ANEXO I: ESTRUCTURA ORGANICA DEL CIT

Unidad	Función General
Telecomunicaciones	Mantener y Monitorear los Servicios red.
Soporte Tecnológico	Mantenimiento y Reparación de Computadoras y equipos tecnológicos.
Administración de Servidores	Velar por la integridad y buen funcionamiento de los Servidores.
Desarrollo Tecnológico	Desarrollar e implementar las necesidades de los usuarios en los Sistemas de Información.
Académica	Verificar y garantizar el correcto funcionamiento de los sistemas implementados.

ANEXO II: FORMATO PARA RELACION DE PROVEEDORES DE HARDWARE / SOFTWARE Y/O SERVICIOS

Razón Social	Dirección	Observación	Teléfono
		Hardware/ Software	

ANEXO III: FORMATO PARA EL REGISTRO DE BACKUPS

Anexo de Periodicidad para la Realización de Backup o Copias de Seguridad	**Código:**
	Versión:
	Fecha de actualización:
	Elaborado por:

Sistema de Información	**Tipo de Backup**	**Periodicidad del Backup**	**Medio de Almacenamiento**	**Lugar de Almacenamiento**	**Persona que lo genera**

ANEXO IV: MEDIDAS DE PRECAUCIÓN Y RECOMENDACIÓN [1]

1. En el Área de Servidores:

- Es recomendable que no esté ubicado en áreas de alto tráfico de personas o con un alto número de invitados.
- Evitar, en lo posible, los grandes ventanales por el riesgo de terrorismo y sabotaje; además de que permiten la entrada del sol y calor (inconvenientes para los equipos).
- En su construcción, no debe existir materiales altamente inflamables, que despiden humos sumamente tóxicos o bien paredes que no quedan perfectamente selladas y despidan polvo.
- Su acceso debe estar restringido al personal autorizado. El personal de la Institución deberá tener su carné de identificación siempre en un lugar visible.
- Establecer un medio de control de entrada y salida al *Área de Servidores*.
- Se recomienda que al personal, de preferencia, se les realice exámenes psicológicos y médico, y tener muy en cuenta sus antecedentes de trabajo, ya que el *Área de Servidores* depende en gran medida, de la integridad, estabilidad y lealtad del personal.
- El acceso a los Sistemas de Información, debe estar controlado mediante la verificación de la identidad de los usuarios autorizados.
- Establecer controles para una efectiva disuasión y detección, de intentos de acceso no autorizados a los sistemas de información.
- Se recomienda establecer políticas para la creación de los password y establecer periodicidad de cambios.
- Establecer políticas de autorizaciones de acceso físico al ambiente y de revisiones periódicas de dichas autorizaciones.
- Establecer políticas de control de entrada y salida del personal, en el caso de visitas, verificar los paquetes u objetos que portan.
- La seguridad de las terminales de un sistema en red podrán ser controlados por medio de anulación del disk drive, anulación de Compartir Discos duros, cubriéndose de esa manera la seguridad contra robos de la información y el acceso de virus informáticos.
- La ubicación de los controles de acceso (vigilancia) y el acceso en sí deben estar ubicados de tal manera que no sea fácil el ingreso de una persona extraña.
- Las cámaras fotográficas no se permitirán en el *Área de Servidores*, sin permiso por escrito de la Jefatura.

2. En la Administración de las Impresiones:

- Todo listado que especialmente contenga información confidencial, debe ser destruido, así como el papel carbón de los formatos de impresión especiales.
- Establecer controles de impresión, respetando prioridades de acuerdo a la cola de impresión.
- Establecer controles respecto a los procesos remotos de impresión.

[1] Referencia “Guía Practica para el Desarrollo de Planes de contingencia de Sistemas de Información”. Instituto Nacional de Estadística e Informática (INEI).

3. En los Niveles de Control:

- Existen dos tipos de activos en un Centro de Cómputo (*Área de Servidores*): los equipos físicos y la información contenida en dichos equipos. Estos activos son susceptibles de robo, daño del equipo, revelación y/o destrucción no autorizada de la información, que interrumpen el soporte a los procesos del negocio.
- El valor de los activos a proteger, está determinado por el nivel de clasificación de la información y por el impacto en el negocio, causado por pérdida o destrucción del Equipo o información. Hay que distinguir los activos en nivel clasificado y no clasificado. Para los de nivel no clasificado, no será necesario control. Para el nivel clasificado, deben observarse todas las medidas de seguridad de la información que estos equipos contengan.

4. Recomendaciones para los Medios de Almacenamientos

- **Mantenimiento de Medios Magnéticos:**
  Deben guardarse bajo ciertas condiciones, con la finalidad de garantizar una adecuada conservación de la información almacenada. Medidas a considerar:
  - ⇒ La temperatura y humedad relativa del ambiente de almacenamiento, debe ser adecuada.
  - ⇒ Las cintas deben colocarse en estantes o armarios adecuados.
  - ⇒ Deberá mantenerse alejados de los campos magnéticos.
  - ⇒ Dar un mantenimiento preventivo en forma periódica a fin de desmagnetizar impurezas.

- **Recomendaciones para el Mantenimiento de los Discos Duros**
  - ⇒ Aunque el conjunto de cabezales y discos viene de fábrica sellado herméticamente, debe evitarse que los circuitos electrónicos que se encuentran alrededor se llenen de partículas de polvo y suciedad que pudieran ser causa de errores.
  - ⇒ El ordenador debe colocarse en un lugar donde no pueda ser golpeado.
  - ⇒ Se debe evitar que la computadora se coloque en zonas donde haya acumulación de calor. Esta es una de las causas más frecuentes de las fallas de los discos duros.
  - ⇒ No se debe mover la CPU conteniendo al disco duro cuando esté encendido, porque los cabezales de lectura-escritura pueden dañar al disco.

- **Respecto a los Monitores**
  - ⇒ La forma más fácil y común de reducir la fatiga en la visión que resulta de mirar a una pantalla todo el día, es el uso de medidas contra la refección. Se recomienda no mirar directamente a la pantalla, si no mirar con una inclinación.
  - ⇒ Se recomienda sentarse por lo menos a 60 cm. (2 pies) de la pantalla. No sólo esto reducirá su exposición a las emisiones, sino que puede ayudar a reducir el esfuerzo visual.
  - ⇒ También manténgase por lo menos a 1 m. o 1.20 m. del monitor de su vecino, ya que la mayoría de los monitores producen más emisiones por detrás, que por delante.
  - ⇒ Finalmente apague su monitor cuando no lo esté usando

- **Recomendación para el cuidado del Equipo de Cómputo**
  - ⇒ Teclado: mantener fuera del teclado grapas y clips pues, de insertarse entre las teclas, puede causar un cruce de función.
  - ⇒ Cpu: mantener la parte posterior del cpu liberado en por lo menos 10 cm. Para asegurar así una ventilación mínima adecuada.
  - ⇒ Mouse: poner debajo del mouse una superficie plana y limpia.

- ⇒ Protectores de pantalla: para evitar la radiación de las pantallas que causan irritación a los ojos.
- ⇒ Impresora: el manejo de las impresoras, en su mayoría, es a través de los botones, tanto para avanzar como para retroceder el papel. Por Ejemplo:
  - o Caso Epson FX-11xx/LQ-10xx no usar rodillo cuando esté prendido.
  - o Caso Epson DFX-50xx/80xx tratar con cuidado los sujetadores de papel y no apagar de súbito, asegurarse que el ON LINE esté apagado, así evitaremos problemas de cabezal y sujetador.
  - o Caso de mala impresión, luego de imprimir documentos o cuadros generados, apagar por unos segundos la impresora para que se pierda el set dejado.

- **Mantener las Áreas Operativas Limpias y Pulcra**

  Todas las razones para mantener las áreas operativas limpias y pulcras son numerosas. Sin embargo, algunos de los problemas que podemos evitar son: el peligro de fuego generado por la excesiva acumulación de papeles, el daño potencial al equipo por derramar líquidos en los componentes del sistema, el peligro por fumar y las falsas alarmas creadas por detectores de humo.

ANEXO V: SISTEMAS DE INFORMACION EN LA UNP, CRITICOS PARA LA CONTINUIDAD DEL NEGOCIO.

La relación de los sistemas de información deberá detallar los siguientes datos:

Nombre del sistema	Lenguaje de Programación / Sw Base de datos	Área que genera la información base	Áreas que usan la información	Tamaño promedio del archivo	Volumen de transacciones	Equipamiento necesario	Fechas en que la infor. se necesita urgente
Sistema Integrado de Administración Financiera (SIAF) Uso obligatorio en Instituciones públicas, por el MEF.		La Oficina Central de ejecución Presupuestaria.	OCEP, Oficina de Presupuesto			Conexión a Internet.	Diario
Sistema Integrado de Gestión Académico. Desarrollo CIT		Las Oficinas de Secretarias Académicas, OCRCA.	Las Oficinas Académicas, OCRCA, Autoridades Académicas-Administrativas-Control.		Proceso de Inscripción de cursos y Entrega de Actas.		Diario.
Sistema de Gestión Administrativa - Ingresos Desarrollo CIT		Todas las Unidades Operativas– Area Administrativa	Todas las Unidades Operativas – Of. Adminis., Autoridades Administrativas.		Descarga diario de los archivos del banco.		Diario
Sistema de Trámite Documentario Desarrollo CIT		Todas las Unidades Operativas – Tramite documentario	Todas las Unidades Operativas – Tramite documentario, Autoridades		Registro diario de los documentos.		Diario
Sistema de Abastecimientos. Desarrollo Externo		Oficina de Abastecimientos	Oficina de Abastecimientos		Registro diario de Ordenes de Trabajo.		Diario
Sistema de Control de Asistencia del personal Desarrollo CIT		Oficina de Recursos Humanos-Control de Asistencia	Oficina de Recursos Humanos-Control de Asistencia		Registro diario de las Asistencias de los trabajadores.		Diario
Sistema de Banco de Preguntas. Desarrollo CIT		Comisión de Exámenes de Idepunp	Comisión de Exámenes de Idepunp		Periodo de promedio cada cinco semanas		Exámenes Admisión

ANEXO VI: ESTADOS DE EMERGENCIA

Permiten identificar cuáles pueden ser los eventos que se pueden presentar que afecten el normal funcionamiento de la plataforma y afecte el ingreso de datos y la operación de los Sistemas de Información.

Evento	Descripción	Proceso alterno que debe realizar el usuario del sistema	Proceso alterno que debe realizar el personal de sistemas
Caída De Los Sistemas	Se produce cuando: Ninguna estación de trabajo funciona, el computador no ingresa a las aplicaciones o no hay comunicación con la red. Algunos de los elementos principales que impiden que la red funcione adecuadamente, pueden ser: Servidor, UPS del servidor, concentrador o swiches, puntos de red.	Mientras se restablece el sistema se debe realizar las operaciones de registro de manera manual. Solicitar soporte a la Coordinación Administrativa del CIT - UNP.	Informar del problema a la Coordinación Administrativa, para asignar al personal del soporte. Los mismos que identifican cual de los elementos no están funcionando y se procede a hacer el reemplazo.
Estación de trabajo no funciona	Se produce cuando: No hay energía en el toma, Cables de energía flojos o mal conectados, punto de red deteriorado, patchcord flojo en la conexión de equipo o la caja de punto de red, clave de acceso a la red bloqueada, problemas con el Hardware.	En la toma de energía no hay corriente eléctrica o el cable de energía esta flojo o mal conectado: Los usuarios deben verificar que estos elementos estén bien conectados, o utilizar otra estación de trabajo disponible. Solicitar soporte a la Coordinación Administrativa del CIT - UNP. Si los elementos del equipo están dañados: Solicitar soporte a la Coordinación Administrativa del CIT - UNP.	Verificar cada uno de los elementos que describen el problema y corregir el elemento en conflicto o reemplazarlo. La Coordinación Administrativa del CIT - UNP y de Soporte debe apoyar.
El programa o aplicación transaccional no ingresa al sistema	Se puede producir porque la conexión de red esta deshabilitada, borraron acceso directo o icono al programa, archivos de	Utilizar otra estación de trabajo para realizar sus tareas diarias, sino es posible realizarlas manualmente de acuerdo a las instrucciones dadas en caída de sistemas, reportar a la Coordinación Administrativa del CIT - UNP.	Verificar el caso mencionado y restaurar los elementos que están en conflicto. La Coordinación Administrativa del CIT - UNP y Desarrollo de

	configuración del programa fueron borrados, servidor fuera de servicio		Sistemas debe apoyar.
Pérdida de datos en el programa o aplicación transaccional	Ocurre cuando se pierden datos de registro diario del área operativa que ingresa a las aplicaciones transaccionales para realizar las operaciones.	Mientras se restablece el sistema se debe reportar a la Coordinación Administrativa del CIT – UNP.	Restauración de archivos del backup si se realizo entre las fechas indicadas. Revisar tabla de referencia de realización de backup y las políticas de seguridad de la información.
Errores de realizar: advertencia de los programas o aplicaciones transaccionales	Los mensajes de error de la aplicación expresan alguna anomalía dentro de los procesos normales que se realizan. Cada mensaje de error dentro de la aplicación emite un código con el que se puede identificar la causa, con el código del error que aparece en la pantalla, indica que puede estar pasando, es muy importante reconocer cual es el código del error y el mensaje completo para poder identificar y realizar el proceso de corrección de dicha falla.	Tomar nota del mensaje de error y comunicar a la Coordinación Administrativa del CIT – UNP, para que sea analizado y se establezca una posible solución. Mientras se restablece el sistema se debe realizar lo siguiente de acuerdo a la actividad que necesite realizar:	Se debe reportar al personal de Soporte de la Coordinación Administrativa del CIT – UNP y de Sistemas, sí el error persiste y no permite realizar o continuar con el proceso.

ANEXO VII: CONCEPTOS GENERALES

- **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.

- **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.

- **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.

- **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), vídeo (secuencia de tramas), etc.

- **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.

- **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.

- **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.

- **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.

- **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.

- **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.

- **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

- **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.

ANEXO VIII: PROBABILIDAD DE QUE TENGA EFECTO ALGUNO DE LOS RIESGOS MENCIONADOS

PREGUNTA	RESPUESTA
Fallas eléctricas, que dañen los equipos	
¿La Institución cuenta con grupo electrógeno ?	No
¿Se cuenta con Planos Eléctricos de la distribución del cableado?	No
¿Esta falla cuánto daño puede ocasionar?	10%
El fuego que destruyen los equipos y los archivos	
¿La institución cuenta con protección contra incendios?	No
¿Se cuenta con sistema de aspersión automática?	No
¿Diversos Extintores?	Sí
¿Detectores de Humo?	No
¿Los empleados están preparados para un posible incendio?	No
Robo común, llevándose los equipos	
¿En que tipo de vecindario se encuentra la institución?	poco peligroso
¿Hay venta de drogas?	No
¿Las computadoras se ven desde la calle?	No
¿Hay personal de seguridad en la institución?	Si
¿Cuántos vigilantes hay?	2 por turno
Fallas en los equipos, que dañen los archivos	
¿Los equipos tienen mantenimiento continuo por parte de personal calificado?	Sí, según un plan de mantenimiento
¿Cuáles son las condiciones actuales de Hardware?	Bueno
¿Es posible predecir las fallas a que están expuestos los equipos?	Sí, es posible saberlo
Errores de los usuarios que dañen los archivos	
¿Cuánto saben los empleados de computadoras o redes?	Un nivel medio
Los que no conocen de manejo de computadoras, ¿Saben a quien pedir ayuda?	Si
Durante el tiempo de vacaciones de los empleados, ¿Qué tipo de personal los sustituye y que tanto saben del manejo de computadoras?	Con conocimientos similares
La acción de virus que dañen los archivos	
¿Se prueba software sin hacer un examen previo?	No
¿Esta permitido el uso de dispositvo de almacenamiento en la oficina?	Si
¿Todas las máquinas tienen dispositvo de almacenamiento?	Si
¿Se cuenta con procedimientos contra virus?	Si
Terremotos que destruyan los equipos y archivos	
¿La institución se encuentra en zona sísmica?	No
¿El local cumple con las normas antisísmicas?	Si

Un terremoto, ¿Cuánto daño podría causar?	75%
Accesos no autorizados, filtrando datos importantes	
¿Cuánta competencia hay para la institución?	
¿Qué probabilidad hay que un competidor intente hacer un acceso no autorizado?	
¿El módem se usa para llamar fuera y también se puede utilizar para comunicarse hacia dentro?	
¿Contamos con sistema de seguridad en el servidor?	
¿Contamos con seguridad en internet?	
Robo de Datos: difundiéndose los datos	
¿Cuánto valor tiene actualmente la Base de Datos?	Muy importante
¿Cuánta pérdida podría causar en caso de que se hicieran públicas?	
¿Se ha elaborado una lista de los posibles sospechosos que pudieran efectuar el robo?	
Fraude desviando fondos merced a la computadora.	
¿Cuántas personas se ocupan de la contabilidad de la institución?	
¿El sistema de contabilidad es confiable?	Si
Las personas que trabajan en el departamento de contabilidad ¿Qué tipo de antecedentes laborales tiene?	
¿Existe acceso al Sistema de Contabilidad desde otros sistemas o personas?	No, únicamente los encargados
¿Existen sistemas que manejen cuentas corrientes?	
¿Existen posibles manipulaciones en los archivos de cuentas corrientes?	
¿Existen algún sistema de seguridad para evitar manipulaciones en determinados archivos?	