4.2.2.8.6. Sincronización del reloj.-

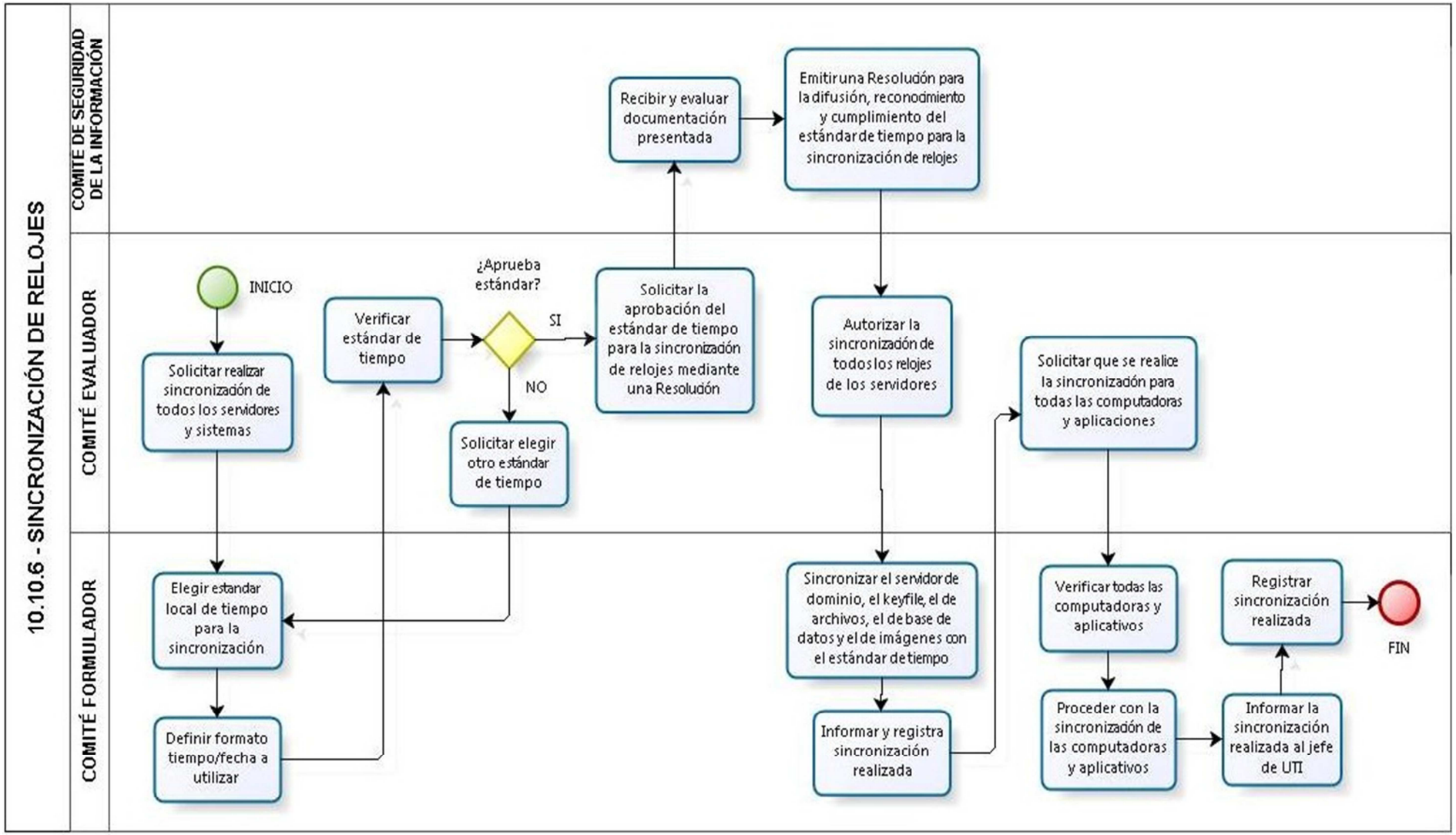
Control:
Los relojes de todos los sistemas de procesamiento de información dentro de la organización o en el dominio de seguridad deben ser sincronizados con una fuente acordada y exacta de tiempo.

Guía de Implementación:
Donde una computadora o un dispositivo de comunicación tengan la capacidad de operar con un reloj en tiempo real, este reloj debe de ser instalado con un estándar acordado, como el Tiempo Coordinado Universal o un estándar local de tiempo. Debido a que muchos relojes son conocidos por variar el tiempo, debe existir un procedimiento que verifique y corrija cualquier variación significativa.
La interpretación correcta del formato tiempo/fecha es importante para asegurar que se refleje el tiempo/fecha correcto. Las especificaciones locales deben ser tomadas en cuenta.

Diagrama de Actividades N°24 - Sincronización del reloj (10.10.6)

1. El Comité Evaluador solicita que se realice una sincronización de todos los relojes de los servidores y sistemas. Esta tarea la asigna al Comité Formulador.
2. El Comité Formulador recibe asignación y elige un estándar local de tiempo para la sincronización. Con ello define el formato tiempo/fecha a utilizar.
3. El Comité Evaluador verifica el estándar de tiempo, si es que no lo aprueba, solicita elegir otro estándar de tiempo. Si es que aprueba estándar, Solicita al Comité de Seguridad de la Información, la aprobación del estándar de tiempo para la sincronización de los relojes mediante una Resolución.
4. El Comité de Seguridad de la Información recibe y evalúa la documentación presentada, luego de ello emite una Resolución para la difusión, reconocimiento y cumplimiento del estándar de tiempo para la sincronización de relojes.
5. Una vez recibida la resolución, El Comité Evaluador, autoriza la sincronización de todos los relojes de los servidores.
6. El Comité Formulador sincroniza los relojes del servidor de dominio, del servidor de keyfile, del servidor de archivos y del servidor de base de datos con dicho estándar. Terminado ello, informa y registra la sincronización realizada.
7. El Comité Evaluador, recibe el informe de la sincronización realizada en los servidores e inmediatamente autoriza que se realice la sincronización para todas las computadoras y aplicaciones.
8. El Comité Formulador recibe asignación y verifica todas las computadoras y aplicativos existentes, luego de ello procede con la sincronización Comité Evaluador.

Diagrama de Procesos N°25 - Sincronización del reloj (10.10.6)



Formulario N°24 - Sincronización del reloj (10.10.6)

Zona Registral N° X Sede Cusco – Unidad de Tecnologías de la Información	**FORMULARIO 10.10.6 - SINCRONIZACIÓN DE RELOJES**	**Código:** [FRM - 10.10.6 - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **184** de **1**

1 DE LOS ESTÁNDARES A UTILIZAR:

Fecha: [dd/mm/aaaa]

Estándar local de tiempo: [Describir el estándar local de tiempo utilizado para realizar las sincronizaciones]

Formato Tiempo/Fecha: [Indicar el formato Tiempo/Fecha utilizado para realizar las sincronizaciones y para el registro de las mismas]

Informe presentado: [Indicar el N° de informe con el que se detalla el proceso de sincronización de relojes realizado]

DE LAS SINCRONIZACIONES:

Sincronizaciones Iniciales

Servidor Sincronizado	Encargado de la Sincronización	Fecha de Sincronización
[Indicar el servidor sincronizado] ❖ Servidor Keyfile [ ] ❖ Servidor de archivos [ ] ❖ Servidor Base de Datos [ ]	[Nombre de la persona encargada de la sincronización]	[DD/MM/AAAA HH:MM:SS]

Sincronizaciones Posteriores

Sincronizado	Encargado de la Sincronización	Fecha de Sincronización
[Indicar lo sincronizado] ❖ Aplicativos [ ] ❖ Computadoras [ ] ❖ Otros [ ]	[Nombre de la persona encargada de la sincronización]	[DD/MM/AAAA HH:MM:SS]

**** Número de Resolución de aprobación de los procedimientos para realizar la sincronización de relojes.***

2 DE LA ELABORACIÓN:

Personal del Comité Formulador

Fecha: [dd/mm/aaaa]

Nombre: [Nombre de la persona que elaboró los procedimientos para realizar la sincronización de relojes]

Cargo: [Indicar el cargo que ocupa en la institución]

_____
Firma y Sello

3 DE LA REVISIÓN:

Personal del Comité Evaluador

Fecha: [dd/mm/aaaa]

Nombre: [Nombre completo de la persona que revisó los procedimientos para realizar la sincronización de relojes]

Cargo: [Indicar el cargo que ocupa en la institución]

_____
Firma y Sello

4 DE LA APROBACIÓN:

Personal del Comité de Seguridad de la Información

Fecha: [dd/mm/aaaa]

Nombre: [Nombre de la persona que emitió la Resolución de Aprobación de los procedimientos para realizar la sincronización de relojes]

Cargo: [Indicar el cargo que ocupa en la institución]

_____
Firma y Sello

4.2.3. Formulación y Concientización.-

(Ver Anexo A.6)

Una vez que se han generado los procedimientos, diagramas y formatos para la implementación de cada control, se debe de asegurar que todo el personal de la Unidad de Tecnologías de la Información que esté involucrado en el proyecto, tome conciencia de la relevancia e importancia de las actividades de seguridad de la información y cómo estas contribuyen el logro de los objetivos del proyecto. [30]

Para ello se realizarán capacitaciones en donde se tocarán temas referidos a la seguridad de la información y a la Gestión de Comunicaciones y Operaciones. Estas capacitaciones serán constantemente evaluadas para medir el aprendizaje y conocimiento del personal.

El Plan de Capacitación y Concientización para la Gestión de Comunicaciones y Operaciones del presente proyecto está plasmado en el documento de **Versión 1.1 del Anexo A.6.**

[30] Esquema de Norma Técnica Peruana ENTP ISO/IEC 27001:2006 - 'Capacitación, concientización y competencia'

4.2.4. Operar el Plan de Actividades.-

(Ver Anexo A.7)

El siguiente paso a realizar, una vez que el personal se ha capacitado y ha entendido la importancia de la seguridad de la información en la gestión de comunicaciones y operaciones, es el de proceder con la implementación del plan de actividades sugerido para el presente proyecto.

Dicha implementación considera los controles seleccionados en el Documento de la Declaración de la Aplicabilidad (SOA), con sus respectivos procedimientos descritos en los diagramas de actividad, diagramas de procesos y formularios para registrar el uso de los controles.

Se establece un cronograma con el tiempo de duración de la implementación, indicando qué personal está implicado en el proceso, y además de ello, se define como medir la efectividad de los controles o grupos de control seleccionados.

El Plan de implementación de los controles para la Gestión de Comunicaciones y Operaciones del presente proyecto está plasmado en el documento de **Versión 1.1 del Anexo A.7.**

4.3 Control.-

4.3.1. Realizar auditorías internas de lo implementado.-

(Ver Anexo A.8)

Una vez culminada la etapa de Desarrollo del Ciclo de Deming, empieza la etapa del Control, en el que se realizarán los procedimientos necesarios para proceder con la auditoría interna de los controles implementados en la Unidad de Tecnología de la Información (UTI) de la SUNARP, verificando que éstos cumplan los requisitos señalados y sugeridos en la **NTP - ISO/IEC 17799:2007**.

Las auditorías internas se realizan generalmente una vez al año y son planificadas por un personal capacitado para realizarlas. Durante esta revisión se analiza, en base a las evidencias de las auditorías

Éste proceso comprende realizar un Programa Anual de Auditoría, Planes de Auditorías Internas para cada control y los Informes de Auditorías correspondientes una vez finalizado cada evaluación.

Además de ello, se explicará la manera de evaluar a las personas asignadas para realizar las auditorías tomando en cuenta criterios y perfiles propuestos con los que un auditor interno debe de contar.

Todo ello se detalla a continuación y con mayor detalle a seguir en el documento de **Versión 1.1 del Anexo A.8.**

4.3.1.1. Programa de Auditoría Anual.-

Un programa de Auditoría Anual recoge cada uno de los procesos que han de ser auditados anualmente, el/los auditor/es responsable/s y el rango de tiempo dentro del cual ha de ejecutarse cada auditoría. Elaborado para un periodo determinado.

El Formato del Programa de Auditoría Anual que se sugiere utilizar está plasmado en el inciso 3.1 del documento de **Versión 1.1 del Anexo A.8.**

A continuación se detalla el Programa de Auditoría Anual para el presente proyecto, tomando como base el formato mencionado líneas arriba.

Zona Registral N° X Sede Cusco – Unidad de Tecnologías de la Información	**PROGRAMA ANUAL DE AUDITORÍA**	**Código:** [FRM - AUD - 001] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** 189 de 2

Norma de Referencia:	NTP - ISO/IEC 17799:2007
Objetivo:	Planificar la auditoría anual para evaluar los controles implementados de la Gestión de Comunicaciones y Operaciones en la Unidad de Tecnologías de la Información de la Zona Registral N°X – Sede Cusco – SUNARP siguiendo las normal sugeridas en la NTP-ISO/IEC 17799:2007.
Alcance:	Controles elegidos a implementar en el documento de la Declaración de la Aplicabilidad
Programa para el período:	Agosto de 2015 a Julio de 2016

N	**Auditoría**	**Programación ***																							
	Control a auditar	**Agosto**				**Setiembre**				**Octubre**				**Noviembre**				**Diciembre**				**Enero**			
		1	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
1	10.8.3 – Medios físicos en tránsito	X	X																						
2	10.10.1 – Registro de la auditoría				X	X																			
3	10.10.2 – Monitoreando el uso del sistema							X	X																
4	10.1.3 – Segregación de tareas										X	X													
5	10.10.4 – Registro de administradores y operadores													X	X										
6	10.1.1 – Documentación de procesos operativos																X	X							
7	10.5.1 – Recuperación de la información																			X	X				
8	10.10.3 - Protección de la información de registro																						X	X	
	Nº de Auditorías:	**2**				**1**				**1**				**2**				**1**				**1**			

N	Auditoría	Programación *																							
	Control a auditar	Febrero				Marzo				Abril				Mayo				Junio				Julio			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
9	10.7.3 – Procedimientos de manipulación de la información	X	X																						
10	10.7.4 – Seguridad de la documentación de sistemas				X	X																			
11	10.10.6 – Sincronización del Reloj							X	X																
12	10.1.2 – Gestión de Cambios										X	X													
13	10.1.4 – Separación de los recursos para desarrollo y producción													X	X										
14	10.3.1 – Planificación de la capacidad																X	X							
15	10.3.2 – Aceptación del Sistema																			X	X				
16	10.4.1 – Medidas y controles contra software malicioso																						X	X	
Nº de Auditorías:		**2**				**1**				**1**				**2**				**1**				**1**			

TOTAL DE AUDITORÍAS DEL PROGRAMA ANUAL: Agosto de 2015 a Agosto de 2016	**16**

Programa para el período:	Agosto 2016 a Agosto de 2017

N	Auditoría	Programación *																							
	Control a auditar	Agosto				Setiembre				Octubre				Noviembre				Diciembre				Enero			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
17	10.4.2 – Medidas y controles contra código móvil	X	X																						
18	10.6.1 - Controles de red				X	X																			
19	10.6.2 – Seguridad en los servicios de redes							X	X																
20	10.7.1 – Gestión de medios removibles										X	X													
21	10.7.2 – Eliminación de medios													X	X										
22	10.8.1 – Políticas y procedimientos para el intercambio de información y software																X	X							
23	10.8.5 – Sistemas de información de negocios																			X	X				
24	10.10.5 – Registro de la avería																						X	X	
Nº de Auditorías:		**2**				**1**				**1**				**2**				**1**				**1**			

TOTAL DE AUDITORÍAS DEL PROGRAMA ANUAL: Agosto de 2016 a Enero de 2017	**8**

* Consignar con una “X” en el número de semana del mes en que se realizará la auditoría.

Tabla N°7 - *Programa anual de auditoría de los controles implementados en la UTI*

Fuente: *Elaboración Propia*

4.3.1.2. Plan de Auditoría Interna.-

En un Plan de Auditoría Interna se coordina la(s) fecha(s) y hora(s) de ejecución para cada auditoría, a fin de asegurar la disponibilidad de los participantes durante la auditoría interna.

Se seleccionan a los auditores internos que conformarán el Equipo Auditor, de acuerdo al perfil de Puesto de Auditor Interno y haciendo uso del Formato de "Evaluación del Auditor Interno" (Véase el inciso 5 del Anexo A.8), así como, de ser necesario, selecciona a la(s) persona(s) que participará(n) como experto(s), técnico(s) y observador(es).

El Formato del Plan de Auditoría que se sugiere utilizar está plasmado en el inciso 3.1 del documento de **Versión 1.1 del Anexo A.8.**

4.3.1.3. Informes de Auditoría Interna.-

Una vez ejecutada la auditoría, el auditor elabora el Informe de Auditoría Interna, en donde registra las deficiencias encontradas.
Este informe será consensuado con el responsable del área auditada y sus colaboradores de manera que se produzca un reconocimiento colectivo de la situación y una aceptación de la necesidad de aplicar las medidas correctivas que sean precisas.

Cada Informe de Auditoría se utilizará para el estudio de acciones correctivas posibles, que se presentarán posteriormente para su aprobación durante el ciclo de "Actuar" del Ciclo de Deming.

El Formato del Informe de Auditoría Interna que se sugiere utilizar está plasmado en el inciso 3.3 del documento **de Versión 1.1 del Anexo A.8.**

4.3.2. Registrar acciones y eventos.-

Una vez realizado los respectivos informes de auditorías internas, serán encontradas las No Conformidades o Incidencias y Hallazgos, que deberán ser estudiadas para establecer acciones necesarias y solventar dichas no conformidades.

Las No Conformidades que son detectadas con mayor frecuencia pueden ser el incumplimiento de plazos de las auditorías programadas, la falta de informes o evidencias que respalden el cumplimiento de lo establecido en la implementación de cada control, o el incumplimiento de algún requisito de la norma.

Estas incidencias, hallazgos y no conformidades encontradas, se redactan y registran en el formato sugerido a utilizar del inciso 4 del documento de **Versión 1.1 del Anexo A.8.**

4.4 Acción.-

Con base en las conclusiones de la etapa anterior, lo siguiente que se sugiere realizar es elegir una de las siguientes acciones, dependiendo del caso que amerite:

- Si se han detectado errores parciales en la etapa de Control, realizar un nuevo ciclo PDCA con nuevas mejoras.
- Si no se han detectado errores relevantes, aplicar a gran escala las modificaciones de los procesos.
- Si se han detectado errores insalvables, abandonar las modificaciones de los procesos.

Una vez identificado el caso, se debe documentar el proceso y ofrecer una retroalimentación para la mejora en la fase de planificación.
Esta etapa cierra el Ciclo de Deming con la realimentación para acercar los resultados obtenidos a los objetivos.

Según lo establecido en el documento del alcance (Anexo A.2), esta etapa no se llegará a realizar en la implementación de los controles del presente proyecto.

GLOSARIO

- **Aceptación del riesgo:** Decisión de aceptar el riesgo.
- **Activo:** Algo que presenta valor para la organización.
- **Análisis del riesgo:** Uso sistemático de información para identificar amenazas y estimar el riesgo.
- **Antivirus:** Programa cuyo objetivo es detectar o eliminar virus informático.
- **Autenticidad:** Característica que se refiere a la comprobación y confirmación de la identidad real de los activos (procesos, sistemas, información) y/o actores (usuarios) y/o de la autorización por parte de los autorizadores, así como la verificación de estas tres cuestiones.
- **Bach:** Bachiller.
- **Backup:** Respaldo de Información.
- **Banda ancha:** Acceso de alta velocidad a Internet.
- **Business Continuity:** Continuidad del Negocio.
- **CD:** Disco Compacto.
- **Código móvil:** software de transferencia entre sistemas, transferidas a través de una red ejecutado en un sistema local sin necesidad de instalación o ejecución explícita por parte del beneficiario.
- **Confidencialidad:** garantizar que la información sea accesible únicamente para quienes tengan acceso autorizado.
- **Data Center:** Centro de Datos
- **Declaración de aplicabilidad:** Documento que describe los objetivos y los controles que son pertinentes y aplicables al SGSI de la organización.
- **Diagrama BPM:** Diagramas de Modelo y Notación de Procesos de Negocio, que permite el modelado de procesos de negocio, en un formato de flujo de trabajo.
- **Disaster Recovery:** Recuperación ante desastres.

- **Disponibilidad:** Garantizar que los usuarios autorizados tengan acceso a la información y activos asociados cuando sea necesario.
- **EDI:** Intercambio Electrónico de Datos.
- **Estimación del riesgo:** Proceso total de análisis y valoración del riesgo.
- **Evaluación del riesgo:** Proceso de comparación del riesgo estimado frente al criterio de riesgo para determinar el significado del riesgo.
- **Evento de la seguridad de la información:** Ocurrencia identificada en un sistema, servicio o red indicando una posible brecha de la política de información o falla de las salvaguardas o una situación desconocida previa que puede ser relevante.
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar el riesgo en una organización.
- **Hardware:** Parte física de un sistema informático.
- **Hosting:** Es un servicio que provee a los usuarios un Sistema para poder almacenar información.
- **Housing:** Modalidad de alojamiento web destinado principalmente a grandes empresas y a empresas de servicios web.
- **IEC:** Comisión Electrotécnica Internacional.
- **Incidente de la seguridad de la información:** Serie de eventos inesperados que tienen una probabilidad significativa de comprometer operaciones del negocio y amenazar la seguridad de la información.
- **ING:** Ingeniero.
- **Integridad:** Salvaguardar la exactitud e integridad de la información y métodos de procesamiento.
- **ISO:** Organización Internacional de Normalización.
- **Keyfile:** Servidor de Imágenes de partidas electrónicas.
- **Malware:** Software malicioso que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

- **MOF:** Manual de Organización y Funciones.
- **NTP:** Norma Técnica Peruana.
- **ONGEI:** Oficina Nacional de Gobierno Electrónico e Informático.
- **PCM:** Presidencia del Consejo de Ministros.
- **PDCA:** Planificación, Desarrollo, Control y Acción (Ciclo de Deming).
- **Riesgo residual:** Riesgo remanente después de un tratamiento del riesgo.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **SN:** Superintendencia Nacional.
- **Tratamiento del riesgo:** Proceso de selección e implementación de medidas para minimizar el riesgo.
- **Trazabilidad:** Capacidad de registro de las operaciones de un sistema informático, de manera que cualquier operación pueda ser rastreada hasta su origen.
- **UTI:** Unidad de Tecnologías de la Información.
- **Virus:** Malware que tiene por objetivo alterar el normal funcionamiento del ordenador, sin el permiso o el conocimiento del usuario.
- **Vulnerabilidades:** capacidad, condiciones y características del sistema mismo, que lo hace susceptible a amenazas, con el resultado de sufrir algún daño.

CONCLUSIONES

1. Se logró identificar y desarrollar diagramas de actividades que respondan a lo sugerido en la cláusula de Gestión de Operaciones y Comunicaciones de la NTP-ISO/IEC 17799:2007 para los procesos desarrollados en la UTI y que permitan identificar los roles del recurso humano que participará en la misma.

2. Se realizaron diagramas de procesos para cada actividad sugerida a realizar en la guía de implementación de la cláusula de Gestión de Operaciones y Comunicaciones de la NTP ISO/IEC 17799:2007.

3. Los formularios correspondientes a los controles de la Cláusula de Gestión de Operaciones y Comunicaciones de la NTP ISO/IEC 17799:2007 han sido elaborados para ser usados durante la implementación de los mismos, cumpliendo así lo establecido en la norma.

4. Se elaboraron formatos dentro del plan de auditoría que evalúan los correspondientes controles implementados y se cercioran que hayan sido desarrollados según la cláusula de Gestión de Operaciones y Comunicaciones de la NTP ISO/IEC 17799:2007.

5. Con el plan de actividades propuesto bajo la cláusula de Gestión de Comunicaciones y Operaciones de la NTP-ISO/IEC 17799:2007 se logra contribuir al buen uso y a la buena práctica de tener procedimientos que estén ejecutados bajo normas y políticas a cumplir siempre.

6. Toda empresa necesita un área implementada de Seguridad de la Información, para que de ésta manera se pueda implementar los correspondientes controles determinados por su negocio, y plasmarlos en un Sistema de Gestión de Seguridad de la Información

7. La presente investigación ayuda al mejor manejo de los procesos de Tecnologías de la Información de la Zona Registral N°X Sede Cusco, procesos que estén relacionados en la Gestión de la Seguridad de la Información, brindando protección y manteniendo la confidencialidad, integridad y disponibilidad de su información. Generando así una mayor credibilidad y confiabilidad a toda la institución.

8. Con el presente proyecto pudimos ampliar nuestros conocimientos en Seguridad de la Información y las Normas Técnicas Peruanas, además de ello, llegamos a la conclusión de que no existen muchos profesionales especializados en el tema, y la bibliografía referida a la misma es mínima.

RECOMENDACIONES

1. Una vez acabadas las 3 etapas iniciales del Ciclo de Deming, se recomienda continuar con la última etapa: “Acción”, en la cual se ejecutarán las mejoras continuas, acciones preventivas y acciones correctivas que han sido elaboradas para cada control implementado.

2. Una vez completado el ciclo de Deming, es recomendable contratar auditores certificados, que sean terceros y externos a la organización para que realicen las respectivas auditorías externas evaluando el SGSI y todos los controles implementados.

3. Con la implementación adecuada de los controles sugeridos en la NTP-ISO/IEC 17799:2007, se recomienda continuar con los procesos necesarios para conseguir la Certificación ISO 27001.

4. Se recomienda hacer uso de un software y/o aplicación especial que facilite el manejo de la documentación y de la información contenida en cada control implementado, para que de esa manera se lleve un mejor seguimiento de lo avanzado con los formatos y actividades sugeridos en el presente proyecto.

5. Para próximos proyectos, se recomienda tomar de base la presente documentación y continuar con la implementación de los controles siguiendo lo recomendado en la NTP-ISO/IEC 17799:2014, aprobada en noviembre del 2014.

6. Todas las organizaciones dispongan y asignen un presupuesto para generar y/o implementar un Área de Seguridad de la Información, con personal capacitado en la implementación de Sistemas de Gestión de Seguridad de la Información y que cuenten con conocimiento en Gestión de Riesgos y Auditoría.

7. Para otras entidades se debe de conformar los Comités del SGSI, Formulador, Evaluador, de Seguridad de la información, ya que este proyecto podrá servir de modelo a seguir en la implementación de un SGSI para cualquier organización.

8. Para futuros proyectos, se puede tomar de modelo la presente investigación utilizando los estándares recomendados en el PMBOK®

REFERENCIAS

Aceituno Canal, V. (2006). *Seguridad de la Información.* México: Limusa - Noriega Editores.

Daltabuid Godas, E., & Hernandez Audelo, L. (2007). *La Seguridad de la Información* (Primera ed.). México: Limusa - Noriega Editores.

El portal de ISO 27001 es español. (s.f.). Obtenido de http://www.iso27000.es

Formación sobre SGSI. (s.f.). Obtenido de http://www.slideshare.net/RamiroCid/formacin-bsica-en-sgsi-seguridad-it

Gómez Vieites, A. (2007). *Enciclopedia de la Seguridad de la Información* (Primera ed.). Madrid, España: Afaomega.

INCOTEC. (2010). *Compendio Sistema de Gestión de la Seguridad de la Información (SGSI)* (Segunda ed.). Bogotá, Colombia.

Morales, F. (s.f.). *Pensamiento Imaginactivo*. Obtenido de Conozca 3 tipos de investigación: Descriptiva, Exploratoria y Explicativa: http://manuelgross.bligoo.com/conozca-3-tipos-de-investigacion-descriptiva-exploratoria-y-explicativa

Noemágico. (s.f.). Obtenido de La Investigación Descriptiva: http://noemagico.blogia.com/2006/091301-la-investigacion-descriptiva.php

Norma Técnica Peruana NTP ISO/IEC 17799:2007. (s.f.). Perú.

Norma Técnica Peruana NTP ISO/IEC 27001:2007. (s.f.). Perú.

Scribd. (s.f.). Obtenido de Gestión de las Comunicaciones y Operaciones: http://es.scribd.com/doc/13498973/Gestion-de-Las-Comunicaciones-y-Operaciones

SUNARP. (s.f.). *Manual de Organizaciones y Funciones de la Unidad de Tecnologías de la Información de la Zona Registral N°X - Sede Cusco.* Cusco, Perú.

SUNARP. (s.f.). *Página web de la Superintendencia Nacional de los Registros Públicos*. Obtenido de http://www.sunarp.gob.pe

Universidad Nacional Abierta y a Distancia. (s.f.). *Sistema de Gestión de Seguridad de la Información*. Obtenido de http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/index.html

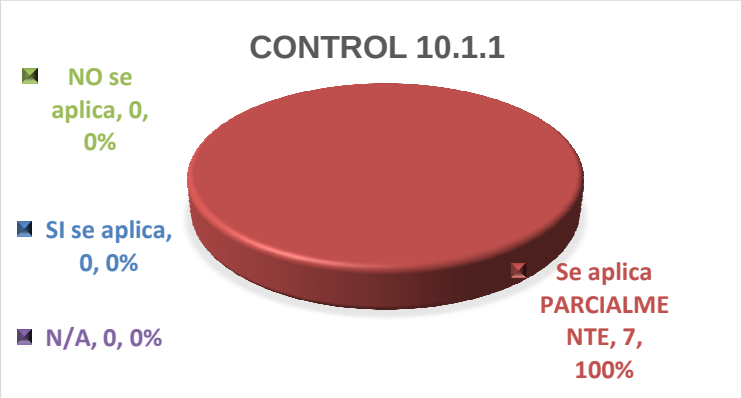
Wikipedia. (s.f.). *Wikipedia, la enciclopedia libre*. Obtenido de ISO/IEC 27002: http://es.wikipedia.org/wiki/ISO/IEC_27002

ANEXOS

Encuesta sobre la situación actual

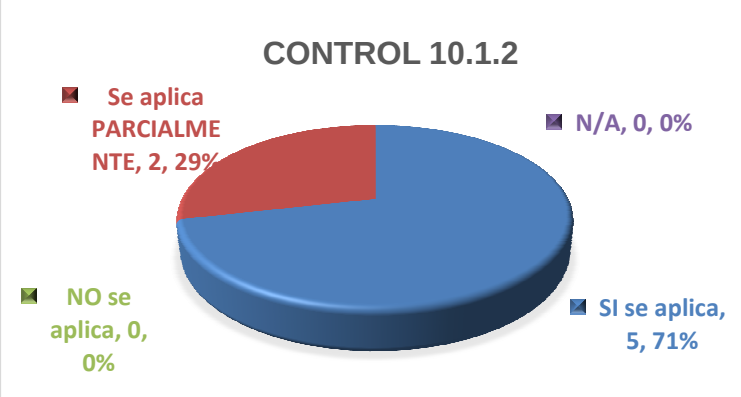
Encuesta realizada al personal de la Unidad de Tecnologías de la Información de la Zona Registral N° X – Sede Cusco – SUNARP, para conocer la situación actual de la información, relacionada con los controles propuestos de la cláusula Gestión de Comunicaciones y Operaciones de la NTP ISO/IEC 17799:2007:
El total de trabajadores que respondieron a la encuesta es de 7 personas.

Gestión de Comunicaciones y Operaciones	
10.1. Responsabilidad y Procedimientos Operacionales	
Control	**Pregunta**
10.1.1. Procedimientos operacionales documentados	¿Los procedimientos están documentados, mantenidos y puestos a disposición de todos los usuarios que los necesitan?



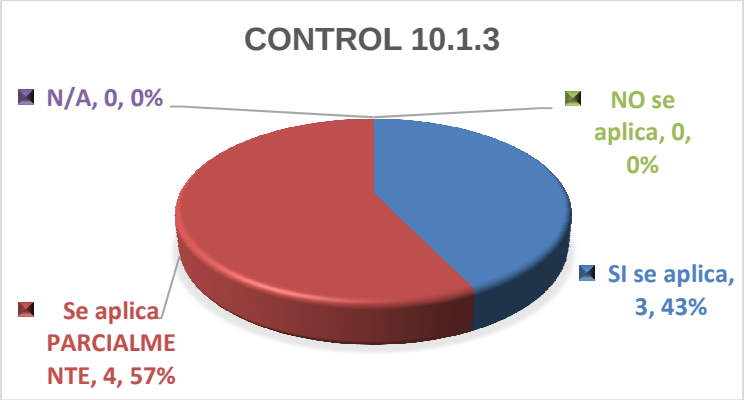
- El 100% de los Trabajadores de la UTI indicaron que el control 10.1.1 se aplica de manera Parcial en un 58%.

Control	Pregunta
10.1.2. Administración de cambios	¿Se controlan los cambios a la infraestructura para el tratamiento de la información y los sistemas?



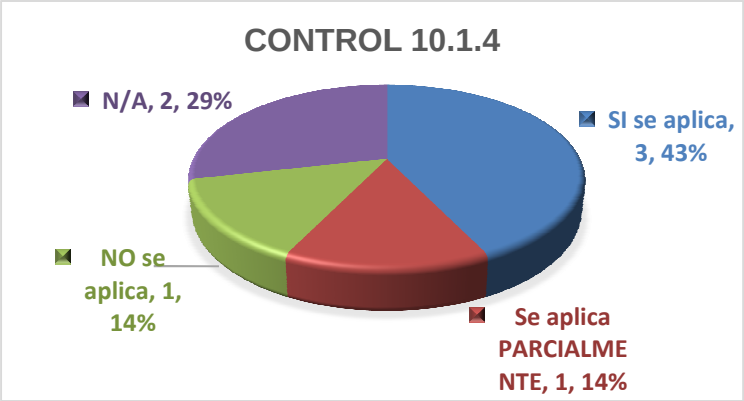
- El 71% de los Trabajadores de la UTI indicaron que el control 10.1.2 SI se aplica en un 82%.
- El 29% indicó que el control se aplica de manera PARCIAL en un 50%.

Control	Pregunta
10.1.3. Segregación de funciones	¿Los deberes y áreas de responsabilidad están segregados para reducir las oportunidades de modificación o uso indebido, no autorizado o no intencional, de los activos de la organización?



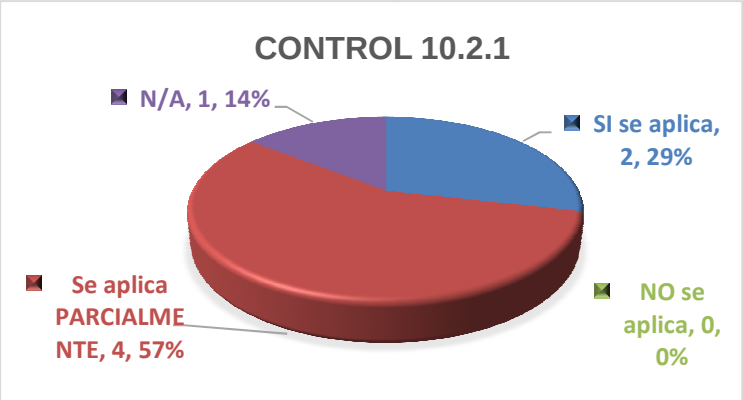
- El 43% de los trabajadores indicó que el control 10.1.3 SI se aplica en un 80%.
- El 57% indicó que el control 10.1.3 se aplica de manera parcial en un 55%.

Control	Pregunta
10.1.4. Separación de ambientes	¿Las instalaciones de desarrollo, producción y pruebas están separadas para reducir los riesgos de accesos o cambios en los sistemas operativos no autorizados?



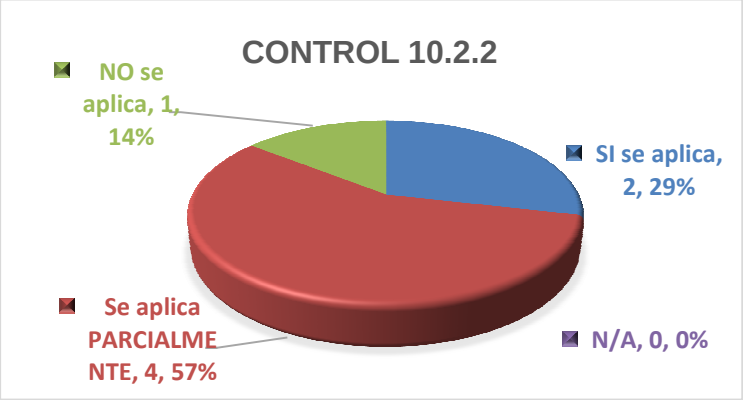
- El 43% de los Trabajadores de la UTI indicaron que el control 10.1.4 SI se aplica en un 83.3%.
- El 14% indicó que el control se aplica de manera PARCIAL en un 60%.
- El 14% indicó que el control no se aplica (20%).
- El 29% indicó que el control no debe aplicarse.

10.2. Gestión de servicios por terceras partes	
Control	**Pregunta**
10.2.1. Entrega de Servicios	¿La organización se asegura que los controles de seguridad, las definiciones de servicio y la distribución de niveles incluida en el acuerdo de prestación de servicios con terceras partes están implantados, operados y mantenidos por las terceras partes?



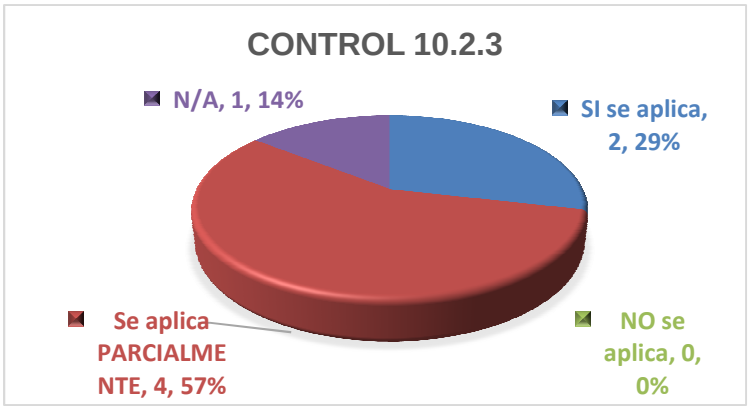
- El 29% de los Trabajadores de la UTI indicaron que el control 10.2.1 SI se aplica en un 85%.
- El 57% indicó que el control se aplica de manera PARCIAL en un 64%.
- El 14% indicó que el control no debe aplicarse.

Control	Pregunta
10.2.2. Monitoreo y revisión de los servicios de terceros	¿Los servicios, informes y registros proporcionados por terceras partes, se monitorizan y revisan de forma regular, y se llevan a cabo auditorías de forma regular?



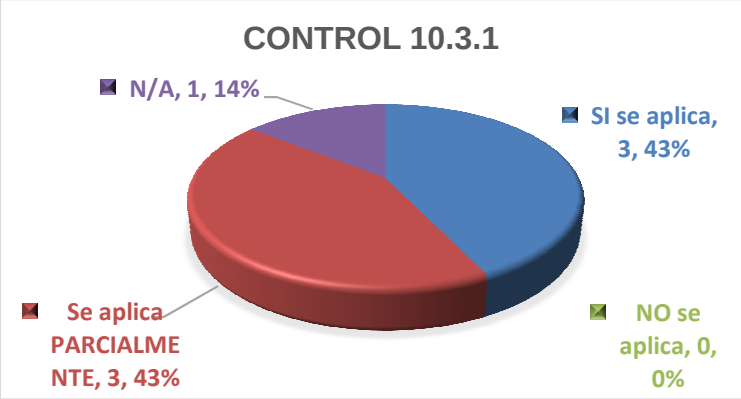
- El 29% de los Trabajadores de la UTI indicaron que el control 10.2.2 SI se aplica en un 80%.
- El 57% indicó que el control se aplica de manera PARCIAL en un 55%.
- El 14% indicó que el control NO se aplica (20%).

Control	Pregunta
10.2.3. Administración de cambios en los servicios de terceros	¿Se gestionan los cambios de provisión de los servicios (incluyendo el mantenimiento y mejora de las políticas existentes, procedimientos y controles de seguridad de la información) tomando en cuenta la criticidad de los sistemas y procesos del negocio implicados y la reevaluación del riesgo?



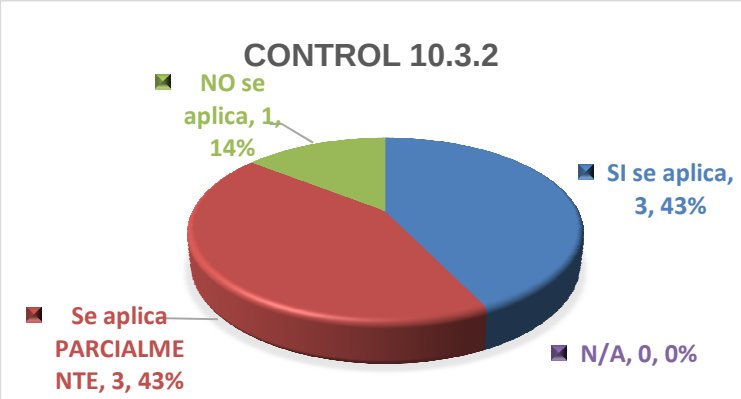
- El 29% de los Trabajadores de la UTI indicaron que el control 10.2.3 SI se aplica en un 80%.
- El 57% indicó que el control se aplica de manera PARCIAL en un 50%.
- El 14% indicó que el control no debe de aplicarse.

10.3. Planificación y aceptación del sistema	
Control	**Pregunta**
10.3.1 Gestión de la capacidad	¿El uso de recursos es monitoreado, afinado y se realizan proyecciones de futuros requisitos de capacidad para asegurar el rendimiento del sistema?



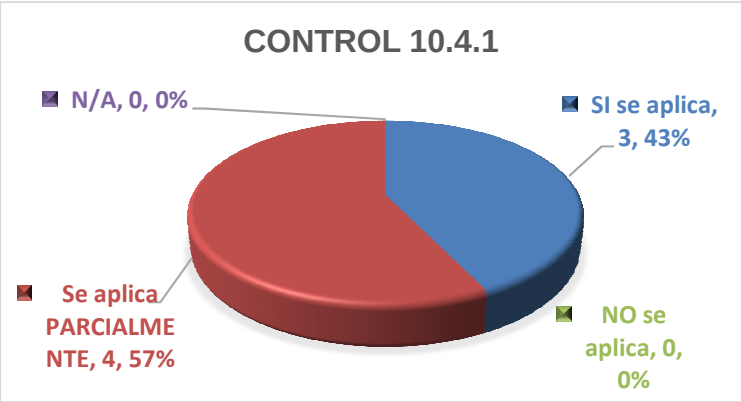
- El 43% de los Trabajadores de la UTI indicaron que el control 10.3.1 SI se aplica en un 80%.
- El 43% indicó que el control se aplica de manera PARCIAL en un 53.3%.
- El 14% indicó que el control no debe de aplicarse.

Control	Pregunta
10.3.2 Aceptación de sistemas	¿Hay criterios de aceptación establecidos para nuevos sistemas de información, actualizaciones y nuevas versiones y se realizan pruebas del sistema durante el desarrollo y previamente a la aceptación?



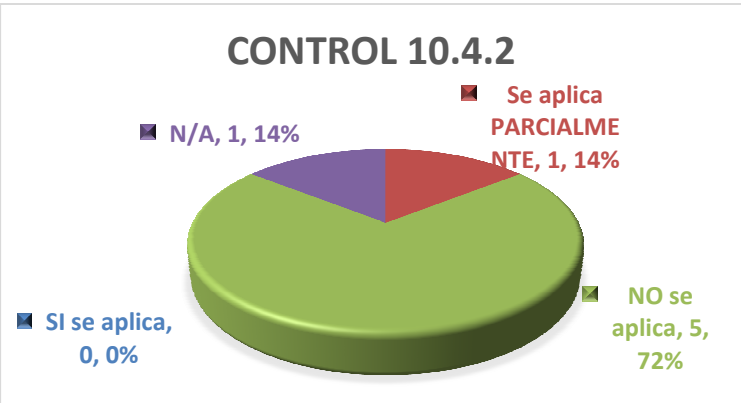
- El 43% de los Trabajadores de la UTI indicaron que el control 10.3.2 SI se aplica en un 80%.
- El 43% indicó que el control se aplica de manera PARCIAL en un 50%.
- El 14% indicó que el control NO se aplica (30%)

10.4 Protección contra código móvil y malicioso	
Control	**Pregunta**
10.4.1 Controles contra software malicioso	¿Se han implementado controles de detección, prevención y recuperación para protegerse de código malicioso, así como procedimientos apropiados para la concientización de los usuarios sobre éste?



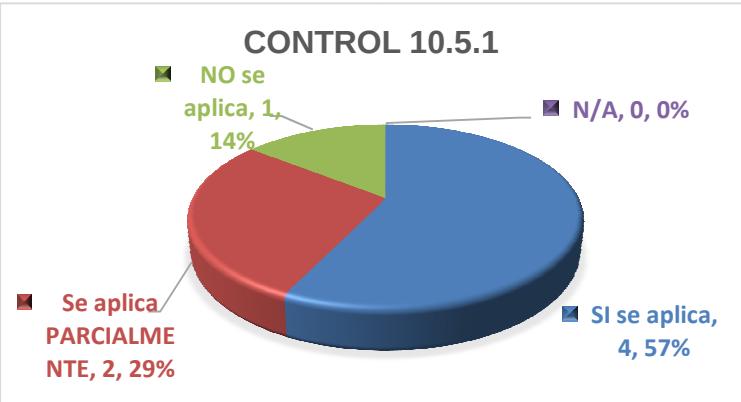
- El 43% de los Trabajadores de la UTI indicaron que el control 10.4.1 SI se aplica en un 80%.
- El 57% indicó que el control se aplica de manera PARCIAL en un 62.5%.

Control	Pregunta
10.4.2 Controles contra código móvil	¿Cuándo el uso del código móvil está autorizado, la configuración asegura que éste código opera de acuerdo a una política de seguridad claramente definida y se impide su uso si es un código móvil no autorizado?



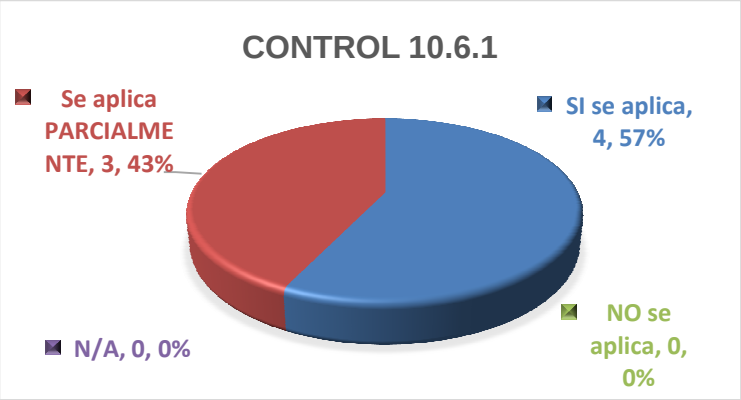
- El 14% de los Trabajadores de la UTI indicaron que el control 10.4.2 se aplica de manera PARCIAL en un 50%.
- El 72% indicó que el control NO se aplica (24%).
- El 14% indicó que el control no debe de aplicarse

10.5. Copia de respaldo de información	
Control	**Pregunta**
10.5.1 Copia de respaldo de información	¿Se realizan las copias de seguridad y se comprueban regularmente conforme a lo establecido en la política acordada?



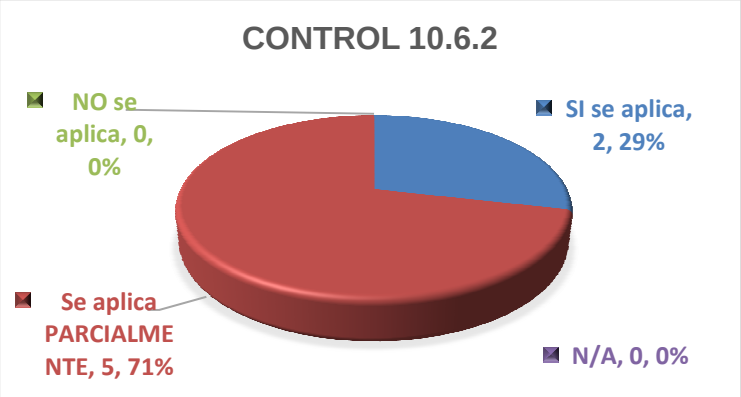
- El 57% de los Trabajadores de la UTI indicaron que el control 10.5.1 SI se aplica en un 85%.
- El 29% indicó que el control se aplica de manera PARCIAL en un 50%.
- El 14% indicó que el control NO se aplica (20%).

10.6. Gestión de seguridad en la red	
Control	**Pregunta**
10.6.1 Controles de red	¿La red está adecuadamente administrada y controlada, con el fin de protegerla de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usa la red, incluida la información en tránsito?



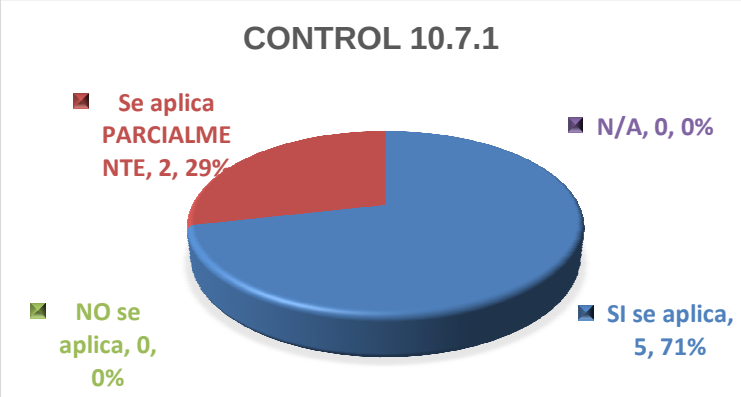
- El 57% de los Trabajadores de la UTI indicaron que el control 10.6.1 SI se aplica en un 85%.
- El 43% indicó que el control se aplica de manera PARCIAL en un 53.3%.

Control	Pregunta
10.6.2 Seguridad de servicios de red	¿Las características de seguridad, los niveles de servicio, y los requerimientos de administración de todos los servicios de red, están identificados e incluidos en los acuerdos con los diferentes proveedores de servicios de red, bien sean internos o externos?



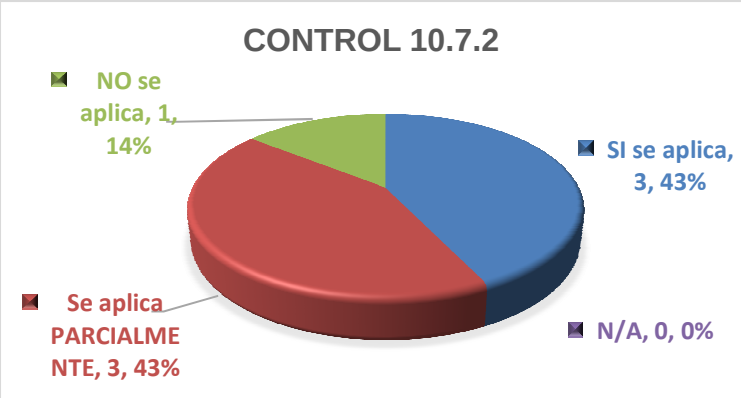
- El 29% de los Trabajadores de la UTI indicaron que el control 10.6.2 SI se aplica en un 87.5%.
- El 71% indicó que el control se aplica de manera PARCIAL en un 52%.

10.7. Gestión de soportes	
Control	**Pregunta**
10.7.1 Gestión de los medios removibles	¿Existen procedimientos para la administración de los medios removibles?



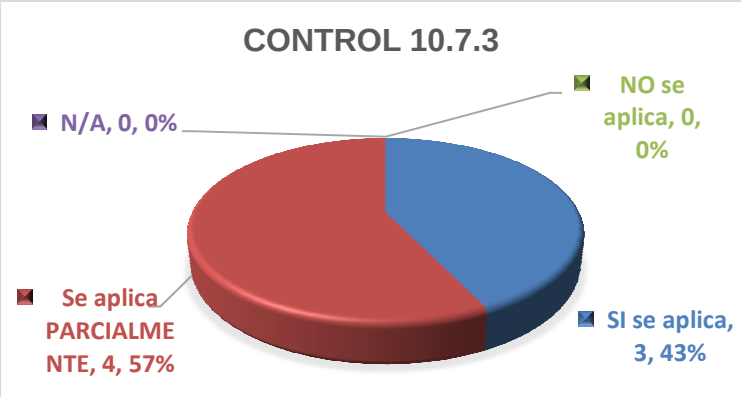
- El 71% de los Trabajadores de la UTI indicaron que el control 10.7.1 SI se aplica en un 83%.
- El 29% indicó que el control se aplica de manera PARCIAL en un 50%.

Control	Pregunta
10.7.2 Eliminación de medios	¿Los soportes que no se vayan a utilizar más, son eliminados de forma segura y sin inconvenientes por medio de procedimientos formales?



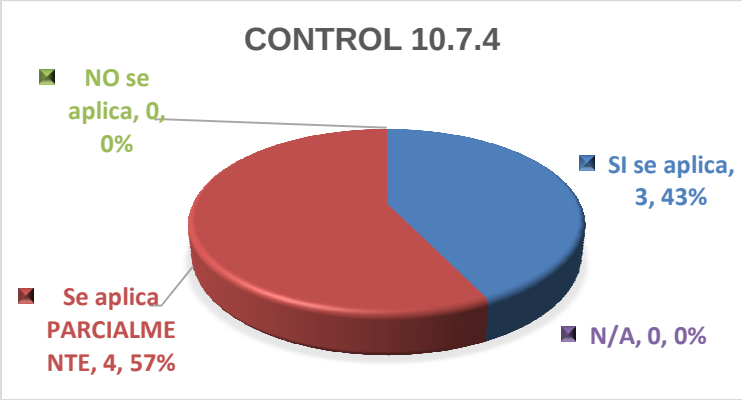
- El 43% de los Trabajadores de la UTI indicaron que el control 10.7.2 SI se aplica en un 86.6%.
- El 43% indicó que el control se aplica de manera PARCIAL en un 53.3%.
- El 14% indicó que el control NO se aplica (20%).

Control	Pregunta
10.7.3 Procedimientos para el manejo de información	¿Hay procedimientos establecidos para el manejo y el almacenamiento de la información de forma que se proteja de la divulgación no autorizada o del uso inapropiado?



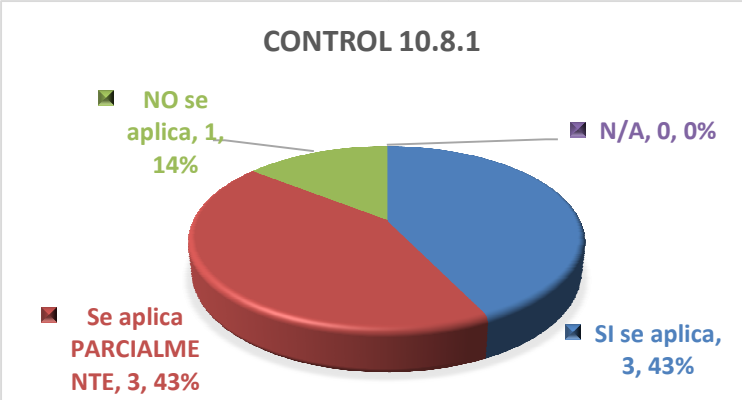
- El 43% de los Trabajadores de la UTI indicaron que el control 10.7.3 SI se aplica en un 85%.
- El 57% indicó que el control se aplica de manera PARCIAL en un 57.5%.

Control	Pregunta
10.7.4 Seguridad de la documentación de los sistemas	¿Se encuentra protegida la documentación del sistema contra accesos no autorizados?



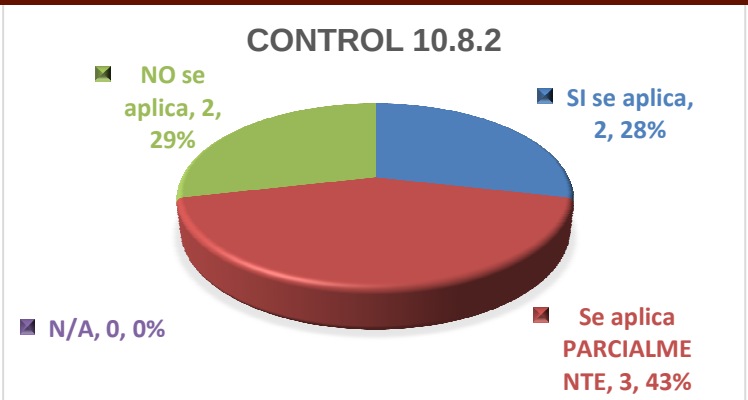
- El 43% de los Trabajadores de la UTI indicaron que el control 10.7.4 SI se aplica en un 80%.
- El 57% indicó que el control se aplica de manera PARCIAL en un 52.5%.

10.8. Intercambio de información	
Control	**Pregunta**
10.8.1 Políticas y procedimientos de intercambio de información	¿Hay establecida una política formal de intercambio, procedimientos y controles para proteger el intercambio de información a través de los servicios de comunicación?



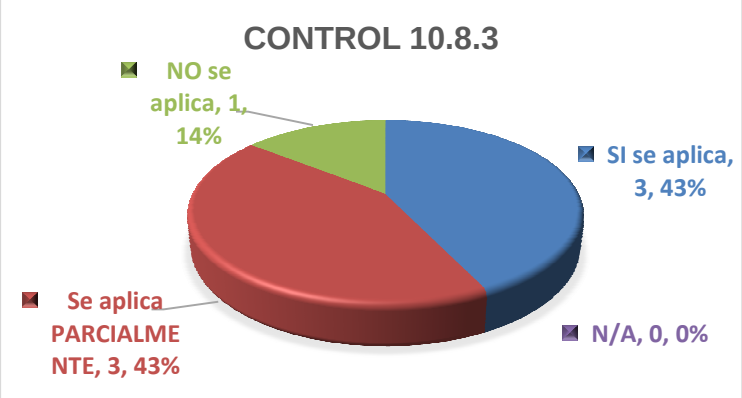
- El 43% de los Trabajadores de la UTI indicaron que el control 10.8.1 SI se aplica en un 80%.
- El 57% indicó que el control se aplica de manera PARCIAL en un 52.5%.

Control	Pregunta
10.8.2 Acuerdos de Intercambio	¿Se han establecido acuerdos para el intercambio de información y software dentro de la organización y con organizaciones externas?



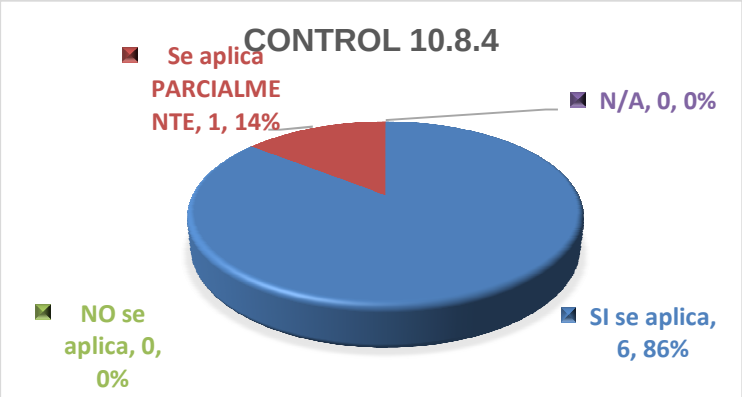
- El 28% de los Trabajadores de la UTI indicaron que el control 10.8.2 SI se aplica en un 80%.
- El 42% indicó que el control se aplica de manera PARCIAL en un 61.6%.
- El 29% indicó que el control NO se aplica (15%).

Control	Pregunta
10.8.3 Medios físicos en tránsito	¿Los medios que contienen información, están protegidos en contra del acceso no autorizado, el mal uso o su alteración durante el transporte más allá de los límites físicos de la organización?



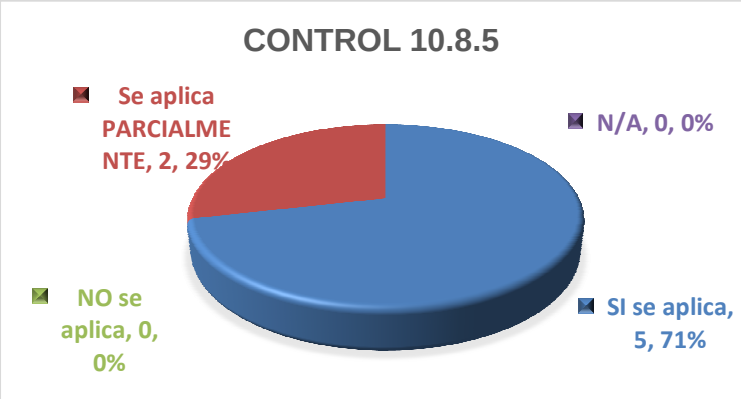
- El 43% de los Trabajadores de la UTI indicaron que el control 10.8.3 SI se aplica en un 86.6%.
- El 43% indicó que el control se aplica de manera PARCIAL en un 50%.
- El 14% indicó que el control NO se aplica (20%).

Control	Pregunta
10.8.4 Mensajería electrónica	¿Está adecuadamente protegida la información involucrada en la mensajería electrónica?



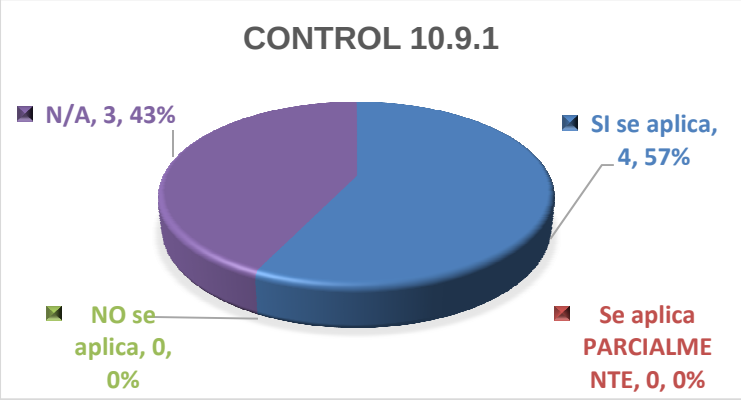
- El 86% de los Trabajadores de la UTI indicaron que el control 10.8.4 SI se aplica en un 83.3%.
- El 14% indicó que el control se aplica de manera PARCIAL en un 40%.

Control	Pregunta
10.8.5 Sistemas de información de negocio	¿Se han desarrollado e implementado políticas y procedimientos para proteger la información asociada a la interconexión de los sistemas de información del negocio?



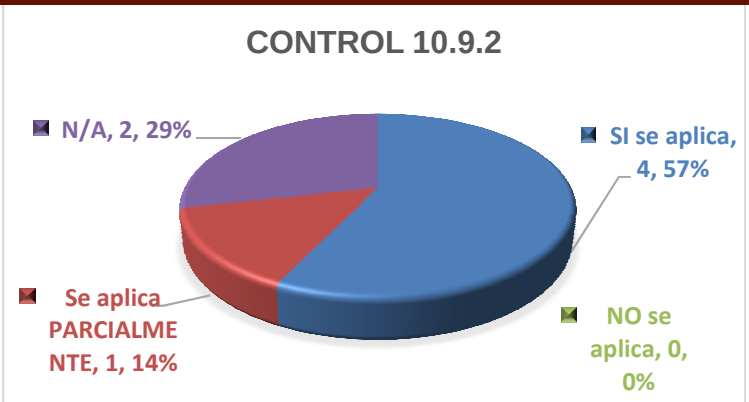
- El 71% de los Trabajadores de la UTI indicaron que el control 10.8.5 SI se aplica en un 82%.
- El 29% indicó que el control se aplica de manera PARCIAL en un 62.5%.

10.9. Servicios de comercio electrónico	
Control	**Pregunta**
10.9.1 Comercio electrónico	¿La información relacionada con el comercio electrónico, que pasa a través de redes públicas, está protegida de las actividades fraudulentas, disputas contractuales, y la divulgación y modificación no autorizada?



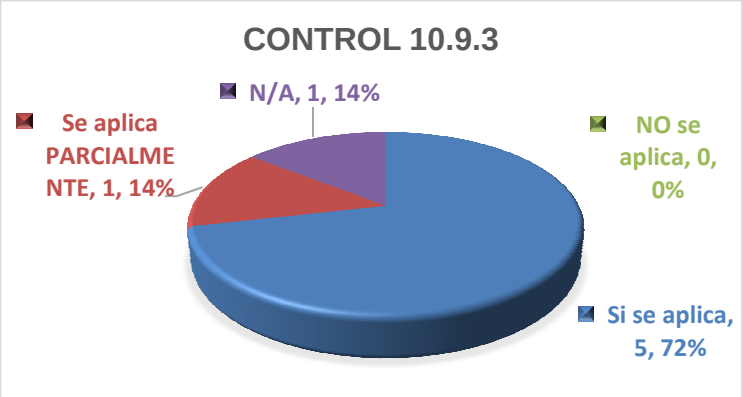
- El 57% de los Trabajadores de la UTI indicaron que el control 10.9.1 SI se aplica en un 85%.
- El 43% indicó que el control no debe de aplicarse.

Control	Pregunta
10.9.2 Transacciones en línea	¿La información involucrada en transacciones on-line, está protegida para prevenir transmisiones incompletas, desvío, modificación no autorizada del mensaje, divulgación no autorizada y para evitar la duplicación o reproducción?



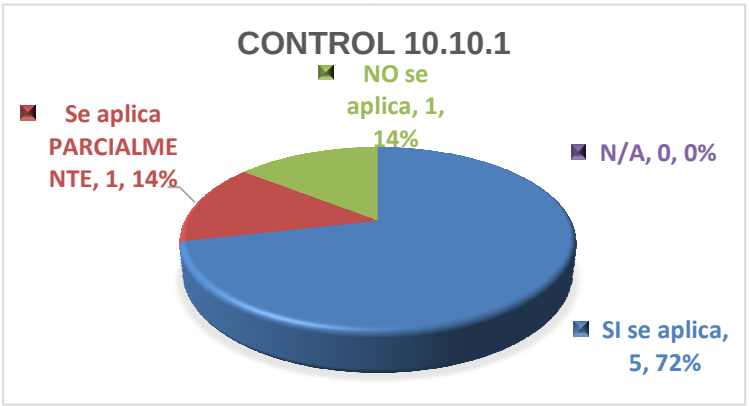
- El 57% de los Trabajadores de la UTI indicaron que el control 10.9.2 SI se aplica en un 82.5%.
- El 14% indicó que el control se aplica de manera PARCIAL en un 50%.
- El 29% indicó que el control no debe de aplicarse.

Control	Pregunta
10.9.3 Información de acceso público	¿La información disponible a través de un sistema público, se encuentra protegida para asegurar su integridad y prevenir modificaciones no autorizadas?



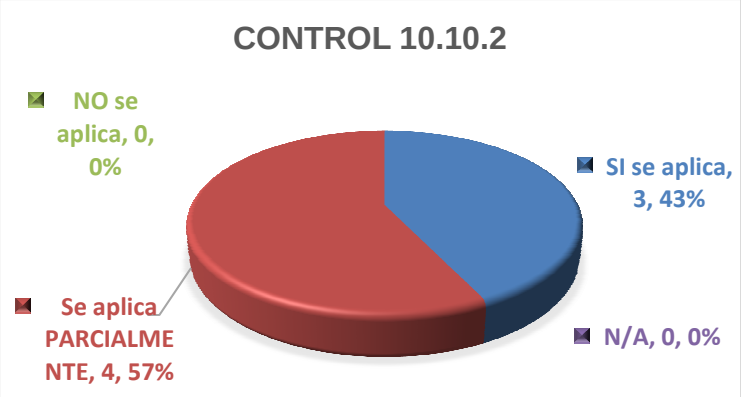
- El 72% de los Trabajadores de la UTI indicaron que el control 10.9.3 SI se aplica en un 85%.
- El 14% indicó que el control se aplica de manera PARCIAL en un 60%.
- El 14% indicó que el control no debe de aplicarse.

10.10. Monitoreo	
Control	**Pregunta**
10.10.1 Registro de eventos	¿Los logs de auditoría registran y mantienen las actividades de los usuarios, las excepciones y los eventos de seguridad de la información, durante un periodo de tiempo acordado, con el fin de ser utilizados en investigaciones futuras y monitorear el control de acceso?



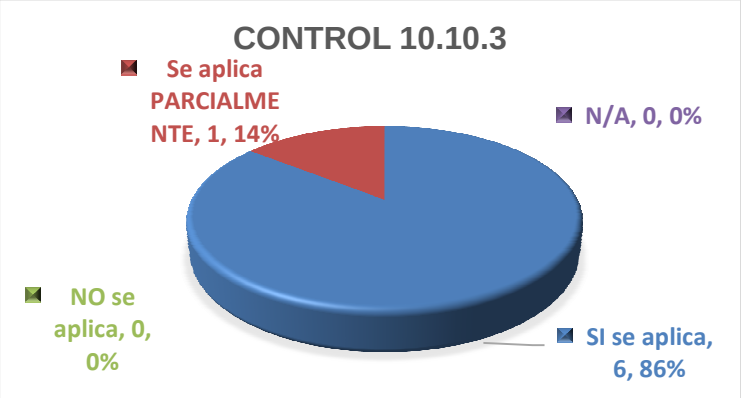
- El 72% de los Trabajadores de la UTI indicaron que el control 10.10.1 SI se aplica en un 87%.
- El 14% indicó que el control se aplica de manera PARCIAL en un 50%.
- El 14% indicó que el control NO se aplica (20%).

Control	Pregunta
10.10.2 Monitoreo del uso de los sistemas	¿Se han establecido procedimientos para monitorear la infraestructura para el procesamiento de la información y los resultados de estas actividades son revisados regularmente?



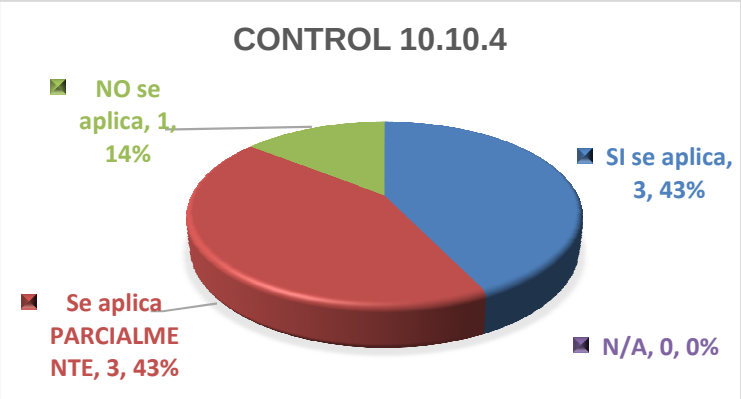
- El 43% de los Trabajadores de la UTI indicaron que el control 10.10.2 SI se aplica en un 85%.
- El 57% indicó que el control se aplica de manera PARCIAL en un 57.5%.

Control	Pregunta
10.10.3 Protección de la información de registros	¿La infraestructura para los registros y la información de estos registros, son protegidos en contra de acceso forzoso o no autorizado?



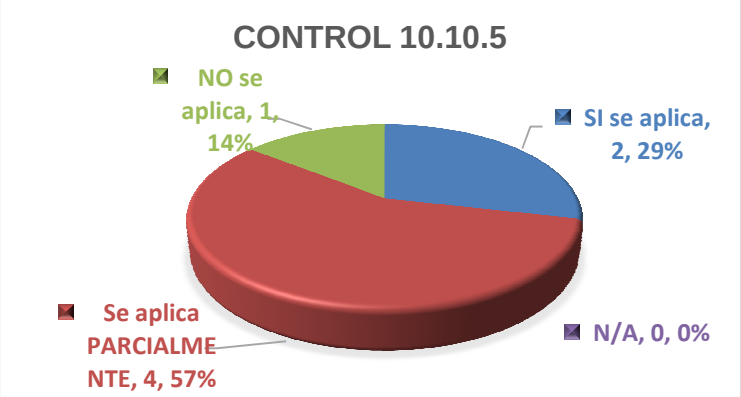
- El 86% de los Trabajadores de la UTI indicaron que el control 10.10.3 SI se aplica en un 85%.
- El 14% indicó que el control se aplica de manera PARCIAL en un 50%.

Control	Pregunta
10.10.4 Registros del administrador y operador	¿Las actividades del administrador y del operador del sistema, son registradas?



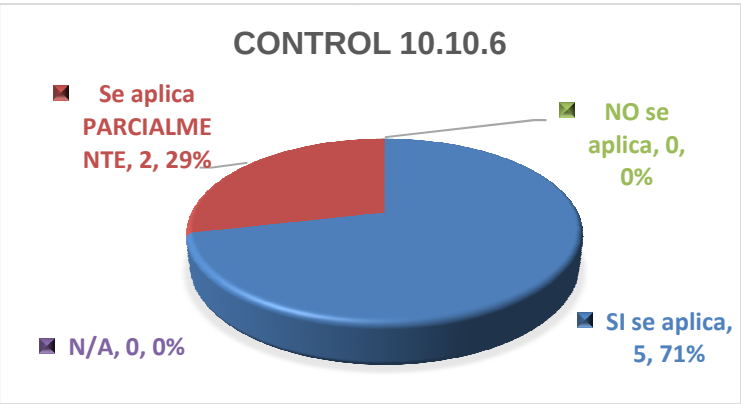
- El 43% de los Trabajadores de la UTI indicaron que el control 10.10.4 SI se aplica en un 90%.
- El 43% indicó que el control se aplica de manera PARCIAL en un 56.6%.
- El 14% indicó que el control NO se aplica (30%).

Control	Pregunta
10.10.5 Registro de fallas	¿Se registran y almacenan los fallos y se toman las medidas oportunas?



- El 29% de los Trabajadores de la UTI indicaron que el control 10.10.5 SI se aplica en un 80%.
- El 57% indicó que el control se aplica de manera PARCIAL en un 50%.
- El 14% indicó que el control NO se aplica (20%).

Control	Pregunta
10.10.6 Sincronización de relojes	¿Se encuentran sincronizados todos los relojes de todos los sistemas relevantes de procesamiento de información en la organización o contenidos en el dominio de seguridad, conforme a una fuente de tiempo de confianza?



- El 71% de los Trabajadores de la UTI indicaron que el control 10.10.6 SI se aplica en un 84%.
- El 29% indicó que el control se aplica de manera PARCIAL en un 55%.

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

ZONA REGISTRAL N°X – SEDE CUSCO

SUPERINTENDENCIA NACIONAL DE LOS REGISTROS PÚBLICOS

DOCUMENTO SOBRE EL ALCANCE DEL PROYECTO

Versión 1.1

Datos sobre la presente edición.-

Versión:	Versión 1.1
Fecha de la Versión:	15 de agosto de 2014
Elaborado por:	[Representante del Comité Operativo de Seguridad]
Revisado por:	[Encargado de Seguridad]
Aprobado por:	[Jefe del Servicio]

Firmas de los responsables.-

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Representante del Comité Operativo de Seguridad	Encargado de Seguridad	Jefe del Servicio

Historial y Control de Versiones.-

Revisión del Documento de la Política de Seguridad de la Información				
Versión	**Fecha**	**Creado por**	**Descripción de la modificación**	**Páginas Modificadas**
V 1.1	15/08/2014	[Representante del Comité Operativo de Seguridad]	Elaboración Inicial	Todas

Consideraciones de Seguridad.-

La presente documentación es propiedad de la Zona Registral N° X – Sede Cusco – SUNARP y tiene el carácter de uso interno. No podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquier otro. Asimismo tampoco podrá ser objeto de préstamo, o cualquier forma de cesión de uso sin el permiso previo y por escrito de la Zona Registral N° X – Sede Cusco, titular de los derechos de propiedad intelectual. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga accesos a la documentación será perseguida conforme dicte la ley.

Tabla de Contenido.-

1. Objetivo, Alcance y Usuarios.-

El objetivo de este documento es definir claramente los límites de seguridad del proyecto, así como también el servicio en el cuál se llevará a cabo, en la Unidad de Tecnologías de la Información (UTI) de la Zona Registral N° X - Sede Cusco.

Este documento se aplica en el transcurso de ejecución del proyecto y en las actividades relacionadas con la Gestión de Comunicaciones y Operaciones de la UTI.

Los usuarios de este documento son los trabajadores de la UTI de la Zona Registral N° X – Sede Cusco y todos los miembros de l equipo del proyecto.

2. Documentos de Referencia.-

- Resolución Ministerial N° 246-2007-PCM “Uso obligat orio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI en todas las entidades integrantes del Sistema Nacional de Informática”.
- 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.
- Norma ISO/IEC 27001, Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Punto 4.3 “Requisitos de documentación”.
- Resolución del Superintendente Nacional de los Registros Públicos N°-044-2014-SUNARP/SN.

3. Definición del Alcance.-

Se requiere definir los límites del proyecto para decidir qué información y/o servicios se quiere proteger dentro de la UTI.

Tomando en cuenta los requisitos legales, normativos, contractuales y de otra índole, el alcance del proyecto se define de acuerdo a los siguientes aspectos:

3.1. Procesos y servicios.-

Los procesos que se toman en cuenta dentro del alcance, para el desarrollo del proyecto, son los que están relacionados netamente con el Servicio de Tecnologías de la Información.

Dichos servicios están considerados en los controles de la cláusula de Gestión de Comunicaciones y Operaciones de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007.

3.2. Unidades Organizativas.-

El presente proyecto se lleva a cabo en la Unidad de Tecnologías de la Información de la Zona Registral N° X – Sede Cusco. SUNARP.

Dicha unidad, cuenta con el apoyo de los siguientes cargos:

- 1 Jefe de UTI
- 1 Operador de Sistemas
- 1 Especialista en Base de Datos
- 2 Técnicos de Sistemas
- 1 Replicador de Base de Datos
- 1 Programador
- 1 Secretaria
- 5 Practicantes

3.3. Ubicaciones.-

La Unidad de Tecnologías de la Información, se ubica físicamente en el 2do piso de las instalaciones de la Zona Registral N° X – Sede Cusco, local ubicado en la Av. Manco Inca N° 210, distrito de Wanchaq, provincia de Cusco.
Cuenta con 3 ambientes, de los cuales 2 de ellos son utilizados para la labor del personal, y el tercero para las instalaciones del Data Center.

3.4. Exclusiones del alcance.-

De las 11 cláusulas estipuladas en la NTP-ISO/IEC 17799:2007, sólo se está tomando en cuenta la cláusula A10 Gestión de Comunicaciones y Operaciones, por estar relacionada directamente con los procesos y servicios de tecnología de información.

Las 10 cláusulas restantes, no se toman en cuenta en el desarrollo del presente proyecto.

Además de ello, como base para la ejecución del presente proyecto, se utilizará la metodología del Ciclo de Deming; el cual incluye 4 etapas a seguir: Planificación, Desarrollo, Control y Acción.

Ésta última etapa (Acción) del Ciclo de Deming no se llevará a cabo en el desarrollo del presente proyecto.

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

ZONA REGISTRAL N°X – SEDE CUSCO

SUPERINTENDENCIA NACIONAL DE LOS REGISTROS PÚBLICOS

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Versión 1.1

Datos sobre la presente edición.-

Versión:	Versión 1.1
Fecha de la Versión:	12 de setiembre de 2014
Elaborado por:	[Representante del Comité Operativo de Seguridad]
Revisado por:	[Encargado de Seguridad]
Aprobado por:	[Jefe del Servicio]

Firmas de los responsables.-

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Representante del Comité Operativo de Seguridad	Encargado de Seguridad	Jefe del Servicio

Historial y Control de Versiones.-

Revisión del Documento de la Política de Seguridad de la Información				
Versión	**Fecha**	**Creado por**	**Descripción de la modificación**	**Páginas Modificadas**
V 1.1	12/09/2014	[Representante del Comité Operativo de Seguridad]	Elaboración Inicial	Todas

Consideraciones de Seguridad.-

La presente documentación es propiedad de la Zona Registral N° X – Sede Cusco – SUNARP y tiene el carácter de uso interno. No podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquier otro. Asimismo tampoco podrá ser objeto de préstamo, o cualquier forma de cesión de uso sin el permiso previo y por escrito de la Zona Registral N° X – Sede Cusco, titular de los derechos de propiedad intelectual. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga accesos a la documentación será perseguida conforme dicte la ley.

Tabla de Contenido.-

1. Objetivo, Alcance y Usuarios.-

La Unidad de Tecnologías de la Información (UTI) de la Zona Registral N° X – Sede Cusco – SUNARP quiere dar a conocer, a través de este documento, a sus trabajadores, clientes, proveedores y otras partes interesadas, su convencimiento de que la Seguridad de la Información es un factor clave para el correcto desarrollo de la organización.

La UTI, reconoce a la Información como activo importante, con la finalidad de mantener su integridad, confidencialidad y disponibilidad. Considera que la Gestión de la Seguridad de la Información, junto con la dotación de formación y recursos necesarios para el desarrollo de la actividad propia de la organización, son los principales pilares en los que se fundamenta el trabajo y esfuerzo diario.

Esta Política de Seguridad se aplica a todo el proyecto, comprendiendo todos los procesos y servicios ya definidos en el Documento del Alcance.

Los usuarios de este documento son los trabajadores de la UTI de la Zona Registral N° X – Sede Cusco y todos los miembros de l equipo del proyecto.

2. Documentos de Referencia.-

- Resolución Ministerial N° 246-2007-PCM “Uso obligat orio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI en todas las entidades integrantes del Sistema Nacional de Informática”.
- Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI, capítulo 5.1 ‘Política de Seguridad’.
- Norma ISO/IEC 27001, Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Punto 5.1 “Compromiso de la gerencia”.
- Documento sobre el Alcance del Proyecto.
- Declaración de la Aplicabilidad (SOA)

3. Terminología básica sobre Seguridad de la Información.-

Para la interpretación adecuada del presente documento se debe tener en cuenta las definiciones establecidas en la NTP-ISO/IEC 17799:2007, las cuáles se listan a continuación:

- **Confidencialidad.-** Característica de la información, que sea accedida por personas autorizadas y que sea usada sólo para los fines para los cuales se le fue entregada.
- **Integridad.-** Característica de la información, que sea exacta y completa. Modificada solo por personas o sistemas autorizados y de una forma permitida.
- **Disponibilidad.-** Característica de la información, que se encuentre disponible en su punto de uso y pueda ser accedida por los entes autorizados en el momento que se requiera.
- **Seguridad de la Información**.- Es la preservación de la Confidencialidad, Integridad y Disponibilidad de la Información.

4. Gestión de la Seguridad de la Información.-

4.1. Objetivos y Medición.-

- Asegurar el cumplimiento de la legislación, reglamentación y normativas aplicables, así como todos aquellos requisitos que la organización considere oportunos llevar a cabo para mantener un la Seguridad de la Información.
- Asignación eficaz de funciones y responsabilidades en el ámbito de la seguridad
- Prevención de posibles defectos y posibles incidentes de seguridad de la información antes de que ocurran.

- Concientización y motivación del personal de la UTI sobre la importancia de la Seguridad de la Información.

4.2. Requisitos para la Seguridad de la Información.-

1. Valoración de los riesgos de la UTI, con ellos se evalúa las amenazas a los activos, se evalúa la vulnerabilidad y la probabilidad de su ocurrencia, estimando su posible impacto.
2. Conjunto de requisitos legales, estatutos, regulaciones y contratos que debería satisfacer la organización.
3. Los principios, objetivos y requisitos que forman parte del tratamiento de la información que la UTI ha desarrollado para apoyar sus operaciones.

4.3. Controles de Seguridad de la Información.-

Se implementará los controles de Seguridad de la Información de una de las cláusulas que la NTP ISO/IEC 17799:2007 recomienda:

- A10. Gestión de Comunicaciones y Operaciones.

Los objetivos de control y controles serán evaluados y elegidos en el Documento de la Declaración de la Aplicabilidad (SOA).

4.4. Responsabilidades.-

Las actividades de seguridad de la Información deben de coordinarse con los representantes elegidos para liderar el presente proyecto.

La seguridad de la Información en la UTI está a cargo de:

- **Comité Formulador:** Se deberá determinar e incluir dentro de este comité al personal técnico y operativo, quienes manejan los sistemas y procedimientos en mayor porcentaje y en primer plano. En ese caso, el Operador, el Especialista en Base de Datos, el Técnico de Sistemas, el Replicador en Base de Datos, el personal encargado de Central de Atenciones, el Programador y los practicantes, conformarían el presente comité.
- **Comité Evaluador:** Se deberá incluir dentro de este grupo al personal jefe del área, quien toma decisiones, delega tareas y supervisa el cumplimiento de las mismas. En ese caso, el Jefe de la Unidad de Tecnologías de información y/o la persona asignada para la jefatura de dicha oficina, conformaría el presente comité.
- **Comité de Seguridad de la Información:** Se deberá incluir dentro de este grupo al personal que represente en un cargo mayor a la institución, toma decisiones, delega tareas, supervisa el cumplimiento de las mismas y emite resoluciones en toda la institución. En ese caso, el Jefe Zonal de la ZRX - Cusco y/o la persona asignada para la jefatura zonal, conformaría el presente comité.

- Equipo de Trabajo
- Propietario
- Custodios
- Usuarios

4.5. Comunicación de la Política.-

El presente documento debe de ser aprobado mediante resolución de la Jefatura de la Zona Registral N° X – Sede Cusco (Co mité de Seguridad de la Información), para poder proceder con la difusión del mismo. La Unidad de Asesoría Legal deberá apoyar con el cumplimiento del presente punto.

La Unidad de Tecnologías de la Información o las que hagan sus veces, dentro del ámbito de su competencia, son responsables de comunicar y difundir entre el personal a su cargo, la presente Política de Seguridad de la Información una vez emitida la Resolución nombrada en el punto anterior.

La Unidad de Comunicaciones deberá publicar dicha Resolución en el Portal Web y en la Intranet de la Superintendencia Nacional de los Registros Públicos.

5. Apoyo para la Implementación del SGSI.-

Cada trabajador de la Unidad de Tecnologías de la Información de la Zona Registral N° X – Sede Cusco, deberá brindar las fac ilidades tanto al Comité de Seguridad de la Información como al Equipo de trabajo y Jefe de Seguridad, para que dichas personas puedan realizar las labores pertinentes para preservar la confidencialidad, integridad y disponibilidad de la información de la organización utilizando los controles de la Gestión de Comunicaciones y Operaciones.

El equipo de trabajo deberá organizarse para concientizar y sensibilizar al 100% de los trabajadores de la UTI sobre el presente proyecto. Todo el personal debe de conocer el objeto de la presente implementación y los beneficios que se traerá consigo.

El jefe de la UTI, deberá controlar y revisar que los trabajadores de su área cumplan con los controles formulados en la cláusula A10 Gestión de Comunicaciones y Operaciones. A la vez, cada trabajador deberá tener presente dichos controles y someterse a ellos, tener en cuenta que la información es propiedad de la organización, por lo tanto no debe de ser difundida.

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

ZONA REGISTRAL N°X – SEDE CUSCO

SUPERINTENDENCIA NACIONAL DE LOS REGISTROS PÚBLICOS

METODOLOGÍA DE GESTIÓN DE RIESGOS

Versión 1.1

Datos sobre la presente edición.-

Versión:	Versión 1.1
Fecha de la Versión:	15 de octubre de 2014
Elaborado por:	[Representante del Comité Operativo de Seguridad]
Revisado por:	[Encargado de Seguridad]
Aprobado por:	[Jefe del Servicio]

Firmas de los responsables.-

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Representante del Comité Operativo de Seguridad	Encargado de Seguridad	Jefe del Servicio

Historial y Control de Versiones.-

Revisión del Documento de la Política de Seguridad de la Información				
Versión	**Fecha**	**Creado por**	**Descripción de la modificación**	**Páginas Modificadas**
V 1.1	15/10/2014	[Representante del Comité Operativo de Seguridad]	Elaboración Inicial	Todas

Consideraciones de Seguridad.-

La presente documentación es propiedad de la Zona Registral N° X – Sede Cusco – SUNARP y tiene el carácter de uso interno. No podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquier otro. Asimismo tampoco podrá ser objeto de préstamo, o cualquier forma de cesión de uso sin el permiso previo y por escrito de la Zona Registral N° X – Sede Cusco, titular de los derechos de propiedad intelectual. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga accesos a la documentación será perseguida conforme dicte la ley.

Tabla de Contenido.-

1. Objetivo, Alcance y Usuarios.-

El objetivo del presente documento es definir la metodología para la gestión de los riesgos de la información en la Unidad de Tecnologías de la Información (UTI) de la Zona Registral N° X – Sede Cusco.

La Gestión de Riesgos abarca el Inventario de Activos, Análisis, Evaluación y Tratamiento de riesgos, los cuales se aplican de acuerdo al alcance del proyecto; es decir, a todos los activos que se utilizan dentro de la UTI o que pueden tener un impacto sobre la seguridad de la información.

Los usuarios de este documento son todos los empleados de la UTI de la Zona Registral N° X – Sede Cusco que participan en la ev aluación y tratamiento de riesgos.

2. Documentos de Referencia.-

- ISO 27005 - Guía para la gestión del riesgo de la seguridad de la información.
- Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI, capítulo 4 ‘Evaluación y Tratamiento de Riesgos’.
- Documento sobre el Alcance del Proyecto.
- Declaración de la Aplicabilidad (SOA).
- Taller de Gestión de Riesgos brindado por la Oficina Nacional de Gobierno Electrónico e Informática. (ONGEI)
- Metodología utilizada en un Sistema de Gestión de Seguridad de la Información (SGSI) exitosamente implementado.

3. Metodología de Gestión de Riesgos.-

El primer paso en la evaluación de riesgos es la identificación de todos los activos dentro del alcance del proyecto; es decir, todos los activos que pueden afectar la confidencialidad, integridad y disponibilidad de la información en la organización. Los activos pueden ser documentos en papel o en formato electrónico, aplicaciones y bases de datos, personas, equipos de TI, infraestructura y servicios externos o procesos externalizados. Al identificar los activos también es necesario identificar a sus propietarios: la persona o unidad organizativa responsable de cada activo.

El siguiente paso es identificar todas las amenazas y vulnerabilidades relacionadas con cada activo. Cada activo puede estar relacionado a varias amenazas, y cada amenaza puede estar vinculada a varias vulnerabilidades.

3.1. Inventario de Activos.-

a) Para realizar el **Inventario de Activos**, se deberá considerar la siguiente tabla que distribuirá a los activos por Tipo y Categoría:

Inventario de Activos		
Tipo	**Código**	**Categoría**
Activos de Información	I1	Información electrónica
	I2	Información escrita
	I3	Información hablada
	I4	Otro tipo de información
Activos de Software	SW1	Software comercial o herramientas, utilitarios
	SW2	Software desarrollado por terceros
	SW3	Software desarrollado internamente
	SW4	Software de administración de base de datos
	SW5	Otro software

Activos Físicos	F1	Equipos de procesamiento
	F2	Equipos de comunicaciones
	F3	Medios de almacenamientos
	F4	Mobiliario y equipamiento
	F5	Otros equipos
Servicio (Terceros)	S1	Procesamiento y Comunicaciones
	S2	Servicios generales
	S3	Otros servicios
Personal	P1	Clientes
	P2	Empleados
	P3	Accionistas
	P4	Personal externo

b) Para determinar el **Valor del Activo**, se deberá considerar la siguiente tabla en base a la Confidencialidad, Integridad y Disponibilidad de la Información.

Valor del Activo	
Valor	**Confidencialidad**
5 (Muy Alto) **81% a 100%**	Cuando la pérdida o falla del activo de información afecta la divulgación o revelamiento no autorizado de la información, impactando **irreversiblemente** la operatividad, competitividad, el cumplimiento legal o imagen institucional de la entidad.
4 (Alto) **61% a 80%**	Cuando la pérdida o falla del activo de información afecta la divulgación o revelamiento no autorizado de la información, impactando **gravemente** la operatividad, competitividad, el cumplimiento legal o imagen institucional de la entidad.
3 (Medio) **41% a 60%**	Cuando la pérdida o falla del activo de información afecta la divulgación o revelamiento no autorizado de la información, impactando **considerablemente** la operatividad, competitividad, el cumplimiento legal o imagen institucional de la entidad.

2 (Bajo) 21% a 40%	Cuando la pérdida o falla del activo de información afecta la divulgación o revelamiento no autorizado de la información, impactando **parcialmente** la operatividad, competitividad, el cumplimiento legal o imagen institucional de la entidad.
1 (Muy Bajo) 0% a 20%	Cuando la pérdida o falla del activo de información afecta la divulgación o revelamiento no autorizado de la información, **no impactando** la operatividad, competitividad, el cumplimiento legal o imagen institucional de la entidad.

Valor del Activo	
Valor	**Integridad**
5 (Muy Alto) 81% a 100%	Cuando la pérdida o falla del activo de información afecta la exactitud y completitud de la información, impactando **irreversiblemente** la operatividad, competitividad, el cumplimiento legal o imagen institucional de la entidad.
4 (Alto) 61% a 80%	Cuando la pérdida o falla del activo de información afecta la exactitud y completitud de la información, impactando **gravemente** la operatividad, competitividad, el cumplimiento legal o imagen institucional de la entidad
3 (Medio) 41% a 60%	Cuando la pérdida o falla del activo de información afecta la exactitud y completitud de la información, impactando **considerablemente** la operatividad, competitividad, el cumplimiento legal o imagen institucional de la entidad.
2 (Bajo) 21% a 40%	Cuando la pérdida o falla del activo de información afecta la exactitud y completitud de la información, impactando **parcialmente** la operatividad, competitividad, el cumplimiento legal o imagen institucional de la entidad.
1 (Muy Bajo) 0% a 20%	Cuando la pérdida o falla del activo de información afecta la exactitud y completitud de la información, **no impactando** la operatividad, competitividad, el cumplimiento legal o imagen institucional de la entidad.

Valor del Activo	
Valor	**Disponibilidad**
5 (Muy Alto) 81% a 100%	Cuando la pérdida o falla del activo de información afecta la accesibilidad y disposición de la información, impactando **irreversiblemente** la operatividad, competitividad, el cumplimiento legal o imagen institucional de la entidad.
4 (Alto) 61% a 80%	Cuando la pérdida o falla del activo de información afecta la accesibilidad y disposición de la información, impactando **gravemente** la operatividad, competitividad, el cumplimiento legal o imagen institucional de la entidad.
3 (Medio) 41% a 60%	Cuando la pérdida o falla del activo de información afecta la accesibilidad y disposición de la información, impactando **considerablemente** la operatividad, competitividad, el cumplimiento legal o imagen institucional de la entidad.
2 (Bajo) 21% a 40%	Cuando la pérdida o falla del activo de información afecta la accesibilidad y disposición de la información, impactando **parcialmente** la operatividad, competitividad, el cumplimiento legal o imagen institucional de la entidad.
1 (Muy Bajo) 0% a 20%	Cuando la pérdida o falla del activo de información afecta la accesibilidad y disposición de la información, **no impactando** la operatividad, competitividad, el cumplimiento legal o imagen institucional de la entidad.

c) Se estima el Valor del Activo del promedio de sumar los valores del nivel de importancia de la Confidencialidad, Integridad y Disponibilidad.

Valor del Activo = (C + I + D) / 3

d) El Nivel de Tasación del Activo se determina de acuerdo a la siguiente tabla:

Nivel de Tasación del Activo	
Valor del Activo	**Nivel de Tasación**
3.3334 – 5	Alto
1.668 – 3.333	Medio
1 – 1.667	Bajo

e) El formato de tabla a utilizar para el llenado de los datos del Inventario de Activos, es el siguiente:

INVENTARIO DE ACTIVOS																		
N°	Activo	Descripción	Categoría	Clasificación			Frecuencia de Uso					Propietario	Custodio	Valor del Activo y Nivel de Tasación				
				Pública	Uso Interno	Uso Restringido	Diario	Semanal	Quincenal	Mensual	Eventual			Confidencialidad	Integridad	Disponibilidad	Valor del Activo	Nivel de Tasación
Activos de Información																		
Activos de Software																		
Activos Físicos																		
Servicios (Terceros)																		
Persona (Clientes, Empleados, Personal Externo)																		

3.2. Análisis de Riesgos.-

a) Para realizar el Análisis de Riesgos, se deberá tomar en cuenta la siguiente tabla para el correspondiente llenado de datos:

ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN													
N°	Activo	Amenaza		Mecanismo de protección existente						Vulnerabilidad		Riesgo	
		Descripción	Nivel de Amenaza	Preventivo	Nivel de Capacidad	Detectivo	Nivel de Capacidad	Correctivo	Nivel de Capacidad	Descripción	Nivel de Vulnerabilidad	Probabilidad de Ocurrencia	Nivel de Probabilidad de Ocurrencia
Amenazas a los Activos de Información													
Amenazas a los Activos de Software													
Amenazas a los Activos Físicos													
Amenazas a los Servicios (Terceros)													
Amenazas al Personal (Clientes, Empleados, Personal Externo)													

b) Para determinar el **Nivel de Amenaza**, se deberá considerar la siguiente:

- **Amenaza:** Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización.
- **Nivel de Amenaza:** Estimación de la probabilidad de ocurrencia de la amenaza.

Nivel de Amenaza (Escala de Likerd)	
5	Muy Alto (Una vez a la semana)
4	Alto (Una vez al mes)
3	Medio (Una vez cada 6 meses)
2	Bajo (Una vez al año)
1	Muy Bajo (Una vez cada 5 años)

c) El **Nivel de Capacidad**, es el nivel que los mecanismos de protección (Preventivos, Detectivos, Correctivos) existentes han alcanzado.

d)

Nivel de Capacidad (SPICE – ISO 15504)	
5	Predecible: La ejecución de los controles se monitorea a través de la recopilación y análisis de mediciones para controlar y corregir la eficacia de los controles.
4	Definido: La ejecución del control se realiza utilizando un estándar definido por la institución
3	Gestionado: La ejecución del control se gestiona y controla (documentado)
2	Realizado: Control implantado, logra su objetivo definido (no documentado)
1	Incompleto: Control no implantado o no logra conseguir su objetivo

e) Para determinar el **Nivel de Vulnerabilidad**, se deberá considerar lo siguiente:

- **Vulnerabilidad:** Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas.
- **Nivel de Vulnerabilidad:** Grado de exposición que posee el activo frente a una amenaza. Se calcula con la siguiente fórmula:

Nivel de Vulnerabilidad = 6 - (Nivel de Capacidad de Controles Preventivos + Nivel de Capacidad de Controles Detectivos + Nivel de Capacidad de Controles Correctivos) / 3

Nivel de Vulnerabilidad (Escala de Likerd)	
5	Muy Alto (Impactaría irreversiblemente) (81% a 100%)
4	Alto (Impactaría gravemente) (61% a 80%)
3	Medio (Impactaría considerablemente) (41% a 60%)
2	Bajo (Impactaría parcialmente) (21% a 40%)
1	Muy Bajo (No impactaría) (0% a 20%)

f) El **Riesgo** es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad de un activo de información, causando un determinado impacto en la Institución.

- **Probabilidad de Ocurrencia del Riesgo:** Se estima del promedio de los valores resultantes del Nivel de Vulnerabilidad y el Nivel de Amenaza.

Probabilidad de Ocurrencia = (Nivel de Vulnerabilidad + Nivel de Amenaza) / 2

- **Nivel de Probabilidad de Ocurrencia del Riesgo:** Estimación de la probabilidad de ocurrencia del riesgo.

Probabilidad de Ocurrencia	Nivel de Probabilidad de Ocurrencia
3.3334 – 5	Alto
1.668 – 3.333	Medio
1 – 1.667	Bajo

3.3. Evaluación de Riesgos.-

Para la evaluación del riesgo, se deben de tomar en cuenta criterios para determinar el significado del riesgo y los niveles de riesgo:

a) Para determinar los criterios de evaluación del riesgo, se deberán medir de acuerdo a los siguientes Impactos:

- **Impacto Legal:** Estimación de la probabilidad de que el riesgo pueda producir el incumplimiento de cualquier ley, requisito reglamentario y regulación contractual:

Impacto Legal	
5	Muy Alto (Afecta irreversiblemente a la Institución) (81% a 100%)
4	Alto (Afecta drásticamente a la Institución) (61% a 80%)
3	Medio (Afecta seriamente a la Institución) (41% a 60%)
2	Bajo (Afecta parcialmente a la Institución) (21% a 40%)
1	Muy Bajo (No afecta a la Institución) (0% a 20%)

- **Impacto Económico / Imagen Institucional:** Nivel de impacto de la amenaza sobre la capacidad económica (generar ingresos o dejar de percibirlos) de la institución:

Impacto Económico / Imagen Institucional	
5	Muy Alto (Pérdidas iguales o superiores a S/. 100,000)
4	Alto (Pérdidas iguales o superiores a S/. 50,000 y menores que S/. 100,000)
3	Medio (Pérdidas iguales o superiores a S/. 10,000 y menores a S/. 50,000)
2	Bajo (Pérdidas iguales o superiores a S/. 5,000 y menores que S/. 10,000)
1	Muy Bajo (Pérdidas menores a S/. 5,000)

- **Impacto Operacional:** Estimación de la probabilidad de que el riesgo identificado pueda producir la paralización de operaciones de la institución:

Impacto Operacional	
5	Muy Alto (Afecta irreversiblemente la operatividad de los procesos de la Institución) (81% a 100%)
4	Alto (Afecta drásticamente la operatividad de los procesos de la Institución) (61% a 80%)
3	Medio (Afecta seriamente la operatividad de los procesos de la Institución) (41% a 60%)
2	Bajo (Afecta parcialmente la operatividad de los procesos de la Institución) (21% a 40%)
1	Muy Bajo (No afecta la operatividad de los procesos de la Institución) (0% a 20%)

b) El **Nivel de Impacto** del riesgo, se estima del promedio de sumar los valores del Impacto Legal, Operacional y Económico.

Nivel de Impacto = (Impacto Legal + Impacto Operacional + Impacto Económico) / 3

c) El **Nivel de Exposición** del riesgo, se estima del promedio de sumar los valores del Valor del activo, Probabilidad de ocurrencia del riesgo y el Nivel de impacto.

Nivel de Exposición = (Valor del activo + Probabilidad de ocurrencia + Nivel de Impacto) / 3

d) El **Nivel de Riesgo** se determina con los valores de la siguiente tabla:

Nivel de Riesgo	
Nivel de Exposición al Riesgo	**Nivel de Riesgo**
3.334 – 5	Crítico
1.6668 – 3.333	Moderado
1 – 1.667	Aceptado

e) El formato de tabla a utilizar para el llenado de los datos de la Evaluación de Riesgos, es el siguiente:

EVALUACIÓN DE RIESGOS										
N°	Activo	Amenaza	Criterios de Evaluación						Riesgo Efectivo	
			Impacto				Probabilidad de Ocurrencia del Riesgo	Valor del Activo	Nivel de Exposición al Riesgo	Nivel de Riesgo
			Impacto Legal	Impacto Económico / Imagen Institucional	Impacto Operacional	Nivel de Impacto				
Amenazas a los Activos de Información										
Amenazas a los Activos de Software										
Amenazas a los Activos de Físicos										
Amenazas a los Servicios										
Amenazas al Personal (Clientes, Empleados, Personal Externo)										

3.4. Tratamiento de Riesgos.-

a) El valor que define la frontera entre los riesgos aceptables y los que no lo son es conocido como **Umbral de Aceptación de Riesgos**.
Dicho umbral lo define la organización como el Nivel de Tolerancia: **Crítico (3.333)** arriba.

Nivel de Exposición al Riesgo	Nivel de Tolerancia
3.334 - 5	Crítico
1.668 – 3.333	Moderado
1 – 1.667	Aceptado

b) Para valores sobre este umbral se deben evaluar estrategias u opciones de tratamiento para reducir el nivel de exposición a los riesgos identificados, éstas opciones son:

Opción para el Tratamiento	
R	**Reducir** (Reducir el impacto o la probabilidad de ocurrencia a niveles aceptables mediante la implementación de controles de seguridad de la información.
A	**Aceptar** (Aceptar la posibilidad de que pueda ocurrir el riesgo sin tomar medidas de acción concretas)
E	**Evitar** (Reducir a su mínima expresión la posibilidad de ocurrencia de la amenaza)
T	**Transferir** (Transferir el impacto del riesgo a terceros (empresas aseguradoras o proveedores de servicio))

c) El **Costo Aproximado** es la estimación del costo para implementar la función de protección propuesta, se determina con los valores de la siguiente tabla:

Costo Aproximado	
4	Mayor a S/. 100,000
3	De S/. 30,000 a S/. 100,000
2	De S/. 15,000 a S/. 30,000
1	Menor a S/. 15,000
D	Desconocido

d) El **Tiempo Aproximado** es la estimación del costo para implementar la función de protección propuesta, se determina con los valores de la siguiente tabla:

Tiempo Aproximado	
C	Corto plazo (Menos de 3 meses)
M	Mediano plazo (De 3 a 12 meses)
L	Largo plazo (Más de 1 año)
D	Desconocido

e) El **Riesgo Residual** es el riesgo remanente después de un tratamiento de riesgos. Se calcula con la suma del Riesgo Efectivo y el Control elegido para reducir el riesgo:

Riesgo Residual = Riesgo Efectivo + Control (Reduce el riesgo)

f) El formato de tabla a utilizar para el llenado de los datos del Tratamiento de Riesgos, es el siguiente:

TRATAMIENTO DE RIESGOS													
N°	Activo	Amenaza	Riesgo Efectivo					Control Propuesto	Descripción / Observaciones	Cumplimiento del Control (Según NTP-ISO/IEC 17799:2007	Costo Aprox.	Tiempo Aprox.	Opción para el Tratamiento
			Nivel de Impacto	Probabilidad de Ocurrencia del Riesgo	Valor del Activo	Nivel de Exposición al Riesgo	Nivel de Tolerancia						
Amenazas a los Activos de Información													
Amenazas a los Activos de Software													
Amenazas a los Activos Físicos													
Amenazas a los Servicios													
Amenazas al Personal (Clientes, Empleados, Personal Externo)													

Anexo A.5

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

ZONA REGISTRAL N°X – SEDE CUSCO

SUPERINTENDENCIA NACIONAL DE LOS REGISTROS PÚBLICOS

DECLARACIÓN DE LA APLICABILIDAD (SOA)

Versión 1.1

Datos sobre la presente edición.-

Versión:	Versión 1.1
Fecha de la Versión:	20 de noviembre de 2014
Elaborado por:	[Representante del Comité Operativo de Seguridad]
Revisado por:	[Encargado de Seguridad]
Aprobado por:	[Jefe del Servicio]

Firmas de los responsables.-

ELABORADO POR:	**REVISADO POR:**	**APROBADO POR:**
Representante del Comité Operativo de Seguridad	Encargado de Seguridad	Jefe del Servicio

Historial y Control de Versiones.-

Revisión del Documento de la Política de Seguridad de la Información				
Versión	**Fecha**	**Creado por**	**Descripción de la modificación**	**Páginas Modificadas**
V 1.1	20/11/2014	[Representante del Comité Operativo de Seguridad]	Elaboración Inicial	Todas

Consideraciones de Seguridad.-

La presente documentación es propiedad de la Zona Registral N° X – Sede Cusco – SUNARP y tiene el carácter de uso interno. No podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquier otro. Asimismo tampoco podrá ser objeto de préstamo, o cualquier forma de cesión de uso sin el permiso previo y por escrito de la Zona Registral N° X – Sede Cusco, titular de los derechos de propiedad intelectual. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga accesos a la documentación será perseguida conforme dicte la ley.

Tabla de Contenido.-

1. Objetivo, Alcance y Usuarios.-

El objetivo del presente documento es definir qué controles son adecuados para implementar en la Unidad de Tecnologías de la Información de la Zona Registral N° X – Sede Cusco, cuáles son los objetivos de esos controles y cómo se implementan. También tiene como objetivo aprobar riesgos residuales y aprobar formalmente la implementación de los controles mencionados.

Este documento incluye todos los controles detallados en la Norma Técnica Peruana ISO/IEC 17799:2007. Los controles se aplican según lo indicado y limitado en el documento del alcance del proyecto.

Los usuarios de este documento son todos los empleados de la Unidad de Tecnologías de la Información de la Zona Registral N° X – Sede Cusco que cumplen una función dentro del proyecto.

2. Documentos de Referencia.-

- Norma ISO/IEC 27001, Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Punto 4.3 “Requisitos de documentación”.
- Documento sobre el Alcance del Proyecto.
- Documento de la Metodología de Gestión de Riesgos

3. Aplicabilidad de los controles.-

En la siguiente tabla, podemos apreciar la lista de los controles detallados en la cláusula A10. Gestión de Comunicaciones y Operaciones de la Norma Técnica Peruana NTP ISO/IEC 17799:2007, podremos apreciar cuales son aplicables y cuales no lo son en el presente proyecto, con su debida justificación:

APLICABILIDAD DE CONTROLES CLÁUSULA (A10) GESTIÓN DE COMUNICACIONES Y OPERACIONES					
ID	**Controles según la NTP ISO/IEC 17799:2007**	**Aplicabilidad (SI/NO)**	**Justificación de elección / no elección**	**Objetivos de Control**	**Estado**
10.1 Procedimientos y responsabilidades de operación					
10.1.1	Documentación de procedimientos operativos	SI	No todos los procedimientos operativos están documentados, éstos son de gran ayuda para todo el personal diariamente y ante incidentes o problemas	Se deberían documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo requieran.	Parcialmente implementado
10.1.2	Gestión de cambios	SI	Los cambios y actualizaciones que presentan los sistemas no suelen ser documentados ni controlados	Se deberían controlar los cambios en los sistemas y recursos de tratamiento de información.	Planificado
10.1.3	Segregación de tareas	SI	El control de tareas y privilegios ayudará a prevenir accesos no autorizados y a no sobrecargar funciones al personal	Se deberían segregar las tareas y las áreas de responsabilidad con el fin de reducir las oportunidades de una modificación no autorizada o no intencional, o el de un mal uso de los activos de la organización.	Parcialmente implementado
10.1.4	Separación de los recursos para desarrollo y para producción	SI	No se encuentra una separación adecuada de los entornos de desarrollo y producción, por lo que podría causar cambios no deseados en el entorno de desarrollo	La separación de los recursos para desarrollo, prueba y producción es importante para reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional.	Planificado
10.2 Gestión de Servicios externos					
10.2.1	Servicio de entrega	NO	La UTI no maneja ningún servicio de externos y/o de terceros directamente	-	-
10.2.2	Monitoreo y revisión de los servicios externos	NO	La UTI no maneja ningún servicio de externos y/o de terceros directamente	-	-

10.2.3	Gestionando cambios para los servicios externos	NO	La UTI no maneja ningún servicio de externos y/o de terceros directamente	-	-
10.3 Planificación y Aceptación del sistema					
10.3.1	Planificación de la capacidad	SI	El monitoreo de los sistemas utilizados en la UTI ayudará a identificar amenazas a la seguridad del sistema para sus proyecciones.	El uso de recursos debe ser monitoreado y las proyecciones hechas de requisitos de capacidades adecuadas futuras para asegurar el sistema de funcionamiento requerido	Planificado
10.3.2	Aceptación del sistema	SI	Se necesita que se realice un desarrollo de pruebas y criterios de aceptación de los sistemas antes de ser implementados	Se deberían establecer criterios de aceptación para nuevos sistemas de información y versiones nuevas o mejoradas y se deberían desarrollar con ellos las pruebas adecuadas antes de su aceptación	Parcialmente implementado
10.4 Protección contra software malicioso					
10.4.1	Medidas y controles contra software malicioso	SI	La UTI necesita controlar y revisar si es que existe software malicioso para no perjudicar la seguridad de la información	Se deberían implantar controles para detectar el software malicioso y prevenirse contra él, junto a procedimientos adecuados para concientizar a los usuarios.	Parcialmente implementado
10.4.2	Medidas y controles contra código móvil	SI	Se debe controlar y evitar un uso desautorizado de internet asegurando el acceso y utilización del código móvil	Donde el uso de código móvil es autorizado, la configuración debe asegurar que dicho código móvil opera de acuerdo a una política de seguridad definida y que se debe de prevenir que este sea ejecutado	Parcialmente implementado
10.5 Gestión de respaldo y recuperación					
10.5.1	Recuperación de la información	SI	Las copias de seguridad de la información de la UTI se deben de realizar regularmente, para poder recuperarse ante un desastre o fallo de los medios	Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, en concordancia con la política acordada de recuperación	Parcialmente implementado

10.6 Gestión de seguridad en redes					
10.6.1	Controles de red	SI	El administrador de la red de la UTI debe implantar controles y medidas requeridas para conseguir y conservar la seguridad de los datos en las redes de las computadoras	Las redes deben de ser manejadas y controladas adecuadamente para protegerse de amenazas y para mantenerse la seguridad en los sistemas y aplicaciones usando las redes, incluyendo información en tránsito	Parcialmente implementado
10.6.2	Seguridad en los servicios de redes	SI	La UTI suele requerir servicios de red para realizar correctamente sus labores	Las características de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en cualquier acuerdo de servicio de red, así estos servicios sean provistos dentro o fuera de la organización	Parcialmente implementado
10.7 Utilización de los medios de información					
10.7.1	Gestión de medios removibles	SI	Los medios removibles deben de ser controlados y físicamente protegidos para prevenir acceso no autorizado, modificaciones y evitar daños a los activos	Deberían haber procedimientos para la gestión de los medios informáticos removibles	Parcialmente implementado
10.7.2	Eliminación de medios	SI	Los soportes que no se vayan a utilizar más, deben ser eliminados de forma segura y sin inconvenientes por medio de procedimientos formales	Se deberían eliminar los medios de forma segura y sin peligro cuando no se necesiten más, utilizando procedimientos formales	Planificado
10.7.3	Procedimientos de manipulación de la información	SI	La información no se encuentra clasificada correctamente, por lo tanto el procedimiento para su manipulación y almacenamiento no está establecido en su totalidad	Los procedimientos para la manipulación y almacenamiento de la información deben ser establecidos para proteger esta información de divulgaciones o usos no autorizados	Planificado
10.7.4	Seguridad de la documentación de sistemas	SI	El acceso a la documentación de sistemas de la UTI no es totalmente restringido	La documentación de sistemas debe ser protegida contra acceso no autorizado	Planificado

10.8 Intercambio de Información					
10.8.1	Políticas y procedimientos para el intercambio de información y software	SI	En la UTI no existen procedimientos que cuiden la información intercambiada mediante correo electrónico, fax, teléfonos, descargas de internet, etc	Se deberían establecer políticas, procedimientos y controles formales de intercambio con el fin de proteger la información a través de todos los tipos de instalaciones de comunicación	Planificado
10.8.2	Acuerdos de intercambio	NO	En la UTI no se realizan intercambios de información y software entre la organización y terceros	-	-
10.8.3	Medios físicos en tránsito	SI	Cuando los medios físicos se encuentran en tránsito, no se protegen correctamente ni presentan controles que verifiquen que el transporte físico sea correcto	Los medios conteniendo información deben de ser protegidos contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización	Planificado
10.8.4	Seguridad en la mensajería electrónica	NO	El servicio de correo electrónico lo maneja la UTI de la sede central en LIMA	-	-
10.8.5	Sistemas de información de negocios	SI	Los sistemas de información de negocios son compartidos entre los usuarios sin ningún control, lo que puede generar alteraciones al sistema por accesos no autorizados	Se deberían desarrollar e implementar políticas y procedimientos con el fin de proteger la información asociada con la interconexión de sistemas de información de negocios	Planificado
10.9 Servicios de comercio electrónico					
10.9.1	Comercio electrónico	NO	En la UTI no se realizan servicios de comercio electrónico	-	-
10.9.2	Transacciones en línea	NO	En la UTI no se realizan servicios de transacciones en línea	-	-
10.9.3	Información pública disponible	NO	En la UTI de la Zona Registral N°X Sede Cusco no maneja la página web institucional de SUNARP	-	-

10.10 Monitoreo					
10.10.1	Registro de la auditoría	SI	Los registros de auditoria solo están implementados en ciertos servidores por lo que la información en los demás son vulnerables ya que no cuentan con los lineamientos establecidos en la norma.	Los registros de auditoria grabando actividades de los usuarios, excepciones y eventos de la seguridad de información deben ser producidos y guardados para un periodo acordado con el fin de que asistan en investigaciones futuras y en el monitoreo de los controles de acceso.	Parcialmente implementado
10.10.2	Monitoreando el uso del sistema	SI	La UTI revisa alteraciones de información en los sistemas cuando lo soliciten o cuando ocurre un incidente, más no cuenta con un monitoreo planificado de uso de todos los sistemas	Los procedimientos para el uso del monitoreo de las instalaciones de procesamiento de información deben ser establecidos y los resultados de las actividades de monitoreo deben ser revisadas regularmente	Planificado
10.10.3	Protección de la información de registro	SI	La protección a dichos registros si existen pero no están debidamente documentados	Las instalaciones de información de registro deben de ser protegidas contra acciones forzosas u acceso no autorizado	Parcialmente implementado
10.10.4	Registro de administradores y operadores	SI	Las actividades del administrados y del operador del sistema sin son registradas, pero no se aplican en su totalidad y no están documentados	Las actividades del administrador y de los operadores del sistema deben ser registradas	Parcialmente implementado
10.10.5	Registro de la avería	SI	No existe un registro de averías	Las averías deben ser registradas, analizadas y se deben de tomar acciones apropiadas	Planificado
10.10.6	Sincronización del reloj	SI	La UTI no cuenta con una fuente de tiempo para sincronizar los relojes de los sistemas.	Los relojes de todos los sistemas de procesamiento de información dentro de la organización o del dominio de seguridad deben ser sincronizados con una fuente acordada y exacta de tiempo	Parcialmente implementado

Anexo A.6

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

ZONA REGISTRAL N°X – SEDE CUSCO

SUPERINTENDENCIA NACIONAL DE LOS REGISTROS PÚBLICOS

PLAN DE CAPACITACIÓN Y CONCIENCIACIÓN

Versión 1.1

Datos sobre la presente edición.-

Versión:	Versión 1.1
Fecha de la Versión:	20 de febrero de 2015
Elaborado por:	[Representante del Comité Operativo de Seguridad]
Revisado por:	[Encargado de Seguridad]
Aprobado por:	[Jefe del Servicio]

Firmas de los responsables.-

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Representante del Comité Operativo de Seguridad	Encargado de Seguridad	Jefe del Servicio

Historial y Control de Versiones.-

Revisión del Documento de la Política de Seguridad de la Información				
Versión	**Fecha**	**Creado por**	**Descripción de la modificación**	**Páginas Modificadas**
V 1.1	20/02/2015	[Representante del Comité Operativo de Seguridad]	Elaboración Inicial	Todas

Consideraciones de Seguridad.-

La presente documentación es propiedad de la Zona Registral N° X – Sede Cusco – SUNARP y tiene el carácter de uso interno. No podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquier otro. Asimismo tampoco podrá ser objeto de préstamo, o cualquier forma de cesión de uso sin el permiso previo y por escrito de la Zona Registral N° X – Sede Cusco, titular de los derechos de propiedad intelectual. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga accesos a la documentación será perseguida conforme dicte la ley.

Tabla de Contenido.-

1. Introducción.-

La Unidad de Tecnologías de la Información (UTI) de la Zona Registral N° X - Sede Cusco, es el órgano encargado de la sistematización, ejecución del procesamiento de la información, administración, mantenimiento y soporte técnico del Sistema Informático de la Zona.

A través del presente documento se busca establecer programas, fechas, temas, metodologías, de capacitación al personal de la UTI, para que reciban el entrenamiento adecuado en relación a la Cláusula de Gestión de Operaciones y Comunicaciones de la NTP-ISO/IEC 17799:2007.

2. Alcance y Usuarios.-

El Presente documento contiene el plan de capacitación y concienciación establecidos en los requisitos de la Norma Técnica Peruana ISO/IEC 17799:2007, para el personal de la Unidad de Tecnologías de la Información de la Zona Registral N° X – Sede Cusco, según lo indic ado y limitado en el documento del alcance del proyecto.

Los usuarios de este documento son todos los empleados de la Unidad de Tecnologías de la Información de la Zona Registral N° X – Sede Cusco que cumplen una función dentro del proyecto.

3. Documentos de Referencia.-

- Norma ISO/IEC 27001, Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Punto 4.3 “Requisitos de documentación”.
- Documento sobre el Alcance del Proyecto.
- Documento del Plan de Capacitación y Concienciación.

4. Objetivos.-

- Reforzar la Gestión de Operaciones y Comunicaciones de la NTP-ISO/IEC 17799:2007, mediante la capacitación y concientización del personal involucrado en su procesamiento, comprometiéndolos a velar por ella, asumir responsabilidades y seguir los procedimientos para garantizar su seguridad de información.

- Dar a conocer la terminología y los conceptos básicos para realizar una adecuada Gestión de Operaciones y Comunicaciones de la NTP-ISO/IEC 17799:2007.

- Exponer los controles requeridos Gestión de Operaciones y Comunicaciones de acuerdo a la NTP-ISO/IEC 17799:2007.

- Explicar el propósito de la Implementación de la Gestión de Operaciones y Comunicaciones de la NTP-ISO/IEC 17799:2007 y los procesos para el establecimiento, la implementación, el monitoreo y la mejora de la Gestión en mención.

- Interpretar los requisitos y procedimientos para la formulación de un plan de actividades de la Cláusula Gestión de Operaciones y Comunicaciones de la NTP-ISO/IEC 17799:2007, para su implementación en la UTI.

5. Descripción de la Capacitación.-

- La capacitación está dirigida al personal que labora en la Unidad de Tecnologías de la Información de la Zona Registral N°X – Sede Cusco.

- El lugar donde se realizará la capacitación es en la Oficina de la Unidad de Tecnologías de la Información, ubicada en la Av. Manco Inca N° 210, Wanchaq, Cusco.

- La modalidad de la capacitación será presencial.

- La duración de la capacitación será de 19 horas.

- Los materiales de capacitación son :
  - NTP ISO/IEC 27001:2008
  - NTP ISO/IEC 17799:2007
  - Presentaciones de la Capacitación

- Se realizará una evaluación del dictado del curso al final del día.

La descripción de los temas a capacitar y la cantidad de horas, se detallan en el siguiente cuadro:

CRONOGRAMA DE CAPACITACIÓN		
Día	**Descripción**	**Cantidad de Horas**
CAPACITACIÓN EN CONCIENCIACIÓN DEL PERSONAL		**2**
Día 1	Concientización en Seguridad de la Información enfocada a la Gestión de Operaciones y Comunicaciones	2
CAPACITACIÓN EN LA NTP ISO/IEC 17799:2007		**17**
Día 1	**Sesión 1: Introducción**	2
	Consideraciones previas del curso e introducción al tema	
	Terminología y conceptos básicos	
	Norma Técnica Peruana NTP ISO/IEC 17799:2007 e ISO 27001:2005	
	Metodología para la Evaluación de Riesgos	
	Sesión 2: Controles de Seguridad de la Información Pate I	2
	Política de Seguridad de la Información – Comités de Seguridad	
	Consideraciones para el diseño de Políticas de Seguridad	
	Declaración de Aplicabilidad – SOA	
Día 2	**Sesión 3: Implementación de un Sistema de Gestión de Seguridad de la Información**	2
	Documentación requerida	
	Procedimientos del SGSI	
	Implementación del SGSI	
Día 2	**Sesión 4: Controles de Seguridad de la Información Parte II**	3
	Cláusula 5: Política de Seguridad	
	Cláusula 6: Aspectos Organizativos para la Seguridad	
	Cláusula 7: Clasificación y Control de Activos	
	Cláusula 8. Seguridad en Recursos Humanos	
	Cláusula 9: Seguridad Física y del Entorno	
	Cláusula 11: Control de Accesos	
	Cláusula 12: Adquisición, Desarrollo y Mantenimiento	
	Cláusula 13: Gestión de Incidentes de Seguridad	

	Cláusula 14: Gestión de Continuidad del Negocio	
	Cláusula 15: Cumplimiento	
Día 3	**Sesión 5: Controles de la Cláusula 10: Gestión de Comunicaciones y Operaciones**	4
	Cláusula 10: Gestión de Comunicaciones y Operaciones	
Día 4	**Sesión 6: Capacitación en Gestión de Riesgos**	4
	Inventario de Activos	
	Análisis de Riesgos	
	Evaluación de Riesgos	
	Tratamiento de Riesgos	
	Total de Horas	**19**

6. Formato de Evaluación.-

La evaluación al personal, consiste en evaluar el nivel de aprendizaje obtenido durante la capacitación, para lo cual dicha evaluación se realizará cada día al término de capacitación, considerando también importante la participación en los talleres realizados, el método de evaluación es de la siguiente manera:

- Día 1 = (Talleres * 0.3) + (Concientización * 0.3) + (Sesión 1 * 0.2) + (Sesión 2 * 0.2)
- Día 2 = (Talleres * 0.4) + (Sesión 3 * 0.3) + (Sesión 4 * 0.3)
- Día 3 = (Talleres * 0.6) + (Sesión 5 * 0.4)
- Día 4 = (Talleres * 0.6) + (Sesión 6 * 0.4)

La evaluación final considera lo siguiente:

- Evaluación Final = Día 1 * 0.25 + Día 2 * 0.25 + Día 3 * 0.25 + Día 4 * 0.25

Para determinar la aprobación del personal en la capacitación su promedio general debe de ser mayor o igual a 14.
El formato de calificación del personal a capacitar se detalla a continuación:

FORMATO DE EVALUACIÓN AL PERSONAL																			
Nro	Nombres y Apellidos	Día 1					Día 2				Día 3			Día 4			Promedio General	Estado	Observaciones
		Concientización	Sesión 1: Introducción	Sesión 2: Controles de Seguridad SGSI	Talleres	Promedio	Sesión 3: Implementación SGSI	Sesión 4: Controles de Seguridad de la Información Parte II	Talleres	Promedio	Sesión 5: Controles de la Cláusula 10: Gestión de Comunicaciones y Operaciones	Talleres	Promedio	Sesión 6: Capacitación en Gestión de Riesgos	Talleres	Promedio			
1																			
2																			
3																			
4																			
5																			
6																			
7																			
8																			
9																			

Anexo A.7

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

ZONA REGISTRAL N°X – SEDE CUSCO

SUPERINTENDENCIA NACIONAL DE LOS REGISTROS PÚBLICOS

PLAN DE IMPLEMENTACIÓN DE CONTROLES PARA LA GESTIÓN DE COMUNICACIONES Y OPERACIONES

Versión 1.1

Datos sobre la presente edición.-

Versión:	Versión 1.1
Fecha de la Versión:	20 de febrero de 2015
Elaborado por:	[Representante del Comité Operativo de Seguridad]
Revisado por:	[Encargado de Seguridad]
Aprobado por:	[Jefe del Servicio]

Firmas de los responsables.-

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Representante del Comité Operativo de Seguridad	Encargado de Seguridad	Jefe del Servicio

Historial y Control de Versiones.-

Revisión del Documento del Plan de Implementación de los controles				
Versión	**Fecha**	**Creado por**	**Descripción de la modificación**	**Páginas Modificadas**
V 1.1	20/02/2015	[Representante del Comité Operativo de Seguridad]	Elaboración Inicial	Todas

Consideraciones de Seguridad.-

La presente documentación es propiedad de la Zona Registral N°X – Sede Cusco – SUNARP y tiene el carácter de uso interno. No podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquier otro. Asimismo tampoco podrá ser objeto de préstamo, o cualquier forma de cesión de uso sin el permiso previo y por escrito de la Zona Registral N°X – Sede Cusco, titular de los derechos de propiedad intelectual. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga accesos a la documentación será perseguida conforme dicte la ley.

Tabla de Contenido.-

1. Objetivo, Alcance y Usuarios.-

El objetivo del presente documento es definir un Plan de Implementación de los controles para la Gestión de Comunicaciones y Operaciones de la Unidad de Tecnologías de la Información de la Zona Registral N° X – Sede Cusco, priorizando los controles que posean un nivel de exposición al riesgo Crítico.

Este documento incluye todos los controles seleccionados anteriormente en el Documento de la Declaración de la Aplicabilidad (SOA) y los diagramas de actividad, diagramas de proceso y formularios desarrollados para cada control.

Los usuarios de este documento son todos los empleados de la Unidad de Tecnologías de la Información de la Zona Registral N° X – Sede Cusco que cumplen una función dentro del proyecto.

2. Documentos de Referencia.-

- Documento sobre el Alcance del Proyecto (Versión 1.1)
- Documento de la Metodología de Gestión de Riesgos (Versión 1.1)
- Documento de la Declaración de la Aplicabilidad (Versión 1.1)
- Diagramas de actividad, diagramas de procesos y formularios elaborados para cada control.

3. Controles a implementar.-

- Según el Documento de la Declaración de la Aplicabilidad (SOA), se seleccionaron 24 de 32 controles para ser implementados, dichos controles pertenecen a la Cláusula de Gestión de Comunicaciones y Operaciones de la NTP ISO-IEC 17799:2007.

- Se deben de implementar todos los controles seleccionados, priorizando los controles cuyas amenazas presenten un nivel de exposición al riesgo Crítico.

- En segundo plano, se implementarán los controles cuyas amenazas tengan un nivel de exposición de riesgo Moderado y Aceptado, y aquellos controles que no cuenten con amenazas detectadas anteriormente en el Análisis de Riesgos pero que estén declarados a ser implementados en el Documento de la Declaración de la Aplicabilidad (SOA).

- Para la implementación se debe de hacer uso de los siguientes documentos elaborados para cada control y objetivo de control:

    1.1.1. Diagramas de Actividad
    1.1.2. Diagramas de Proceso
    1.1.3. Formularios

3.1. Priorización de Controles.-

Según el análisis realizado en el Tratamiento de Riesgos, los controles que cuentan con amenazas y riesgos críticos **(Nivel de Exposición al Riesgo Mayor a 3.333)** son los siguientes:

Controles a priorizar en la implementación 1 de 5				
Activo	**Amenaza**	**Nivel de Exposición al Riesgo**	**Nivel de Tolerancia**	**Control propuesto para reducir riesgo**
Cintas de Backup DLT	Robo de cintas	4	Crítico	10.8.3 Medios físicos en tránsito
Registro de imágenes digitales	Sustracción de información	3.777	Crítico	10.10.1 Registro de la auditoría
				10.10.2 Monitoreando el uso del sistema
	Modificación no autorizada de la información	3.777	Crítico	10.1.3 Segregación de tareas
Registros de base de datos	Sustracción de información	3.722	Crítico	10.10.1 Registro de la auditoría
				10.10.2 Monitoreando el uso del sistema
	Modificación no autorizada de la información	3.722	Crítico	10.1.3 Segregación de Tareas
				10.10.4 Registro de administradores y operadores

Controles a priorizar en la implementación 2 de 5				
Activo	**Amenaza**	**Nivel de Exposición al Riesgo**	**Nivel de Tolerancia**	**Control propuesto para reducir riesgo**
Cintas de Backup DLT	Daño físico de cintas	3.722	Crítico	10.1.1 Documentación de procesos operativos
				10.5.1 Recuperación de la información
Copias de partidas y títulos registrales	Robo de información	3.556	Crítico	10.1.1 Procedimientos y responsabilidades de operación
Registro de imágenes digitales	Divulgación no autorizada	3.555	Crítico	10.10.1 Registro de la auditoría
				10.10.2 Monitoreando el uso del sistema
Registro de Base de Datos	Divulgación no autorizada	3.5	Crítico	10.10.1 Registro de la auditoría
				10.10.2 Monitoreando el uso del sistema

Controles a priorizar en la implementación 3 de 5				
Activo	**Amenaza**	**Nivel de Exposición al Riesgo**	**Nivel de Tolerancia**	**Control propuesto para reducir riesgo**
SQL Plus	Modificación no autorizada de la información	3.5	Crítico	10.1.3 Segregación de tareas
				10.10.3 Protección de la Información de registro
				10.10.4 Registro de administradores y operadores
Documentos de control de acceso	Divulgación no autorizada	3.445	Crítico	10.7.3 Procedimientos de manipulación de la información
				10.7.4 Seguridad de la documentación de sistemas
Copias de partidas y títulos registrales	Divulgación no autorizada, venta de información	3.445	Crítico	10.7.3 Procedimientos de manipulación de la información

Controles a priorizar en la implementación 4 de 5				
Activo	**Amenaza**	**Nivel de Exposición al Riesgo**	**Nivel de Tolerancia**	**Control propuesto para reducir riesgo**
Computadora	Daño físico de equipo	3.444	Crítico	10.10.1 Documentación de procesos operativos
				10.8.3 Medios físicos en tránsito
	Incoherencia de tiempo con la información registrada	3.444	Crítico	10.10.6 Sincronización del reloj
Servidor de Dominio Zonal	Incoherencia de tiempo con la información registrada	3.444	Crítico	10.10.6 Sincronización del reloj
	Daño físico de equipo	3.389	Crítico	10.10.1 Documentación de procesos operativos
				10.5.1 Recuperación de la información

Controles a priorizar en la implementación 5 de 5				
Activo	**Amenaza**	**Nivel de Exposición al Riesgo**	**Nivel de Tolerancia**	**Control propuesto para reducir riesgo**
Servidor de Keyfile	Incoherencia de tiempo con la información registrada	3.444	Crítico	10.10.6 Sincronización del reloj
	Daño físico de equipos	3.389	Crítico	10.10.1 Documentación de procesos operativos
				10.5.1 Recuperación de la información
Servidor de Base de Datos	Incoherencia de tiempo con la información registrada	3.444	Crítico	10.10.6 Sincronización del reloj
	Daño físico de equipo	3.389	Crítico	10.10.1 Documentación de procesos operativos
				10.5.1 Recuperación de la información
Servidor de Replicación	Incoherencia de tiempo con la información registrada	3.444	Crítico	10.10.6 Sincronización del reloj

4. Cronograma de Implementación.-

De acuerdo al análisis realizado en el inciso anterior, se tomarán en cuenta los controles con nivel de exposición al riesgo Crítico para ser implementados al inicio.

A continuación se detalla el Cronograma de la primera Implementación propuesto:

Cronograma de implementación de los controles de la cláusula Gestión de Comunicaciones y Operaciones de la NTP ISO-IEC 17799:2007 (Controles con nivel de exposición al riesgo Crítico) **1 de 3**

Orden	Control a implementar	Estado a implementar	Semana	Documentación a utilizar	Encargado(s) de la implementación	Encargado de la aprobación
1	10.8.3 Medios físicos en tránsito	Crítico	Semana 1 Semana 2	✓ D. Actividades N°17 ✓ D. Procesos N°17 ✓ Formulario N°17	o Técnico de Sistemas o Central de Atenciones (Comité Formulador)	Jefe de la UTI (Comité Evaluador)
2	10.10.1 Registro de la auditoría	Crítico	Semana 1 Semana 2	✓ D. Actividades N°19 ✓ D. Procesos N°19 ✓ Formulario N°19	o Operador (Comité Formulador)	Jefe de la UTI (Comité Evaluador)
3	10.10.2 Monitoreando el uso del sistema	Crítico	Semana 3 Semana 4	✓ D. Actividades N°20 ✓ D. Procesos N°20 ✓ Formulario N°20	o Técnico de Sistemas (Comité Formulador)	Jefe de la UTI (Comité Evaluador)

Cronograma de implementación de los controles de la cláusula Gestión de Comunicaciones y Operaciones de la NTP ISO-IEC 17799:2007 (Controles con nivel de exposición al riesgo Crítico) 2 de 3						
Orden	**Control a implementar**	**Estado a implementar**	**Semana**	**Documentación a utilizar**	**Encargado(s) de la implementación**	**Encargado de la aprobación**
4	10.1.3 Segregación de tareas	Crítico	Semana 5	✓ D. Actividades N°3 ✓ D. Procesos N°3 ✓ Formulario N°3	o Operador o Especialista en Base de Datos o Técnico de Sistemas (Comité Formulador)	Jefe de la UTI (Comité Evaluador)
5	10.10.4 Registro de administradores y operadores	Crítico	Semana 6 Semana 7	✓ D. Actividades N°22 ✓ D. Procesos N°22 ✓ Formulario N°22	o Operador o Especialista en Base de Datos (Comité Formulador)	Jefe de la UTI (Comité Evaluador)
6	10.1.1 Documentación de procesos operativos	Crítico	Semana 6 Semana 7	✓ D. Actividades N°1 ✓ D. Procesos N°1 ✓ Formulario N°1	o Técnico de Sistemas (Comité Formulador)	Jefe de la UTI (Comité Evaluador)
7	10.5.1 Recuperación de la información	Crítico	Semana 8 Semana 9	✓ D. Actividades N°9 ✓ D. Procesos N°9 ✓ Formulario N°9	o Operador o Especialista en Base de Datos o Central de Atenciones (Comité Formulador)	Jefe de la UTI (Comité Evaluador)

Cronograma de implementación de los controles de la cláusula Gestión de Comunicaciones y Operaciones de la NTP ISO-IEC 17799:2007 (Controles con nivel de exposición al riesgo Crítico) 3 de 3						
Orden	**Control a implementar**	**Estado a implementar**	**Semana**	**Documentación a utilizar**	**Encargado(s) de la implementación**	**Encargado de la aprobación**
8	10.10.3 Protección de la información de registro	Crítico	Semana 10 Semana 11	✓ D. Actividades N°21 ✓ D. Procesos N°21 ✓ Formulario N°21	o Operador (Comité Formulador)	Jefe de la UTI (Comité Evaluador)
9	10.7.3 Procedimientos de manipulación de la información	Crítico	Semana 12	✓ D. Actividades N°14 ✓ D. Procesos N°14 ✓ Formulario N°14	o Operador (Comité Formulador)	Jefe de la UTI (Comité Evaluador)
10	10.7.4 Seguridad de la documentación de sistemas	Crítico	Semana 8	✓ D. Actividades N°15 ✓ D. Procesos N°15 ✓ Formulario N°15	o Técnico de Sistemas (Comité Formulador)	Jefe de la UTI (Comité Evaluador)
11	10.10.6 Sincronización del reloj	Crítico	Semana 13 Semana 14	✓ D. Actividades N°24 ✓ D. Procesos N°24 ✓ Formulario N°24	o Operador o Especialista en Base de Datos o Técnico de Sistemas (Comité Formulador)	Jefe de la UTI (Comité Evaluador)

Una vez culminada la primera implementación, se sugiere continuar con la implementación de los controles con nivel de riesgo **Moderado** y **Aceptado**, y con los controles que no cuenten con amenazas detectadas anteriormente en el Análisis de Riesgos pero que estén declarados a ser implementados en el Documento de la Declaración de la Aplicabilidad (SOA).

A continuación se detalla el Cronograma propuesto para ésta Implementación:

Cronograma de implementación de los controles de la cláusula Gestión de Comunicaciones y Operaciones de la NTP ISO-IEC 17799:2007 (Controles con nivel de exposición al riesgo Moderado y Aceptado) 1 de 3

Orden	Control a implementar	Estado a implementar	Semana	Documentación a utilizar	Encargado(s) de la implementación	Encargado de la aprobación
12	10.1.2 Gestión de Cambios	Moderado	Semana 15	✓ D. Actividades N°2 ✓ D. Procesos N°2 ✓ Formulario N°2	o Técnico de Sistemas (Comité Formulador)	Jefe de la UTI (Comité Evaluador)
13	10.1.4 Separación de los recursos para desarrollo y producción	Moderado	Semana 15 Semana 16 Semana 17	✓ D. Actividades N°4 ✓ D. Procesos N°4 ✓ Formulario N°4	o Operador o Especialista en Base de Datos (Comité Formulador)	Jefe de la UTI (Comité Evaluador)
14	10.3.1 Planificación de la capacidad	Moderado	Semana 16 Semana 17	✓ D. Actividades N°5 ✓ D. Procesos N°5 ✓ Formulario N°5	o Técnico de Sistemas (Comité Formulador)	Jefe de la UTI (Comité Evaluador)

Cronograma de implementación de los controles de la cláusula Gestión de Comunicaciones y Operaciones de la NTP ISO-IEC 17799:2007 (Controles con nivel de exposición al riesgo Moderado y Aceptado) 2 de 3

Orden	Control a implementar	Estado a implementar	Semana	Documentación a utilizar	Encargado(s) de la implementación	Encargado de la aprobación
15	10.3.2 Aceptación del Sistema	Moderado	Semana 18 Semana 19	✓ D. Actividades N°6 ✓ D. Procesos N°6 ✓ Formulario N°6	o Técnico de Sistemas (Comité Formulador)	Jefe de la UTI (Comité Evaluador)
16	10.4.1 Medidas y controles contra software malicioso	Moderado	Semana 20 Semana 21 Semana 22	✓ D. Actividades N°7 ✓ D. Procesos N°7 ✓ Formulario N°7	o Operador o Técnico de Sistemas (Comité Formulador)	Jefe de la UTI (Comité Evaluador)
17	10.4.2 Medidas y controles contra código móvil	Moderado	Semana 23 Semana 24	✓ D. Actividades N°8 ✓ D. Procesos N°8 ✓ Formulario N°8	o Operador (Comité Formulador)	Jefe de la UTI (Comité Evaluador)
18	10.6.1 Controles de red	Moderado	Semana 25 Semana 26	✓ D. Actividades N°10 ✓ D. Procesos N°10 ✓ Formulario N°10	o Operador (Comité Formulador)	Jefe de la UTI (Comité Evaluador)
19	10.6.2 Seguridad en los servicios de redes	Moderado	Semana 27 Semana 28	✓ D. Actividades N°11 ✓ D. Procesos N°11 ✓ Formulario N°11	o Operador (Comité Formulador)	Jefe de la UTI (Comité Evaluador)
20	10.7.1 Gestión de medios removibles	Moderado	Semana 23 Semana 24	✓ D. Actividades N°12 ✓ D. Procesos N°12 ✓ Formulario N°12	o Técnico de Sistemas (Comité Formulador)	Jefe de la UTI (Comité Evaluador)

Cronograma de implementación de los controles de la cláusula Gestión de Comunicaciones y Operaciones de la NTP ISO-IEC 17799:2007 (Controles con nivel de exposición al riesgo Moderado y Aceptado) 3 de 3						
Orden	**Control a implementar**	**Estado a implementar**	**Semana**	**Documentación a utilizar**	**Encargado(s) de la implementación**	**Encargado de la aprobación**
21	10.7.2 Eliminación de medios	Moderado	Semana 25 Semana 26	✓ D. Actividades N°13 ✓ D. Procesos N°13 ✓ Formulario N°13	o Técnico de Sistemas (Comité Formulador)	Jefe de la UTI (Comité Evaluador)
22	10.8.1 Políticas y procedimientos para el intercambio de información y software	Moderado	Semana 27 Semana 28 Semana 29	✓ D. Actividades N°16 ✓ D. Procesos N°16 ✓ Formulario N°15	o Técnico de Sistemas (Comité Formulador)	Jefe de la UTI (Comité Evaluador)
23	10.8.5 Sistemas de información de negocios	Moderado	Semana 29 Semana 30	✓ D. Actividades N°18 ✓ D. Procesos N°18 ✓ Formulario N°18	o Operador (Comité Formulador)	Jefe de la UTI (Comité Evaluador)
24	10.10.5 Registro de la avería	Moderado	Semana 31 Semana 32	✓ D. Actividades N°23 ✓ D. Procesos N°23 ✓ Formulario N°23	o Responsable de avería o Central de Atenciones (Comité Formulador)	Jefe de la UTI (Comité Evaluador)

Tiempo estimado de implementación: 32 semanas aproximadamente. (Incluidos ambos cronogramas)

5. Medición de la efectividad de los controles.-

Una vez determinado el cronograma de implementación, se debe de proponer procedimientos para medir la efectividad de los controles, dichos procedimientos permitirán a los gerentes y al personal determinar que tan bien los controles logran los objetivos de control planeados.

Para determinar la efectividad de los controles se debe de realizar lo siguiente:

- Los encargados de la implementación deben de comprobar que se ha aplicado cada control y que funciona correctamente.
- El encargado de la aprobación debe de dar su conformidad al control implementado sólo si éste se ha realizado correctamente.
- Se deben de realizar pruebas directas con cada uno de los controles para comprobar de forma eficaz el nivel de reducción de riesgo logrado. Estas pruebas pueden ser manuales, automatizadas o realizadas por personal externo especializado en dicha labor.
- Debe de existir un seguimiento continuo para: la implementación de cada control, para la ejecución de las pruebas directas y para los resultados.
- Se deben de realizar informes de cumplimiento periódicos y de avance de la implementación de cada uno de los controles.
- Registrar cada incidencia ocurrida durante la implementación de los controles, y realizar estadísticas para encontrar la raíz de la incidencia.
- Por último, se debe de solicitar a cada personal de la UTI que brinde comentarios y opiniones a medida que se implementan los controles, además de coordinar.

Anexo A.8

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

ZONA REGISTRAL N°X – SEDE CUSCO

SUPERINTENDENCIA NACIONAL DE LOS REGISTROS PÚBLICOS

PLAN DE AUDITORÍA

Versión 1.1

Datos sobre la presente edición.-

Versión:	Versión 1.1
Fecha de la Versión:	09 de agosto de 2015
Elaborado por:	[Representante del Comité Operativo de Seguridad]
Revisado por:	[Encargado de Seguridad]
Aprobado por:	[Jefe del Servicio]

Firmas de los responsables.-

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Representante del Comité Operativo de Seguridad	Encargado de Seguridad	Jefe del Servicio

Historial y Control de Versiones.-

Revisión del Documento del Plan de Implementación de los controles				
Versión	**Fecha**	**Creado por**	**Descripción de la modificación**	**Páginas Modificadas**
V 1.1	09/08/2015	[Representante del Comité Operativo de Seguridad]	Elaboración Inicial	Todas

Consideraciones de Seguridad.-

La presente documentación es propiedad de la Zona Registral N° X – Sede Cusco – SUNARP y tiene el carácter de uso interno. No podrá ser objeto de reproducción total o parcial, tratamiento informático ni transmisión de ninguna forma o por cualquier medio, ya sea electrónico, mecánico, por fotocopia, registro o cualquier otro. Asimismo tampoco podrá ser objeto de préstamo, o cualquier forma de cesión de uso sin el permiso previo y por escrito de la Zona Registral N° X – Sede Cusco, titular de los derechos de propiedad intelectual. El incumplimiento de las limitaciones señaladas por cualquier persona que tenga accesos a la documentación será perseguida conforme dicte la ley.

Tabla de Contenido.-

1. Objetivo, Alcance y Usuarios.-

El objetivo del presente documento es definir un Plan de Auditoría para la revisión respectiva de los controles que han sido implementados para la Gestión de Comunicaciones y Operaciones de la Unidad de Tecnologías de la Información de la Zona Registral N° X – Sede Cusco, priorizando la auditoría de los controles que posean un nivel de exposición al riesgo Crítico.

Este documento incluye los formatos a utilizar para la auditoría de todos los controles seleccionados anteriormente en el Documento de la Declaración de la Aplicabilidad (SOA) utilizando en dicha evaluación, los diagramas de actividad, diagramas de proceso y formularios desarrollados para cada uno

Los usuarios de este documento son todos los empleados de la Unidad de Tecnologías de la Información de la Zona Registral N° X – Sede Cusco que cumplen una función auditora e inspectora dentro del proyecto.

2. Documentos de Referencia.-

- Documento sobre el Alcance del Proyecto (Versión 1.1)
- Documento de la Metodología de Gestión de Riesgos (Versión 1.1)
- Documento de la Declaración de la Aplicabilidad (Versión 1.1)
- Documento del Plan de Implementación de los controles (Versión 1.1)
- Diagramas de actividad, diagramas de procesos y formularios elaborados para cada control.

3. Proceso de Auditoría Interna.-

Las auditorías internas se realizan generalmente una vez al año y son planificadas por un personal capacitado para realizarlas. Durante esta revisión se analiza, en base a las evidencias de las auditorías

Éste proceso comprende realizar un **Programa Anual de Auditoría**, **Planes de Auditorías Internas** para cada control y los **Informes de Auditorías** correspondientes una vez finalizado cada evaluación.

Además de ello, se explicará la manera de evaluar a las personas asignadas para realizar las auditorías tomando en cuenta criterios y perfiles propuestos con los que un auditor interno debe de contar.

3.1. Programa Anual de Auditoría.-

El formato de tabla a utilizar para el llenado de los datos del Programa Anual de Auditoría es el siguiente:

Zona Registral N° X Sede Cusco – Unidad de Tecnologías de la Información	**PROGRAMA ANUAL DE AUDITORÍAS**	**Código:** [FRM - AUD - 001]
		Versión: [Versión 1.1]
		Fecha: [dd/mm/aaaa]
		Página **6** de **1**

Norma de Referencia:	NTP - ISO/IEC 17799:2007
Objetivo:	
Alcance:	
Programa para el período:	[Mes] [Año] a [Mes] [Año]

N	**Auditoría**	**Programación ***																							
	Control a auditar	**Enero**				**Febrero**				**Marzo**				**Abril**				**Mayo**				**Junio**			
		1	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
Nº de Auditorías:																									

N	**Auditoría**	**Programación ***																							
	Control a auditar	**Julio**				**Agosto**				**Setiembre**				**Octubre**				**Noviembre**				**Diciembre**			
		1	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
Nº de Auditorías:																									

TOTAL DE AUDITORÍAS DEL PROGRAMA:	

* Consignar con una “X” en el número de semana del mes en que se realizará la auditoría.

3.2. Plan de Auditoría Interna.-

El formato de tabla a utilizar para el llenado de los datos del Plan de Auditoría Interna es el siguiente:

Zona Registral N° X Sede Cusco – Unidad de Tecnologías de la Información	PLAN DE AUDITORÍA INTERNA	**Código:** [FRM - AUD - 002] **Versión:** [Versión 1.1] **Página** **7** de **1**

Auditoría Nº		**Norma de Referencia:**		**Fecha de elaboración del plan:**	[dd/mm/aaaa]

Objetivo:		
Alcance:		

Auditor líder:		
Auditores Internos:		
Expertos Técnicos:		
Observadores:		

Fecha	**Hora**	**Objetivo de Control a auditar**	**Criterios de Auditoría**		**Auditor**	**Auditado**
			Control a auditar	**Documentación**		

Reunión de Apertura				**Reunión de Cierre**			
Fecha:	[dd/mm/aaaa]	**Hora:**	[hh:mm]	**Fecha:**	[dd/mm/aaaa]	**Hora:**	[hh:mm]

3.3. Informes de Auditorías Internas.-

El formato de tabla a utilizar para el llenado de los datos del Informe de Auditoría Interna es el siguiente:

Zona Registral N° X Sede Cusco Unidad de Tecnologías de la Información	**INFORME DE AUDITORÌA INTERNA**	**Código:** [FRM - AUD - 003] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **8** de **1**

1. DATOS DE LA AUDITORÍA INTERNA.-	
Auditoría Nº:	
Norma de Referencia:	
Período de Auditoría:	Del dd/mm/aaaa al dd/mm/aaaa
Lugar de la Auditoría:	
Equipo Auditor:	

2. ALCANCE DE LA AUDITORÍA INTERNA.-

2.1 Exclusiones reportadas.-

3. OBJETIVOS DE LA AUDITORÍA INTERNA.-

- Determinar el grado en el cual el SGSI y los controles implementados de la cláusula Gestión de Comunicaciones y Operaciones cumplen con los requisitos indicados y sugeridos por la norma NTP - ISO/IEC 17799:2007.

4. DEFINICIONES.-

4.1 No Conformidad: Incumplimiento de un requisito de la norma NTP – ISO/IEC 17799:2007, política o documentos (procedimientos, instrucciones, formatos) del SGSI y de los controles implementados, cuya repetición pone en riesgo la efectividad del Sistema de Gestión y/o la calidad del servicio suministrado.

4.2 Observación: Es una falla aislada o esporádica en el contenido o implementación de los documentos del SGSI, o cualquier incumplimiento parcial en un requisito de la norma de referencia que no llega a afectar directamente o de manera crítica al SGSI

4.3 Oportunidad de Mejora.- Acción recomendada, que al ser implementada, implica una mejora en el SGSI.

5. FORTALEZAS Y DEBILIDADES.-

FORTALEZAS	DEBILIDADES
• Fortaleza A • Fortaleza B	• Debilidad A • Debilidad B

6. RESULTADOS DE LA AUDITORÍA INTERNA.-

6.1 No Conformidades:

Se hallaron _____ No Conformidades (NC) durante la auditoría interna. Las No Conformidades se resumen en el siguiente cuadro.-

Área	No Conformidad	Descripción	Responsable	Auditor

6.2 Observaciones y Oportunidades de Mejora:

Las Observaciones (OBS) y Oportunidades de Mejora (OM) identificadas durante la Auditoría Interna se detallan a continuación.-

• Observación A • Observación B	• Oportunidad de Mejora A • Oportunidad de Mejora B

7. CONCLUSIONES DE LA AUDITORÍA INTERNA.-

- Conclusión A
- Conclusión B

4. Registro de Acciones y Eventos.-

El formato de tabla a utilizar para el llenado de los datos en el registro de Acciones y Eventos hallados en la Auditoría Interna es el siguiente:

Zona Registral N° X Sede Cusco sunarp Unidad de Tecnologías de la Información	**REGISTRO DE HALLAZGOS**	**Código:** [FRM - AUD - 004] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **10** de **1**

Registro Nº :		**Norma de Referencia:**	

Hallazgo encontrado:			
I. DESCRIPCIÓN			
Informado por:			
Responsable:		**Fecha:**	[dd/mm/aaaa]
II. ANÀLISIS DE CAUSAS			
Responsable:		**Fecha:**	[dd/mm/aaaa]
III. ACCIONES A TOMAR			
1. Acción Inmediata o Corrección			
2. Acción Preventiva/Correctiva (Plan de Acción)			

Nº	Actividad	Responsable	Tiempo

Responsable:		**Fecha:**	[dd/mm/aaaa]
Fecha de cierre propuesta:			
IV. VERIFICACIÓN			
Conforme [ ]		**No Conforme [ ]**	
Detalles:		**Detalles:**	
Responsable:		**Fecha de cierre real:**	[dd/mm/aaaa]

5. Puesto de Auditor Interno

5.1. Modelo perfil de puesto de Auditor Interno.-

El perfil de Auditor Interno a utilizar para tomar en cuenta al momento de realizar las auditorías internas sugiere ser el siguiente:

Zona Registral N° X Sede Cusco – Unidad de Tecnologías de la Información	**PERFIL DE PUESTO DE AUDITOR INTERNO**

Función General:	• Planear, preparar y realizar las Auditorías Internas			
Funciones Específicas:	1. Planear y preparar la Auditoría. 2. Comunicar y establecer los requisitos de la auditoría. 3. Tomar conocimiento de los resultados de las auditorías anteriores. 4. Dirigir el proceso de auditoría en el período planificado. 5. Recoger evidencias objetivas del área auditada a través de entrevistas, observación de actividades, y revisión de registros con la finalidad de verificar la implementación de los controles y su efectividad. 6. Verificar que la implementación de los controles es conforme con las disposiciones y requisitos planificados en la norma. 7. Verificar que lo implementado se mantiene de manera eficaz. 8. Planear y realizar las actividades y atribuciones de sus responsabilidades efectiva y eficientemente. 9. Informa al área auditada los hallazgos obtenidos durante el proceso. 10. Documentar las observaciones. 11. Redactar las No Conformidades encontradas. 12. Elaborar y presentar el informe de auditoría.			
Requisitos mínimos del puesto:	**Educación, Formación y Experiencia** • Título Profesional Universitario o Grado Académico Bachiller en Administración, Ingeniería o carreras vinculadas a la actividad o especialidad. • Curso de Auditor Interno ISO 27001. • Deseable Formación de Auditor Líder ISO 27001. Registro IRCA. • Experiencia Profesional mínima de 3 años en ejecución de auditorías de sistemas de gestión de seguridad de la información. **Habilidades:**			
	• Comunicación efectiva	X	• Versátil	X
	• Mentalidad abierta	X	• Integridad y comportamiento ético	X
	• Perceptivo	X	• Liderazgo	X
	• Decidido	X	• Observador	X
	• Respeto y trabajo en equipo	X	• Tenaz	X
	• Organización y planificación	X	• Seguro de sí mismo	X
	• Diplomático	X		

5.2. Formato de Evaluación de Auditor Interno.-

El formato de tabla que se sugiere utilizar para realizar la evaluación al auditor interno es el siguiente:

Zona Registral N° X Sede Cusco – Unidad de Tecnologías de la Información	**EVALUACIÓN DEL AUDITOR INTERNO**	**Código:** [FRM - AUD - 005] **Versión:** [Versión 1.1] **Fecha:** [dd/mm/aaaa] **Página** **12** de **1**

Evaluado:		**Fecha:**	[dd/mm/aaaa]
Evaluador:		**Norma de Referencia:**	

Consideraciones Importantes

Evaluar al Auditor Interno asignando una "x" en el valor de calificación de acuerdo a los criterios de evaluación.
Si la evaluación tiene como resultado "Aceptable" o "Insatisfactorio" o "Incumplimiento" se requerirá tomar acciones.

Nº	Criterios de Evaluación	Calificación				
		Muy Satisfactorio	Bastante Satisfactorio	Satisfactorio	Poco Satisfactorio	Nada Satisfactorio
CONOCIMIENTO Y DESEMPEÑO COMO AUDITOR						
1	Conocimiento de la Norma NTP - ISO/IEC 17799:2007.					
2	Conocimiento de la norma ISO/IEC 27007.					
3	Haber completado y aprobado el curso de formación de auditores.					
4	Experiencia como auditor interno					
5	Desempeño satisfactorio en auditoría(s) previa(s).					
6	Haber realizado inducciones y cursos al personal respecto al SGSI.					
7	Haber realizado las auditorías en el período programado.					
CONOCIMIENTO Y DESEMPEÑO GENERAL						
8	Conocimiento de los procesos de la organización.					
9	Conocimiento de los objetivos, alcance y criterios de la auditoría.					
10	Conocimiento de la documentación del SGSI.					
11	Experiencia laboral en la organización (mínimo seis (6) meses)					
12	Desempeño general en la organización					
HABILIDADES DEL AUDITOR						
13	Comunicación efectiva (informa y se informa de los demás)					
14	Mentalidad abierta (dispuesto a considerar ideas alternativas)					
15	Perceptivo (consciente y capaz de entender las situaciones)					
16	Decidido (alcanza conclusiones oportunas basadas en el análisis y razonamientos lógicos)					

17	Respeto y trabajo en equipo (actúa y colabora en el análisis y razonamientos lógicos)					
18	Organización y planificación (organiza y dispone las cosas logrando fluidez en sus actividades)					
19	Diplomático (con tacto en las relaciones con las personas)					
20	Versátil (se adapta fácilmente a diferentes situaciones)					
21	Integridad y comportamiento ético (imparcial, sincero, honesto y discreto)					
22	Liderazgo (capacidad para dirigir un grupo)					
23	Observador (consciente del entorno físico y las actividades)					
24	Tenaz (persistente, orientado hacia logro de los objetivos)					
25	Seguro de sí mismo (actúa en forma independiente)					

RESUMEN		**Criterios de Calificación**	
		Calificativo	**Puntaje**
CONOCIMIENTO Y DESEMPEÑO COMO AUDITOR	0.00	Muy Satisfactorio	>4 - 5
CONOCIMIENTO Y DESEMPEÑO GENERAL	0.00	Bastante Satisfactorio	>3 - 4
HABILIDADES DEL AUDITOR	0.00	Satisfactorio	>2 - 3
RESULTADO*		Poco Satisfactorio	>1 - 2
	0.00	Nada Satisfactorio	<= 1

OBSERVACIONES / ACCIONES A TOMAR