"AÑO DE LA LUCHA CONTRA LA CORRUPCION Y LA IMPUNIDAD"

RESOLUCION JEFATURAL Nº 046 -2019-SUNARP/ZR.IV-JEF

Iquitos, 15 de abril de 2019.

VISTO: El informe Nº 034-2019/ZR. IV-UTI, de fecha 11.04.2019 del Jefe de la Unidad de Tecnología de la Información, y, el proveído de Jefatura Zonal de fecha 12.04.2019 y;

CONSIDERANDO:

Que, conforme lo dispone el art. 4° de la Resolución Ministerial N° 019-2011-PCM que aprueba la Formulación y Evaluación del Plan Operativo Informático de la entidades de la administración Pública y la Guía de Elaboración cada año fiscal en forma permanente las entidades de la Administración Pública deberán registrar en la Página Web del Portal del Estado Peruano (www.peru.gob.pe/poi) el plan Operativo Informático – POI correspondiente. El indicado registro deberá realizarse antes del último día hábil del mes de febrero del año al que haga referencia y la Evaluación del Plan Operativo Informático deberá registrarse antes del último día hábil del mes de enero del año siguiente;

Que, mediante el documento de visto, el Jefe de la Unidad de Tecnologías de la Información de la Zona Registral N° IV-Sede Iquitos, Ing. Juan Adolfo Salazar Pérez, informa a esta Jefatura Zonal que a la fecha el Plan de Contingencia Informático actualmente vigente data del 15 de octubre 2014, aprobado por Resolución Jefatural N° 130-2014-SUNARP-ZRIV-JEF, el mismo que ha venido en obsoleto debido a que los riesgos identificados en el año 2014 han cambiado y tienen otro valor de impacto en la actualidad.

Asimismo, el Jefe de la Unidad de Tecnologías de la Información ha proyectado el Plan de Contingencia Informático 2019 que tiene por finalidad dar cumplimiento a la NTP 27001 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, a la NTP ISO/IEC 17790-2007-EDI Código de Buenas Prácticas para la Gestión de la Seguridad de la Información, sustentando específicamente en las disposiciones contenidas en a Norma de Control de las Entidades del Estado aprobada con Resolución de Contraloría General N° 320-2006-CG de 30.10.2006.

Que, de acuerdo a lo normado en el artículo 62° del Reglamento de Organización y Funciones de la SUNARP, aprobado por Decreto Supremo Nº 012-2013-JUS, la Jefatura Zonal está encargada de la dirección, ejecución, y supervisión de las actividades de la Zona Registral en armonía con la política y lineamientos generales establecidos por la Alta Dirección, y, de acuerdo a lo señalado en el literal t) le corresponde emitir las resoluciones de su competencia consecuentemente la aprobación del Plan Operativo Informático 2019 corresponde a la Jefatura Zonal;

En uso de las atribuciones conferidas por el inciso t) del art. 63 del Reglamento de Organización y Funciones de la Superintendencia Nacional de los Registros Públicos aprobado por Decreto Supremo Nº 012-2013-JUS; y estando a las atribuciones conferidas mediante la Resolución del Gerente General de la Superintendencia Nacional de los Registros Públicos N°062-2019-SUNARP/GG;

SE RESUELVE:

ARTÍCULO PRIMERO: Dejar sin efecto

Dejar sin efecto, la Resolución Jefatural N°130-2014-SUNARP-ZRIV-JEF, así como, cualquier otro Plan de Contingencia Informático aprobado.

ARTÍCULO SEGUNDO: Aprobar plan de Contingencia Informático 2019

Aprobar el plan de contingencia informático 2019, de la Zona Registral N° IV-Sede Iquitos, elaborado por el Jefe de la Unidad de Tecnologías de la Información, cuyo texto a fojas 58, forma parte integrante de la presente resolución.

ARTÍCULO TERCERO: Notificar

Notificar, los alcances y el contenido de la presente Resolución a la Unidad de Tecnología de la Información de la Zona Registral N° V-Sede Iquitos, para su cumplimiento y las acciones de su competencia.

Regístrese y comuníquese y cúmplase;

Teresa de Jesús Yalta Garcia
Jefe Zonal (e)
Zona Registral N° IV - Sede Iquitos

Zona Registral N° IV – Sede Iquitos

Unidad de Tecnologías de la Información

PLAN DE CONTINGENCIAS 2019

IQUITOS

INDICE

INTRODUCCION

La Zona Registral N° IV - Sede Iquitos depende del procesamiento electrónico de datos, por lo tanto es un factor clave asegurar la continuidad con un rápido manejo en el reinicio de su funcionamiento cuando ocurra una contingencia.

Una contingencia es una interrupción no planificada tiene una duración indeterminada, que no puede ser manejada por procedimientos normales.

Consideraremos que el plan de contingencias debe contemplar todos los elementos del sistema de información y las relaciones entre los mismos, así pues se deberá adaptar a los elementos del sistema de información, a las prioridades establecidas para dichos elementos y las medidas correctivas.

El factor crítico es la disponibilidad permanente de la información actualizada, la integridad y confidencialidad de los datos.

Consideramos que la información es el patrimonio principal de la Zona Registral N° IV - Sede Iquitos, y que se deben tener en cuenta dentro de nuestros planes que estamos expuestos a pasar por etapas imprevistas. Por lo tanto, cabe señalar que es necesario contar con un Plan de Contingencias que enmarque una planificación y compromiso de recursos, que nos permita poder llegar a controlar adecuadamente las circunstancias en el momento en que ocurre una contingencia y así rápidamente poder superarla.

Finalmente, consideramos que este Plan debe considerarse como un documento importante no solamente para la Unidad de Tecnologías de la Información, sino para toda la institución, por lo que merece ser adecuadamente comprendida, compartida y apoyada por todos órganos que tienen que ver con su viabilidad.

ALCANCE

El presente plan contempla la infraestructura y todos los procesos institucionales realizados en la Oficinas Registral de Iquitos y comprende:

- El Hardware, Software y Equipos Electrónicos (servidores, estaciones de trabajo, workstations, laptops, kioscos multimedia, librería de backup, impresoras, refrendadoras, módems, router, concentradores, switch, centrales telefónicas, ups, estabilizadores, etc.)
- Equipos eléctricos y mecánicos.
- La red de energía de corriente alterna estabilizada y no estabilizada.
- La red de cableado para transmisión de datos, la telefonía IP y analógica

OBJETIVOS

- Maximizar la capacidad de mantener el nivel de procesamiento de datos a un costo razonable y en un ámbito totalmente aceptable.
- Mantener la continuidad del normal funcionamiento de los sistemas informáticos durante el periodo de tiempo que hay entre la ocurrencia del siniestro y la recuperación total de las facilidades del procesamiento.
- Minimizar los daños y las pérdidas económicas.
- Recuperar las áreas críticas de equipos de cómputo que han sido afectadas por un desastre físico como: fuego, inundaciones, falla de energía, falta de telecomunicación u otros desastres como robo, accidentes, catástrofes, etc.

FINALIDAD

Superar los problemas presentados y retornar al sistema normal de trabajo, con la finalidad de asegurar la continuidad del servicio.

CAPITULO 1. ANALISIS Y EVALUACION DE RIESGOS

1.1 Plan de Reducción de Riesgos (Plan de Seguridad)

N°	Riesgos que pueden ocurrir	Frecuencia	Consecuencias	Fiabilidad de respuestas	¿Que se intenta proteger?	Determinación de la probabilidad del factor de riesgo		Factor de riesgo
01	Incendio		Destrucción de equipos, archivos, e información.	100%	Edificio, equipos, archivos, e información.	1. ¿La oficina cuenta con protección contra incendios?	Sí	Bajo
						2. ¿Se cuenta con sistemas de aspersión automática?	Sí	
						3. ¿Diversos extintores?	Sí	
						4. ¿Detectores de humo?	Sí	
						5. ¿Los empleados están preparados para enfrentar un posible incendio?, ¿Se realizan simulacros de incendio?	Sí	
02	Robo Común		Perdida de equipos y archivos.	95%	Equipos y archivos.	1. ¿En que tipo de vecindario se encuentra la institución? Vecindario con seguridad normal?	Sí	Bajo
						2. ¿Hay venta de drogas?	No	
						3. ¿Las computadoras se ven desde la calle?	No	
						4. ¿Hay personal de seguridad en la institución?	Si	
						5. ¿Cuántos vigilantes hay?	4	
						6. ¿Los vigilantes, están ubicados en zonas estratégicas?	Si	
03	Vandalismo		Destrucción de equipos y archivos.	90%	Equipos y archivos.	1. ¿Se realizan actos de protesta, manifestaciones, etc.?	No	Bajo
						2. ¿Hay probabilidad que cause algún otro tipo de daño intencionado?	No	
04	Fallas en los equipos		Pérdida de datos y continuidad en el servicio.	95%	Equipos e información.	1. ¿Los equipos tienen un mantenimiento continuo por parte de personal calificado?	Sí	Bajo
						2. ¿Es posible predecir las fallas a que están expuestos los equipos?	Sí	
						3. ¿Cuáles son las condiciones actuales del hardware?	Bueno	

N°	Riesgos que pueden ocurrir	Frecuencia	Consecuencias	Fiabilidad de respuestas	¿Que se intenta proteger?	Determinación de la probabilidad del factor de riesgo		Factor de riesgo
05	Equivocaciones y errores		Pérdida y alteración de información	90%	Equipos e integridad de la información	1. ¿Cuánto saben los empleados de computadoras y redes?	Poco	Alto
						2. ¿Los que no conocen del manejo de computadoras ¿Saben a quién pedir ayuda?	Si	
						3. Durante los periodos de vacaciones ¿Qué tipo de personal los sustituye y cuanto saben del manejo de computadoras?	Ninguno	
06	Virus informático		Pérdida y alteración de información.	90%	Integridad de la información.	1. ¿Se prueba software en la oficina sin hacerle un examen previo?	Si	Bajo
						2. ¿Está permitido el uso de USB en la oficina?	No	
						3. ¿Todas las máquinas tienen unidades USB habilitadas?	No	
						4. ¿Se cuentan con procedimientos contra virus?	Si	
						5.		
07	Terremotos		Destrucción de equipos, archivos, e información.	60%	Edificio, equipos, archivos e información.	1. ¿La institución se encuentra en una zona sísmica?	No	Muy Bajo
						2. ¿El edificio cumple con las normas antisísmicas?	Si	
						3. Un terremoto, ¿Cuánto daño podría causar?	Alto	
						4. ¿La institución realiza simulacros de sismos?	Si	
08	Acceso no autorizados		Alteración de información	90%	Integridad de la información	1. ¿Se tiene interconexión con oficinas dependientes?	Si	Bajo
						2. ¿Se cuenta con sistemas de seguridad en el acceso a Internet?	Si	
						3. ¿Cuánto daño podría causar la alteración de datos?	Alto	
09	Robo de datos		Difusión no autorizada	90%	Integridad de la información	1. ¿Cuánto valor tienen actualmente las Bases de datos?	Muy Alto	Bajo
						2. ¿Cuánta pérdida podría causar en caso de que se hicieran públicas?	Bajo	
						3. ¿Se ha elaborado una lista de los posibles sospechosos que pudieran efectuar el robo?	No existen sospechosos	
10	Fraude		Desvío de fondos a merced del sistema informático	90%	Integridad de la información	1. ¿Cuántas personas se ocupan de la contabilidad de la institución?	Uno	Alto
						2. ¿El sistema de contabilidad es confiable?	No	
						3. Las personas que trabajan en el departamento de Contabilidad, ¿tienen antecedentes negativos?	No	
						4. ¿Existe acceso al Sistema contable desde otros Sistemas o Personas?	Si	

1.2 Análisis De Fallas En La Seguridad

N°	Falla en la seguridad de la red Informática	Software o sistema utilizado sin autorización	¿Qué se intenta proteger?	Determinación de la probabilidad del factor de riesgo		Factor de riesgo
01	Utilización de una PC sin autorización y sin clave de acceso	Sistema SIR, RPV, SCUNAC, SPR, de Producción Registral, SARP, otros Sistemas Registrales, Sistemas Administrativos, MS Office.	Integridad de la información en los sistema registrales y administrativos Configuración de la computadora. Archivos personales confidenciales.	1. ¿Se dispone clave de bloqueo para acceso a la PC?	Si	Muy bajo
				2. ¿Se lleva un control y mantenimiento periódico de códigos de usuario y claves de acceso?	Si	
				3. ¿Se programa anticipadamente el cambio de usuarios y/o permisos para el acceso a los sistemas?	Si	
				4. ¿Los usuarios autorizados mantienen reserva de las claves asignadas?	Si	
				5. ¿Se dispone de vigilancia en el uso de los equipos?	Si	
02	Acceso directo a los servidores de red	Sistema SIR, RPV, SCUNAC, SPR, de Producción Registral, SARP, otros Sistemas Registrales, Sistemas Administrativos, Instaladores de software.	Integridad de la información en el sistema registral y administrativo. Configuración de los servidores.	1. ¿Se dispone de una sala acondicionada con acceso restringido para administradores y operadores de los servidores?	Si	Muy bajo
				2. ¿Los usuarios autorizados mantienen reserva de las claves asignadas?	Si	
03	Acceso a los servidores de red desde oficinas externas	Sistema SIR, RPV, SCUNAC, SPR, de Producción Registral, SARP.	Integridad de la información en los sistema registrales	1. ¿Los routers y switchs pueden recibir datos?	Si	Muy bajo
				2. ¿Se dispone llaves de bloqueo para acceso a las computadoras remotas?	Si	
				3. ¿Se lleva un control y mantenimiento periódico de códigos de usuario remotos y claves de acceso?	Si	
				4. ¿Se programa anticipadamente el cambio de usuarios remotos y/o permisos para el acceso a los sistemas?	Si	
				5. ¿Los usuarios autorizados mantienen reserva de las claves asignadas?	Si	
				6. ¿Se dispone de vigilancia en el uso de los equipos?	Si	
04	Acceso a los servidores de red desde Internet	Sistema SIR, RPV, SCUNAC, SPR, de Producción Registral, SARP.	Integridad de la información en los sistemas registrales y administrativos	1. ¿Los servidores de red para los sistemas locales son accesibles desde la red Internet?	Si	Muy bajo
				2. ¿Se dispone servidores de seguridad para acceso no deseados desde Internet?	Si	
				3. ¿La información mostrada en Internet es una copia de la información local?	Si	

1.3 Protecciones Actuales

N°	Riesgos que pueden ocurrir	Protección Actual	Protección por aplicar
01	Incendio	Sistema detector contra incendios en la Unidad de Tecnologías de la Información.	
02	Robo Común	Se cierran puertas y ventanas. Se mantiene vigilancia privada. Se realizan rondas periódicas por todo el edificio.	
03	Vandalismo	Se mantiene vigilancia privada y por parte de la PNP. Por precaución se cierran puertas y ventanas de las fachadas.	
04	Fallas en los equipos	Los equipos se tratan con cuidado, no se permite fumar, se realizan mantenimientos regulares, Directivas y charlas.	
05	Equivocaciones y errores	Los empleados tienen conocimiento regular en el uso de computadoras. Cuando se requieren nuevos trabajadores, se considera su buena formación en el uso de computadoras.	
06	Virus informático .	Se dispone software antivirus en las computadoras Actualización automática del software antivirus. El ingreso de información se realiza previo análisis con software antivirus. Se utilizan software oficial y licenciado. Los programas de uso público y compartido (shareware) se usan si proceden de fuente confiable.	
07	Terremotos	Se realizan simulacros en forma periódica.	
08	Acceso no autorizados	Se cierran la mayoría de las puertas de entrada. El acceso al área de informática es restringido.	
09	Robo de datos	Se cierran la mayoría de las puertas de entrada. El acceso al área de informática es restringido. El acceso a la red es controlado por un servidor de dominio.	
10	Fraude	La información es contrastada permanentemente a través de informes periódicos. El acceso a los sistemas y documentación es restringido. La Oficina de Auditoría Interna, ejecuta revisiones permanentes.	

N°	Riesgos que pueden ocurrir	Protección Actual	Protección por aplicar
11	Todo riesgo	Se realizan copias de respaldo del sistema registral y administrativo, en cinta en forma diaria automáticamente. Se almacena localmente y bajo seguridad externa. Se realizan copias de respaldo completas "full" de las imágenes, de catastro, en forma diaria.	
12	Corte Eventual del suministro eléctrico	Los equipos en la sala de servidores cuentan con soporte de UPS redundante en caso ocurra un corte no previsto en el suministro eléctrico. Todos los equipos computarizados están conectados a una línea estabilizada UPS central y además contamos con un Grupo Electrógeno que alimenta a toda la Oficina El grupo electrógeno se activa automáticamente máximo en un minuto.	

CAPITULO 2. ASPECTOS DE SEGURIDAD DE LA INFORMACION

2.1 Conceptos Generales

a) Privacidad

Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidos o transmitidos a otros.

b) Seguridad

Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.

El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

c) Integridad

Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.

El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

d) Datos

Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de
Cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), etc.

e) Base de Datos

Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan.
También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos (Data Base Management System-DBMS).
Las características que presenta un DBMS son las siguientes:

- Brinda seguridad e integridad a los datos.
- Provee lenguajes de consulta (interactivo).
- Provee una manera de introducir y editar datos en forma interactiva.
- Existe independencia de los datos, es decir, que los detalles de la organización de los datos no necesitan incorporarse a cada programa de aplicación.

f) Acceso

Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.

g) Ataque

Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

h) Ataque activo

Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

i) Ataque pasivo

Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una

Red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.

j) Amenaza

Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

k) Incidente

Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido

l) Golpe (breach)

Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

2.2 Seguridad Integral de la Información

Respaldos de información BACKUPS.

Para asegurar la correcta ejecución de los Sistemas o aplicativos de la Institución. Se cuenta con los siguientes procesos de Backup: RMAN es un proceso del mismo ORACLE que se ejecuta diariamente en el servidor de producción cuyo resultado "Copia de Respaldo" es almacenado en disco duros externo, adicionalmente a ello se realiza las copias de respaldo en cintas atravez de sistema de BACKUPS con librerías Backup con cintas LTO5, con el fin de preservar la continuidad de los servicios de la institución se realiza los siguientes BACKUPS:

Backups del Software Aplicativo, para producir los resultados con los cuales trabaja el usuario final

Backups de los Datos (Bases de Datos, Sistema ADM y Registral y todo archivo necesario para la correcta ejecución del Software Aplicativo de nuestra Institución).

Backups del Hardware. Está pendiente la instalación de un servidor de contingencia activo.

Normas y Procedimientos de Backups.

Se deben mantener copias de respaldo actualizadas de acuerdo a las siguientes normas:

Periodicidad de cada Tipo de Backup. Los Backups son realizados en forma diaria automáticamente todos los días a las 10:15 pm tanto para el sistema Registral como para el sistema administrativo en general.

Para el control de los backup se utilizará el formato anexo incluido en este documento

Correspondencia entre la relación de Sistemas e Informaciones necesarias para la buena marcha de la Institución, y los Backups efectuados.

Almacenamiento de los Backups en condiciones ambientales óptimas, dependiendo del medio magnético empleado y en concordancia con las recomendaciones anexas.

Reemplazo de los Backups, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar (reciclaje o refresco).

Almacenamiento de los Backups en local situado a 3 Km aproximado de la Oficinia Registral (Local Punchana) donde esta almacena en un gabinete con ambiente apropiado para el almacenamiento de cintas previa validación de restauración aleatoria de la Información.

Realizar pruebas periódicas de los Backups (Restore), verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

CAPITULO 3. SEGURIDAD DE LA INFORMACION

La seguridad de la información y por consiguiente de los equipos informáticos, es una cuestión que llega a afectar, incluso, a la vida privada de la persona humana, de ahí que resulte obvio el interés creciente que día a día se evidencia sobre este aspecto de la nueva sociedad informática.

Ladrones, manipuladores, saboteadores, espías, etc. reconocen que el Data Center de una institución es su nervio central, que normalmente tiene información confidencial y que, a menudo, es vulnerable a cualquier ataque.

La seguridad de la información tiene dos aspectos. El primero consiste en negar el acceso a los datos a aquellas personas que no tengan derecho a ellos, a los cuales también se les puede llamar protección de la privacidad, si se trata de datos personales, y mantenimiento de la seguridad en el caso de datos institucionales.

Un segundo aspecto de la protección es garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad de proteger los datos que se les ha confiado.

En general, la protección de los datos requiere ejercer un control sobre la lectura, escritura y empleo de esa información. Para obtener mayor eficiencia en la protección se debe tener siempre presente la protección de los datos, el mantenimiento de la privacidad y la seguridad del secreto.

El secreto se logra cuando no existe acceso a todos los datos sin autorización. La privacidad adecuada puede lograrse cuando los datos que puedan obtenerse no pueden enlazarse a individuos específicos o no pueden utilizarse para imputar hechos acerca de ellos.

Por otro lado, es importante incorporar dispositivos de seguridad durante el diseño del sistema en vez de añadirlas después. Los diseñadores de sistemas deben entender que las medidas de seguridad han llegado a ser criterios de diseño tan importantes como otras posibilidades funcionales, así como el incremento de costos que significa agregar funciones, después de desarrollado un Sistema de Información.

3.1 Acceso no Autorizado

Sin adecuadas medidas de seguridad se puede producir accesos no autorizados a:

- Área de Sistemas.
- Computadoras personales y/o Terminales de la red.
- Información Confidencial.

3.1.1 Control de Acceso al Área de Sistemas

El acceso al Data Center es restringido, para ello se cuenta con un sistema de doble puerta, sala de servidores y equipos de telecomunicación.

3.1.2 Acceso limitado a los Terminales

El acceso a los equipos de cómputo está restringido únicamente al personal asignado al mismo y es controlado por políticas establecidas en el servidor de Directorio Activo (WIN Server 2008).

3.1.3 Control de Acceso a la Información

El personal no informático tiene acceso a los datos únicamente a través de los sistemas debidamente autorizados. El personal informático para los fines de mantenimientos, tiene acceso a la información a solicitud previa del UREG y ADM. El uso de USB y lectores de CD es restringido.

3.2 Destrucción

Sin adecuadas medidas de seguridad las institución pueden estar a merced no sólo de la destrucción de la información sino también de la destrucción de su equipo informático.

3.2.1 Caso de destrucción total

La destrucción del equipo puede darse por una serie de desastres como son: incendios, inundaciones, sismos, o posibles fallas eléctricas, etc.

Para tal caso se tiene planificado la adquisición cuenta con un centro de cómputo alterno el cual nos va a permitir continuar con nuestras actividades hasta que se reparen los daños producidos en la zona central

El centro de cómputo alterno se encuentra ubicado en los locales de la Oficina Registral de Mollendo.

3.3 Modificaciones

Nuestra mejor protección contra la pérdida de datos consiste en hacer copias de seguridad, almacenando copias actualizadas de todos los archivos valiosos en un lugar seguro.

Adicionalmente a proteger sus programas de Aplicación como activos, es a menudo necesario establecer controles rígidos sobre las modificaciones a los programas, para estar seguros de que los cambios no causan daños accidentales o intencionados a los datos o a su uso no autorizado. Para el caso de la Zona Registral IV se han establecido restricciones para el acceso y la modificación de los Sistemas y de la Base de Datos de la institución por lo cual no puede hacer modificaciones a menos que se le otorgue permisos al personal asignado para dicha función por el propietario de la informacion.

Deben ser considerados como medidas de seguridad para proteger los datos en el sistema, las limitaciones en el ámbito de los programas de aplicación, auditorías y pruebas, revisiones de modificaciones, exclusión cuando sea necesario de los programas de aplicación de las áreas de sistemas

Adicionalmente se han tomado en cuenta los siguientes puntos para la protección de los datos

1. Hacer de la copia de seguridad una política, no una opción.
2. Hacer que la copia de seguridad resulte deseable.
3. Facilitar la ejecución de la copia de seguridad (equipos adecuados, disponibilidad, suministros).
4. Hacer la copia de seguridad obligatoria.

5. Asegurarse de que los usuarios cumplen la política de copias de seguridad (Política de Auditoría a las Copias de Seguridad).

CAPITULO 4. MEDIDAS DE SEGURIDAD

4.1 Responsable de la Seguridad

Debe darse mayor importancia a la toma de medidas de seguridad, teniendo siempre presente que es indispensable, no sólo para el buen funcionamiento sino también para el mantenimiento del sistema.

El responsable del servicio de informática realizará comprobaciones puntuales para asegurar que las copias de seguridad se realizan según el plan aprobado

También se debe tener muy en cuenta: Adoctrinar al personal de procesamiento de datos en la importancia de la seguridad y la responsabilidad de cada uno en su mantenimiento

CAPITULO 5. CUADRO DE RESPONSABILIDADES

Nº	Operación crítica	Responsable
01	Coordinación general	Jefe de la Unidad de Tecnologías de la Información
02	Operatividad de la red y su seguridad	Jefe de la Unidad de Tecnologías de la Información
03	Funcionabilidad de los servidores	Jefe de la Unidad de Tecnologías de la Información
04	Funcionabilidad de las estaciones de trabajo	Jefe UTI
05	Sistema Registral	Jefe de la Unidad de Tecnologías de la Información
06	Seguridad de accesos a los sistemas	Jefe de la Unidad de Tecnologías de la Información
07	Generación de Backups y su seguridad	Técnico en Sistemas
08	Sistema Administrativo SINARP	Jefe de la Unidad de Tecnologías de la Información
09	Sistemas Registrales desarrollados por la institución	Técnico en Sistemas
10	Sistemas administrativos desarrollados por la institución	Técnico en Sistemas

11	Sistema de servicios en Internet	Jefe de la Unidad de Tecnologías de la Información
12	Sistema eléctrico	Técnico en Sistemas
13	Logística	Encargado de Abastecimientos

Equipos de evaluación.

Esta será realizada por la OCI de la institución y específicamente en forma permanente por el coordinador general del cuadro anterior, debiendo cumplir con las siguientes funciones, responsabilidades y objetivos:

- Revisar que se cumplan con responsabilidad las Normas y procedimientos con respecto a Backups y seguridad de equipos y data.
- Supervisar la realización periódica de los backup, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.
- Revisar la correlación entre la relación de Sistemas e Informaciones necesarios para el buen manejo y la buena marcha de la Institución y los Backups realizados.
- Informar de todos los cumplimientos e incumplimientos de las Normas, para así tomar las medidas de corrección respectivas.

CAPITULO 6 INTEGRIDAD DE LA INFORMACION

En la Zona Registral Iquitos se coordina la integridad de los datos con la oficina central sede Lima los cuales proporcionan rutinas para la evaluación de la integridad en lo cual se han comenzado a realizar trabajos para que dicha revision se haga en esta misma sede.

6.1 Concurrencia

En un sistema de gestión de base de datos existen problemas conocidos como concurrencia, que se generan cuando existen procesos en los que dos o más usuarios deben accesar y/o actualizar la misma información de una base de datos.

Para solucionar este problema, es necesario aplicar un control de concurrencia que permita mantener tanto la integridad, es decir, exactitud y precisión de los datos, como la coherencia de los mismos, para lo cual deben prevenirse los errores semánticos, que resultan de la interacción de dos o más procesos que operan simultáneamente en una base de datos.

El control de concurrencia es el mecanismo para mantener los datos correctamente en un ambiente, donde existen muchas fuentes de actualización en forma simultánea.

En un sistema de gestión de base de datos centralizado, el mecanismo consiste en **bloquear** la porción de los datos durante la actualización, para prevenir resultados inconsistentes que puedan generarse. Cuando una transacción accede a un registro bloqueado, espera hasta que el bloqueo sea eliminado y el registro esté nuevamente en un estado consistente.

En un sistema de gestión de base de datos distribuido, en el que las actualizaciones pueden provenir de cualquier modo o de copias en diferente orden y pueden producir resultados inconsistentes, a pesar de existir un control de consistencia local, la consistencia se da mediante la sincronización por lo expuesto anteriormente la BD en Oracle cumpla.

La falta de control de concurrencia produce tres clases principales de incongruencias, con estas características, el cual es actualízalo.

6.2 Auditoria de Sistemas

La auditoría informática es una función cuya misión es garantizar la seguridad, eficacia y rentabilidad del Sistema de Información. Esto es de gran importancia y se ve amenazada por factores intrínsecos de alto riesgo ya que, fallas en los sistemas informáticos pueden generar graves daños, materializados en pérdidas de patrimonio y operatividad, distorsiones en el servicio, inconsistencia en la gestión y deterioro de la imagen.

Los objetivos de una auditoría de sistemas son: implementar los controles necesarios en el ámbito global de los sistemas y establecer las especificaciones necesarias para la verificación y adecuación de éstos, de modo tal que se asegure la exactitud, seguridad e integridad de los sistemas y sus resultados.

La realización de una auditoría implica una estimación de:

- La efectividad en términos de costo de los nuevos sistemas propuestos
- La eficiencia de los sistemas
- Las provisiones de respaldo que existen en el lugar
- La seguridad suministrada
- La integridad de la documentación
- La factibilidad de los planes de implantación

En tal sentido es necesario contar con un sistema de auditoria de base de datos.

CAPITULO 7. MEDIDAS A TOMAR DURANTE EL DESASTRE

Actividades Durante el Desastre

Plan de Emergencias.

En este plan se establecen las acciones que se deben realizar cuando se presente un siniestro.

Utilizar el manual Procedimientos de Emergencia

Principalmente nos valemos de los backups de máquinas virtuales de equipos compatibles de los usuarios operadores de los sistemas Registral, lo cual servirá como respuesta inmediata ante algún siniestro y asimismo se cuenta con servidor de contigencia Activa.

Acondicionar un servidor de similares características al servidor de producción o una PC con suficientes recursos para cumplir funciones de servidor principal o de producción.

Equipamiento mínimo en cuanto a estaciones de trabajo para el funcionamiento continuo de los sistemas SIR, RPV, SARP y de Producción Registral.

Nº	Oficina	PC Estación de trabajo	Impresora laser
01	Publicidad Registral	1	1
02	Ventanillas de atención al público	3	1
03	Diario - Digitación	1	0
04	Catastro	2	1
07	Área Registral	6	1
13	Unidad de Tecnologías de la Información	1	0
14	Unidad Registral	1	0
	Subtotales	**15**	**4**

CAPITULO 8. PLAN DE RECUPERACION DE DESASTRES

Plan de Recuperación de Desastres

Actividades Previas al Desastre

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información, que nos aseguren un proceso de recuperación con el menor costo posible a nuestra institución.

Podemos detallar las siguientes actividades generales:

Establecimiento del Plan de Acción. **Sistemas e Información.**

Prioridad	Nombre del sistema Descripción	Lenguaje o software de creación	Gerencia que genera la información	Gerencia que usa la información	Volumen de los archivos de trabajo	Volumen de transacciones que maneja el sistema	Fechas críticas en las que se debe disponer de la información	Importancia estratégica para la institución (muy baja, baja, medio, alta, muy alta)	Equipamiento mínimo para el funcionamiento continuo	Actividades a realizar para reiniciar el sistema
01	BASE DE DATOS ORACLE	Oracle-	UTI		1 TB		Dias laborales	Muy Alto	1 servidor minimo con 2 Tera Byte	1. Se detallan en los manuales de instalacion. proporcionados por SUNARP
	Sistema de Caja Unica Nacional SCUNAC									2.
	Sistema SPR . Sistema de Publicidad Registral									3.

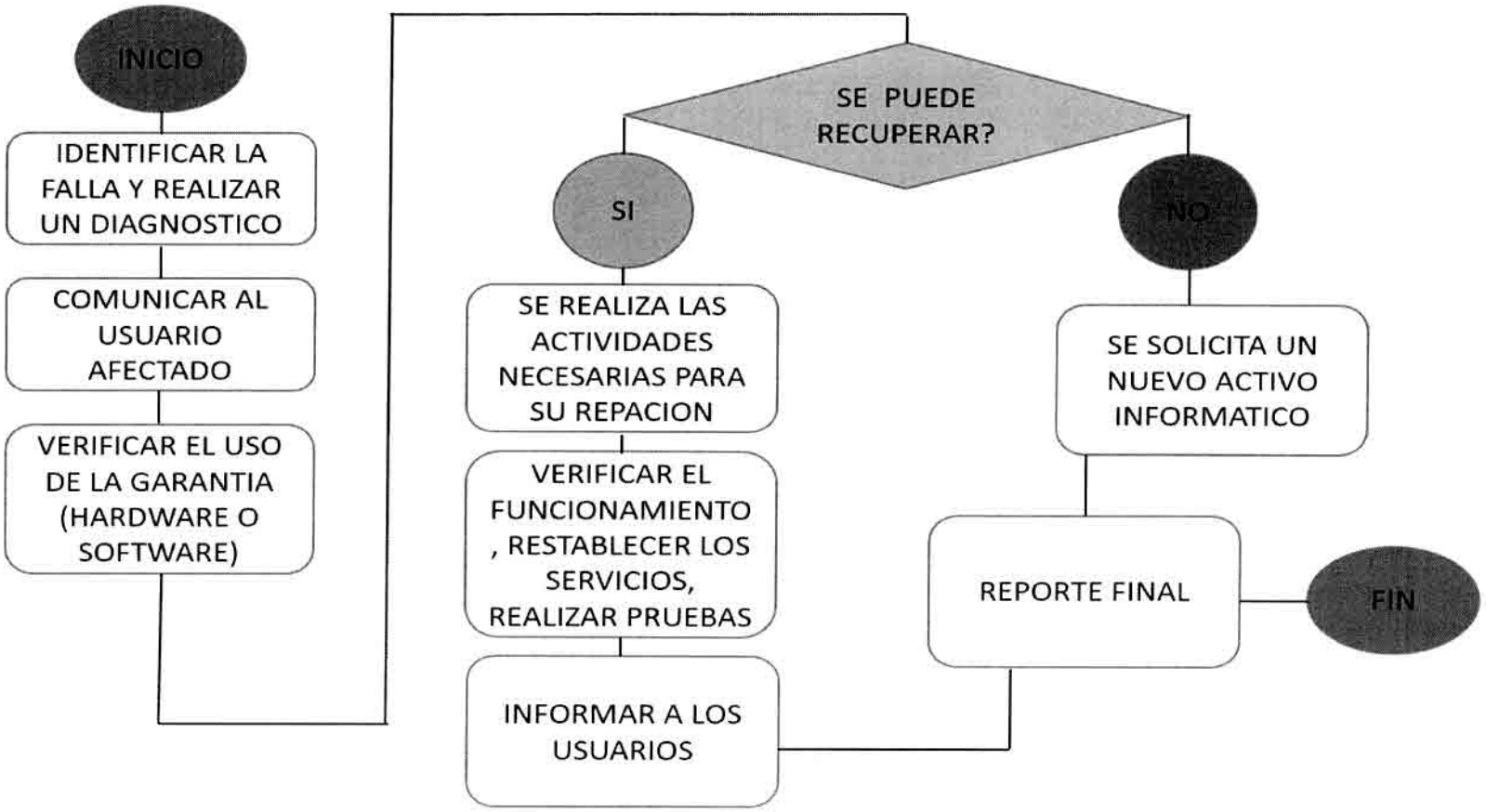
01	Sistema KEYFILE	Keyfile	UTI		80GB		Días laborales	Muy Alto	1 servidor mínimo con 500 GB	4. Se detallan en los manuales de instalacion. proporcionados por SUNARP
02	Sistema de Información Registral (Permite automatizar los procesos de calificación en los Registros de Propiedad Inmueble, Personas Jurídicas, Personas Naturales.	Oracle-Power Builder	GR	GR, Público Usuario	25 GB	100 Mb diario	Días laborales	Muy Alto	30 estaciones de trabajo clientes en Iquitos 11 impresoras láser	5. Se detallan en los manuales de servidores SIR, proporcionados por SUNARP
02	Sistema SIR RPV (registro de Propiedad Vehicular y Registro Mobiliario de Contratos)	Oracle-Developer, Power Builder	UREG	UREG, Público Usuario	70 GB	100 Mb diario	Días laborales	Muy Alto	10 estaciones de trabajo clientes 2 impresoras láser	6. Se detallan en los manuales de instalacion. proporcionados por SUNARP
02	Sistema Automatizado del Registro Predial SARP	Oracle-Developer, Power Builder	UREG	UREG Público Usuario	70 GB	40 Kbytes de incremento diario promedio	Días laborales	Muy Alto	10 estaciones de trabajo clientes 2 impresoras láser	7. Se detallan en los manuales SARP, proporcionados por SUNARP
04	Indice de Verificadores	Oracle-Developer, Power Builder	GR	GR, Público Usuario	-	-	Días laborales	Muy Alto	2 estaciones de trabajo clientes en Iquitos 1 impresoras láser	Se detallan en los manuales de servidores SIV, proporcionados por SUNARP
05	Sistema SIAF	Visual FoxPro	UADM	UADM	12.2 MB		Fin de mes.	Alto	Una estación de trabajo cliente.	En el servidor 1. Restaurar la copia de respaldo en los directorios "apps\adm" del compartido \\iqui01\apps 2. Verificar y actualizar los permisos de acceso de los usuarios. 3. Instalación del acceso directo en la estación cliente y conexión a la unidad de red T: \\iqui01\fpw26.

06	Sistema de Abastecimientos (SUNARP)	Foxpro for Windows 2.6	UADM	UADM	2.57 MB			Medio	Una estación de trabajo cliente.	En el servidor 1. Restaurar la copia de respaldo en los directorios "apps\adm" del compartido \\iqui01\ apps 2. Verificar y actualizar los permisos de acceso de los usuarios. 3. Instalación del acceso directo en la estación cliente y conexión a la unidad de red T: \\iqui01\fpw26.
07	Sistema de Tesorería (SUNARP)	Foxpro for Windows 2.6	UADM	UADM	6.20 MB			Medio	Una estación de trabajo cliente.	En el servidor 1. Restaurar la copia de respaldo en los directorios "apps\adm" del compartido \\iqui01\ apps. 2. Verificar y actualizar los permisos de acceso de los usuarios. 3. Instalación del acceso directo en la estación cliente y conexión a la unidad de red T: \\iqui01\fpw26.
09	Módulo de Caja Chica (SUNARP)	Foxpro for Windows 2.6	UADM	UADM	742 KB			Bajo	Una estación de trabajo cliente.	En el servidor 1. Restaurar la copia de respaldo en los directorios "apps\adm" del compartido \\iqui01\ apps 2. Verificar y actualizar los permisos de acceso de los usuarios. 3. Instalación del acceso directo en la estación cliente y conexión a la unidad de red T: \\iqui01\fpw26.
10	Módulo de Requerimientos (SUNARP)	Foxpro for Windows 2.6	UADM	UADM	159 KB			Medio	Una estación de trabajo cliente.	En el servidor 1. Restaurar la copia de respaldo en los directorios "apps\adm" del compartido \\iqui01\ apps. 2. Verificar y actualizar los permisos de acceso de los usuarios. 3. Instalación del acceso directo en la estación cliente y conexión a la unidad de red T: \\iqui01\fpw26.
11	Registro de Compras (SUNARP)	Foxpro for Windows 2.6	UADM	UADM	893 KB			Medio	Una estación de trabajo cliente.	En el servidor 1. Restaurar la copia de respaldo en los directorios "apps\adm" del compartido \\iqui01\ apps. 2. Verificar y actualizar los permisos de acceso de los usuarios. 3. Instalación del acceso directo en la estación cliente y conexión a la unidad de red T: \\iqui01\fpw26.

12	Sistema de Personal (Datos Generales del trabajador Generación de Planillas Control de faltas permisos, tardanzas y otros).	Foxpro for Windows 2.6	UADM	UADM	13.1 MB	10 MB mensual	Del 01 al 05 y del 19 al 30 de cada mes	alto	Una estación de trabajo cliente.	1. Restaurar la copia de respaldo en los directorios "personal\dbases" del compartido \\iqui01\fpw26. 2. Verificar y actualizar los permisos de acceso de los usuarios. 3. Instalación del cliente y conexión a la unidad de red T: \\iqui01\fpw26.
	Sistema AXIOM	SQL Server 8	UADM							4.
15	Sistema Peruano de Información Jurídica SPIJ	N/C	UREG	GR	413 MB			Bajo	Una estación de trabajo cliente.	En el servidor 1. Reinstalar desde el CD-ROM original en el servidor de produccion. 2. Solicitar la actualización de la clave via teléfono SPIJ. 3. Verificar y actualizar los permisos de acceso de los usuarios. 4. Instalación del acceso directo en la estación cliente.
	Sistema SIGA – MEF Patrimonio	Sql Server 12	UADM							

CAPITULO 9. PROCESO DE RESPUESTA ANTE INCIDENTES

9.1 Diagrama de Flujo



9.2 Actividades o tareas

N° Act	Actividad o Tarea	Descripción	Responsable	Recursos
1	Identificar la falla y realizar un diagnostico	Identificar el tipo de falla	Personal de soporte y/o Jefe de la Unidad	Humano
2	Comunicar a los usuarios afectados	Dar a conocer al usuario de la mejor manera como está la situación (tiempos de solución)	Personal de soporte y/o Jefe de la Unidad	Chat, teléfono, correo
3	Verificar el uso de la garantía	Si esta existe proceder, de lo contrario buscar las piezas con los proveedores	Personal de soporte y/o Jefe de la Unidad	Contrato de garantica
4	¿Se puede recuperar?	Si la respuesta es positiva continuar el paso siguiente, caso contrario ir al reporte.	Personal de soporte y/o Jefe de la Unidad	Humano
5	Realizar la actividad necesaria para su reparación	Se buscan los medios necesarios para poder solucionar el problema	Personal de soporte y/o Jefe de la Unidad	Humano
6	Verificar el funcionamiento	Se verifica que los servicios y las operaciones estén en buen estado.	Personal de soporte y/o Jefe de la Unidad	Humano, equipos pc, servidor de respaldo
7	Informar al usuario	Se informa a los usuarios para que realicen las pruebas necesarias.	Personal de soporte y/o Jefe de la Unidad	Chat, teléfono, correo
8	Reporte	El jefe del área informa de manera formal la situación y la solución de esta.	Jefe de la Unidad	Correo