las librerías de programas fuente.		DS5.7, DS9.6, DS9.7, DS9.8 <u>ITIL</u> 7.2, 5.4, 3.5, 4, 3.3, 4.2

# OC	Objetivo de Control	Descripción
8.5	Seguridad en los procesos de desarrollo y soporte	OBJETIVO: Mantener la seguridad del software de aplicación y la información. Se deberían controlar estrictamente los entornos del proyecto y de soporte. Los directivos responsables de los sistemas de aplicaciones también lo deberían ser de la seguridad del entorno del proyecto o su soporte. Se deberían asegurar de la revisión de todo cambio propuesto al sistema para comprobar que no debilite su seguridad o la del sistema operativo.

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.5.1	La Unidad Ejecutora	• Preventivo Manual	• Responsable de	1. Verificar que se cuenta con una norma de administración de cambios de	<u>Norma:</u>	<u>NTP-IO/IEC</u>

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
	403 deberá contar con estrictos controles sobre la implementación de cambios. Frecuencia: Permanente		sistemas de información.	sistema de información en los que se describe los controles requeridos para minimizar la corrupción de los sistemas de información. 2. Verificar que se cuenta con un procedimiento para el cambio en las operaciones en el que se establece una actividad de autorización del cambio por parte del responsable de sistemas. 3. Verificar la existencia de un formato en el cual se registran los cambios a los sistemas de información. 4. Verificar que los cambios a los sistemas de información son revisados por el área de calidad de software antes de realizar el pase a producción.	Norma de administración de cambios de sistemas de información. Procedimiento: Gestión para el cambio en los sistemas de información Documento Estándar: Registro de control de requerimientos	17799:2004 Procedimientos de control de cambios COBIT PO6.9, PO11.10, AI1.4, AI1.15, AI1.16, AI2.4, AI2.10, AI3.6, AI5.12, AI6.1, AI6.2, AI6.3, AI6.4, AI6.5, AI6.7, AI6.8, DS2.5, DS2.6, DS2.7, DS2.8 ITIL 5.6, 5.2, 5.2, 5.3, 3.3, 9.6, 3.5, 8.3, 8.5, 7.9, 8.2, 2.2, 9.5, 9.3, 9.3, 7.1, 7.4

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.5.2	La Unidad Ejecutora 403 deberá efectuar cambios en el sistema operativo, por ejemplo, para instalar una nueva versión o un parche de software. Frecuencia: Permanente	• Preventivo Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma que incluya la documentación de los cambios efectuados en los sistemas operativos y la autorización de los cambios por parte del responsable de sistemas.	Norma: Norma de administración de cambios de sistemas de información.	NTP-IO/IEC 17799:2004 Revisión técnica de los cambios en el sistema operativo COBIT PO6.9, PO11.10, AI1.4, AI1.15, AI1.16, AI2.4, AI2.10, AI3.6, AI5.12, AI6.1, AI6.2, AI6.3, AI6.4, AI6.5, AI6.7, AI6.8, DS2.5, DS2.6, DS2.7, DS2.8 ITIL 5.6, 5.2, 5.2, 5.3, 3.3, 9.6, 3.5, 8.3, 8.5, 7.9, 8.2, 2.2, 9.5, 9.3, 9.3, 7.1, 7.4

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.5.3	La Unidad Ejecutora 403 deberá limitar los cambios necesarios a los paquetes de software. Frecuencia: Permanente	• Preventivo Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma en la cual se incluya cláusulas en donde solo se realicen cambios autorizados por parte del responsable de sistemas de información.	Norma: Norma de administración de cambios de sistemas de información.	NTP-IO/IEC 17799:2004 Restricciones en los cambios a los paquetes de software COBIT PO6.9, PO11.10, AI1.4, AI1.15, AI1.16, AI2.4, AI2.10, AI3.6, AI5.12, AI6.1, AI6.2, AI6.3, AI6.4, AI6.5, AI6.7, AI6.8, DS2.5, DS2.6, DS2.7, DS2.8 ITIL 5.6, 5.2, 5.2, 5.3, 3.3, 9.6, 3.5, 8.3, 8.5, 7.9, 8.2, 2.2, 9.5, 9.3, 9.3, 7.1, 7.4

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.5.4	La Unidad Ejecutora 403 deberá establecer cláusulas que protejan a la institución respecto al monitoreo de canales encubiertos o código troyanos en el software adquirido o en el mantenimiento del mismo. Frecuencia: Anual	• Preventivo Manual	• Responsable de sistemas de información.	1. Verificar que la Política General de Seguridad de la Información contenga cláusulas que protejan a la institución respecto a los canales encubiertos o código troyano. 2. Verificar que se cuente con una norma que incluya cláusulas para el uso de antivirus.	Política Política General de Seguridad de Información. Norma: Norma de seguridad de los equipos informáticos.	NTP-IO/IEC 17799:2004 Canales encubiertos y código Troyano COBIT PO6.9, PO11.10, AI1.4, AI1.15, AI1.16, AI2.4, AI2.10, AI3.6, AI5.12, AI6.1, AI6.2, AI6.3, AI6.4, AI6.5, AI6.7, AI6.8, DS2.5, DS2.6, DS2.7, DS2.8 ITIL 5.6, 5.2, 5.2, 5.3, 3.3, 9.6, 3.5, 8.3, 8.5, 7.9, 8.2, 2.2, 9.5, 9.3, 9.3, 7.1, 7.4

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
8.5.5	La Unidad Ejecutora 403 deberá establecer acuerdos bajo licencia, propiedad del código y derechos de propiedad intelectual, derechos de acceso para auditar la calidad y exactitud del trabajo realizado, requisitos contractuales sobre la calidad del código, pruebas	• Preventivo • Manual	• Responsable de sistemas de información.	1. Verificar que se cuente con una norma en la cual se indique las cláusulas en las cuales se detallan la propiedad intelectual, garantías entre otros.	Norma: Norma de desarrollo externo de software.	NTP-IO/IEC 17799:2004 Desarrollo externo del software COBIT PO6.9, PO11.10, AI1.4, AI1.15, AI1.16, AI2.4, AI2.10, AI3.6, AI5.12, AI6.1, AI6.2, AI6.3, AI6.4, AI6.5, AI6.7, AI6.8, DS2.5, DS2.6, DS2.7, DS2.8 ITIL 5.6, 5.2, 5.2, 5.3, 3.3, 9.6, 3.5, 8.3, 8.5, 7.9, 8.2, 2.2, 9.5, 9.3, 9.3, 7.1, 7.4

# AC	Actividad de control	Tipo de control	Responsable de ejecutar el control	Narrativa de la actividad de control	Documentación relacionada	Estándar relacionado
	antes de la implantación para detectar el código Troyano. Frecuencia: Anual					

Cuadro 11: Adquisición, Desarrollo y Mantenimiento de Sistemas NTP ISO 17799.

4.4 COSTO DE LA APLICACION DE LA NTP ISO 17799

El costo de la aplicación de la Norma técnica Peruana ISO 17799 para la propuesta planteada en el presente trabajo es el costo de recurso humano, en el presente Cuadro se resume el costo de las tecnologías a usar. En tal sentido que el licenciamiento y costo de la mano de obra para la aplicación de NTP ISO 17799 es como se detalla a continuación.

TECNOLOGÍAS	**COSTO (S/.)**
Lic. Windows Server Standard 2008 R2 / SP1 X 64 idioma español lic. 5 CAL 1 server.	3,000.00
Lic. SQL SERVER 2008 R2 Standard	2,000.00
TOTAL TECNOLOGIAS	5,000.00
RECURSO HUMANO	1,500.00
TOTAL RR. HH.	**1,500.00**
TOTAL	**6,500.00**

Cuadro 12: Costo de aplicación de la NTP ISO 117799

Fuente: Elaboración Propia.

En este Capítulo, se plantea como propuesta para resguardar la integridad de la información de la Dirección Subregional de salud Alto Huallaga Tocache – UE 403.

CONCLUSIONES

- Se propuso la utilización de la Norma Técnica Peruana ISO 17799 en el desarrollo del Sistema de Información de Gestión Administrativa en la Dirección Subregional de Salud Alto Huallaga Tocache.

- Se desarrolló la documentación con la norma técnica peruana ISO 17799 en el Sistema de Información de Gestión Administrativa, que permitirá administrar de manera centralizada las información del Siga.

- Se implanto la documentación con la norma técnica peruana ISO 17799, para tener como una guía de buenas prácticas para la gestión de la seguridad de la información de la Dirección Subregional de Salud Alto Huallaga - Unidad Ejecutora 403 Tocache.

- Se implementó de controles para la seguridad de la información, para poder una buena gestión de la seguridad de la información de la Dirección Subregional de Salud Alto Huallaga - Unidad Ejecutora 403 Tocache.

RECOMENDACIONES

- Se recomienda que exista un buen uso y manejo de los equipos terminales que tienen acceso al servidor del Sistema de Información de Gestión Administrativa.
- Realizar los Back Up del Sistema de Información de Gestión Administrativa en línea y que tenga una frecuencia diaria en discos externos.
- Realizar el mantenimiento correctivo y preventivo de los equipos (Switch y router) de la red de datos una vez por año, para su mejor funcionamiento evitando cualquier deterioro provocado por el medio ambiente.
- Por la demanda de usuarios se recomienda hacer un mantenimiento y afinamiento de base de datos Siga.

REFERENCIAS BIBLIOGRAFÍCAS

- JAMES PETERS, JONATHAN DAVIDSON. 2001. Fundamentos de seguridad de la información. Trad. Maribel Martínez Moyano. 1ed. Madrid, Pearson educación. 344 p.

- ISO/IEC 17799 Segunda Edición, Tecnología de la Información – Técnicas de Seguridad – Código para la Práctica de la Gestión de la Seguridad de la Información. Pág. 170. Año 2005-06-15.

- ECHENIQUE GARCIA, JOSE ANTONIO. (2004). Auditoría en Informática. México, México D.F. McGraw-Hill Interamericana Editores S.A.

- CASTILLO SOTO, WILSON; ESTEBAN CHURAMPI, EFRAÍN. (2001). Normas Técnicas para Redacción y Presentación de Documentos Científicos. Perú, Tingo María, UNAS (CIUNAS), Imprenta La Florida.

- UNMSM (2003). AUDITORÍA A LA GESTIÓN DE LAS TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN [En Línea]: unmsm.edu.pe (http://sisbib.unmsm.edu.pe/bibvirtualdata/publicaciones/indata/Vol6_n1/pdf/auditoria.pdf, 10 Ago. 2011).

ANEXOS

GLOSARIO DE TERMINOS

ISO: International Organization for Standardization

IEC: International Electrotechnical Commission

SGSI: Sistema de Gestión de Seguridad de la información

BSI: British Standards Institution

COBIT: Control Objectives for Information and Related Technologies

ISACA:

ITIL: Information Technology Infrastructure Library

ANEXO 01: CODIGO SQL PARA AFINAMIENTO DE BASE DE DATOS Y EXTORNO DE ORDENES DE COMPRA Y DE SERVICIOS.

AFINAMIENTO DE BASE DE DATOS

sp_dboption 'siga', 'single user', 'true' – AFINAMIENTO DE BASE

go

DBCC checkalloc ('siga') -- REVISA EL CATALOGO DEL SISTEMA

GO

DBCC CHECKDB ('siga', repair_rebuild)

GO

DBCC CHECKDB ('siga', REPAIR_ALLOW_DATA_LOSS) -- REPARA LOS OBJETOS DE MANERA LOGICA

GO

sp_dboption 'siga', 'single user', 'false'

go

EXEC sp_MSforeachtable @command1="print '?' DBCC DBREINDEX ('?')" -- REINDEXADO LOGICO

go

sp_dboption 'siga', 'single user', 'false' --MULTIUSUARIO

EXTORNO DE ORDEN COMPRA 104

USE SIGA

UPDATE SIG_ORDEN_PRESUPUESTO **SET** SECUENCIAL = NULL, EXP_SIAF = NULL, SECU_SIAF = '', CORR_SIAF = '', FECHA_SIAF = NULL, ESTADO_EXP = ''

WHERE ANO_EJE = 2014 **and** SEC_EJEC = 1060 **and** NRO_ORDEN = 104 **and** TIPO_BIEN = 'B' **and** TIPO_PPTO = 1 **and** SEC_ORDEN = 1;

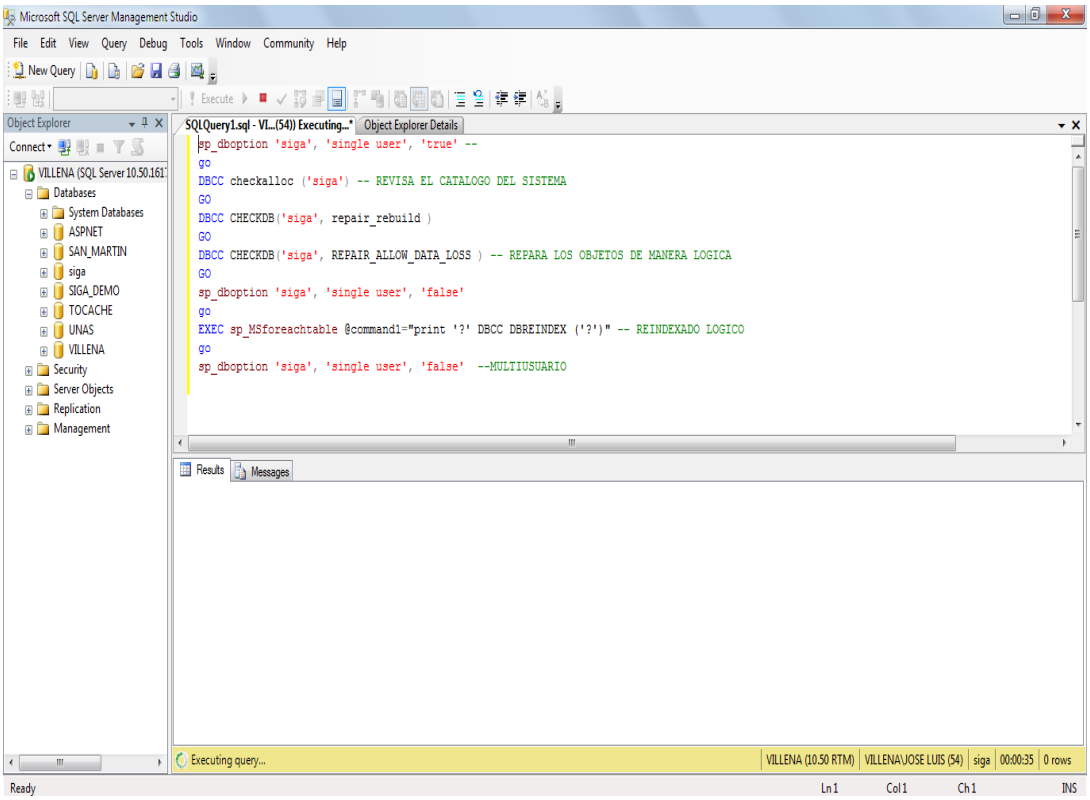
UPDATE SIG_ORDEN_SECUENCIA **SET** ESTADO_FASE = '0'

WHERE ANO_EJE = 2014 **and** SEC_EJEC = 1060 **and** NRO_ORDEN = 104 **and** TIPO_BIEN = 'B' **and** TIPO_PPTO = 1 **and** SEC_ORDEN = 1;

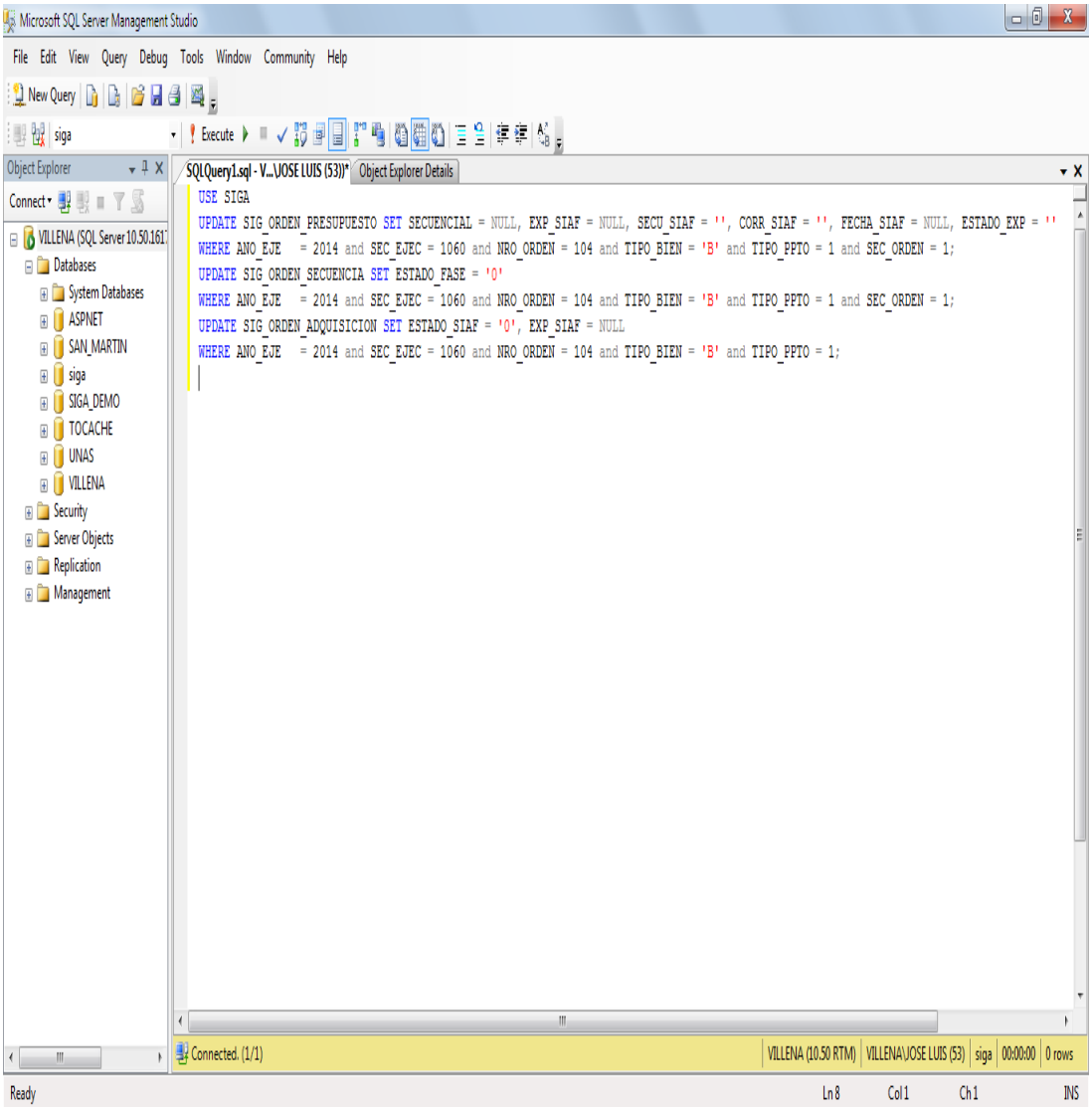
UPDATE SIG_ORDEN_ADQUISICION **SET** ESTADO_SIAF = '0', EXP_SIAF = NULL

WHERE ANO_EJE = 2014 **and** SEC_EJEC = 1060 **and** NRO_ORDEN = 104 **and** TIPO_BIEN = 'B' **and** TIPO_PPTO = 1;

MANTENIMIENTO Y AFINAMIENTO DE LA BASE DE DATOS SIGA



EXTORNO DE UNA ORDEN DE COMPRA 104 EN EL SIGA



ANEXO 02: INFORMES DE SITUACION DEL DATA CENTER Y SERVIDORES DE DATOS

DIRECCION REGIONAL DE SALUD SAN MARTIN
DIRECCION DE LA OFICINA DE OPERACIONES - SALUD
ALTO HUALLAGA TOCACHE

"Año de la Inversión para el Desarrollo Rural y la Seguridad Alimentaria"

INFORME Nº 004 -13-JLVA/O.O.S. –A.H.T.

Señor : **G.P. GEOVANNI W. CONDEZO SALVATIERRA**
DIRECTOR DE LA OFICINA DE OPERACIONES SALUD ALTO HUALLAGA – TOCACHE

De : **Bach. JOSE LUIS VILLENA ACUÑA**
INFORMATICO DE LA OFICINA DE OPERACIONES SALUD ALTO HUALLAGA – TOCACHE

REFERENCIA: ORDEN DE COMPRA N° 0261.

ASUNTO : MEJORAS TECNICAS DE EQUIPOS COMPUTACIONALES.

FECHA : 20 DE NOVIEMBRE DEL 2013

Me dirijo a Ud. a fin de informarle que se ha tomado conocimiento del documento de la referencia Orden de Compra Nº 0261, dentro de las cuales se mencionan los siguientes equipos:

- SERVIDOR DE DATOS SIGA.
- COMPUTADORA DE ESCRITORIO.
- PANTALLA.

El cuanto a la Estación de Trabajo con el Servidor la mejor opción es el **Servidor** con Procesador **Xeón E3-1220 V2** marca **HP**; mientras que la

Estación de Trabajo marca **HP** tiene un Procesador **Xeón E3-1240 V2**, Computadora de Escritorio con procesador AMD A10-5800B 3.80 GHZ con el procesador INTEL CORE i5-3470 3.20 GHZ la mejor opción es la computadora de Escritorio con **procesador INTEL CORE i5-3470 3.20 GHZ**; y con respecto al **PANTALLA** si está conforme**.**

Se recomienda adquirir el servidor con Procesador **Xeon E3-1220 V2** marca HP, Computadora de Escritorio con **procesador INTEL CORE i5-3470 3.20 GHZ.**

Es cuanto informo a Ud. para su conocimiento y fin.

Atentamente.,

Bach. JOSE LUIS VILLENA ACUÑA

"Año de la Promoción de la Industria Responsable y del Compromiso Climático"

INFORME Nº 003 -14-JLVA/O.O.S. –A.H.T.

Señor : C.P.C. Mg. AGUSTIN CORONEL ALARCÓN.
Director de la Oficina de Operaciones S.A.H.T.

De : Bach. JOSE LUIS VILLENA ACUÑA.
Informático Oficina de Operaciones S.A.H.T.

Asunto : Data Center e Internet y Propuesta de la NTP ISO 17799.

Fecha : 10 DE MARZO DEL 2014

Es grato dirigirme a Usted para saludarle muy cordialmente y a la vez informarle que los equipos de cómputo del área de Estadística e Informática se detallan a continuación:

El Data Center donde se ubican los servidores de datos tanto del SISTEMA DE INFORMACIÓN DE GESTIÓN ADMINISTRATIVA – SIGA ML y del SISTEMA INTEGRADO DE ADMINISTRACIÓN FINANCIERA – SIAF SP tiene problemas con respecto al acceso de personas no autorizadas por no contar con un ambiente adecuado y con sistema de aire acondicionado, reinicia constantemente, por tener programas de digitación como son: HIS, SEM, SIEN, NOTI-SP, REHIS y otros programas; el Equipo de cómputo en mención está sin los UPS para evitar el corte de energía eléctrica.

Además el área de estadística e informática no cuenta con red de datos e internet para él envió de información oportuna; por falta de una red estructurada de CAT 6.

Se recomienda para la adquisición de UPS para los servidores de datos y una nueva red de cableado estructurado CAT 6.

Adquirir un sistema de aire acondicionado de 24 BTU para mantener los servidores en condiciones normales sabiendo que a temperatura ambiente es elevada y los servidores están encendidos todos los días de la semana, como también adquirir antivirus con licencia corporativos que trabajen en sistemas cliente servidor.

Además le hago llegar la propuesta de la implementación de la NTP ISO 17799 en la Oficina de Operaciones Salud Alto Huallaga Tocache Unidad Ejecutora 403.

Es cuanto informo a Ud. para su conocimiento y fin.

Atentamente.,

Bach. JOSE LUIS VILLENA ACUÑA

ANEXO 03: IINFRAESTRUCTURA ACTUAL DE LA RED INTERNA