

**UNIVERSIDAD MAYOR DE SAN ANDRES**

**FACULTAD DE ARQUITECTURA, ARTES, DISEÑO Y  
URBANISMO**

**POLITICAS Y NORMAS DE SEGURIDAD DE LA  
INFORMACION**

**Aprobado según Res. Fac. N° 332/07 de fecha 15 de  
mayo de 2007**

**La Paz -Bolivia**

	Políticas y Normas Desarrolladas	
<b>POLITICA</b>	<b>Política de Seguridad</b>	<b>PS/001</b>
<b>POLITICA</b>	<b>Política de Organización de la Seguridad</b>	<b>PS/002</b>
Norma	Infraestructura de seguridad de la Información	NS/2.001
Norma	Seguridad frente al acceso por parte de terceros	NS/2.002
<b>POLITICA</b>	<b>Política de Clasificación y Control de Activos</b>	<b>PS/003</b>
Norma	Responsabilidad por rendición de cuentas de los Activos	NS/3.001
Norma	Clasificación de la Información	NS/3.002
<b>POLITICA</b>	<b>Política de seguridad del personal</b>	<b>PS/004</b>
Norma	Seguridad en la definición de puestos de trabajo y la asignación de recursos	NS/4.001
Norma	Capacitación al usuario	NS/4.002
Norma	Respuestas a incidentes y anomalías en materia de seguridad	NS/4.003
<b>POLITICA</b>	<b>Política de seguridad física y ambiental</b>	<b>PS/005</b>
Norma	Áreas seguras	NS/5.001
Norma	Seguridad del equipamiento	NS/5.002
Norma	Controles generales (Escritorios y Pantallas limpios)	NS/5.003
<b>POLITICA</b>	<b>Política de gestión de comunicaciones y operaciones</b>	<b>PS/006</b>
Norma	Procedimientos y responsabilidades operativas	NS/6.001
Norma	Planificación y aprobación de sistemas	NS/6.002
Norma	Protección contra software malicioso	NS/6.003
Norma	Mantenimiento	NS/6.004
Norma	Gestión de la red	NS/6.005
Norma	Gestión y seguridad de los medios de almacenamiento	NS/6.006
Norma	Intercambios de información y software	NS/6.007
<b>POLITICA</b>	<b>Política de control de accesos</b>	<b>PS/007</b>
Norma	Requerimientos de negocio para el control de accesos	NS/7.001
Norma	Gestión de accesos de usuarios	NS/7.002
Norma	Responsabilidades del usuario	NS/7.003
Norma	Control de acceso a la red	NS/7.004
Norma	Control de acceso al sistema operativo	NS/7.005
Norma	Control de acceso a las aplicaciones	NS/7.006
Norma	Monitoreo del acceso y uso de los sistemas	NS/7.007
<b>POLITICA</b>	<b>Política de desarrollo y mantenimiento</b>	<b>PS/008</b>
Norma	Requerimiento de seguridad de los sistemas	NS/8.001
Norma	Seguridad en los sistemas de aplicación	NS/8.002
Norma	Controles criptográficos	NS/8.003
Norma	Seguridad de los archivos del sistema	NS/8.004
Norma	Seguridad de los procesos de desarrollo y soporte	NS/8.005
<b>POLITICA</b>	<b>Política de Gestión de Continuidad de los Negocios</b>	<b>PS/009</b>
Norma	Plan de Contingencias	NS/9.001
<b>POLITICA</b>	<b>Cumplimiento</b>	<b>PS/010</b>
Norma	Cumplimiento de los requisitos legales	NS/10.001
Norma	Revisión de la política de seguridad y compatibilidad técnica	NS/10.002
Norma	Consideraciones de auditoría de sistemas	NS/10.003

	<h1 style="text-align: center;">POLÍTICA DE SEGURIDAD</h1> <p style="text-align: center;"><b>Actualización al 27 de febrero de 2007</b></p>	<p style="text-align: center;"><b>Página</b> <b>1 de 3</b></p>
---	---	--

## **1. Propósito y Alcance**

La política de seguridad de la información de la Facultad de Arquitectura, Artes, Diseño y Urbanismo pretende proporcionar a todas las instancias facultativas y de sus carreras la guía y el soporte necesario para poner en ejecución un marco de seguridad adecuado a sus necesidades.

## **2. Definición**

### ***Seguridad de la Información***

La información es un recurso que, como el resto de los importantes activos, tiene valor para la Facultad, y por consiguiente, debe ser debidamente protegida. La seguridad de la información protege a ésta de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información y minimizar el daño que podría ser ocasionado por una amenaza no controlada.

La información en la Facultad puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo, utilizando medios electrónicos, o presentada en imágenes. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

La seguridad de la información se define aquí como la preservación de las siguientes características:

- a) confidencialidad: garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.
- b) Integridad: salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento.
- c) Disponibilidad: garantizar que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera.
- d) No divulgación: debe existir una cláusula en el contrato de contratación de personal que indique claramente que el personal de la Facultad está prohibido de divulgar información hacia el exterior sin el consentimiento del Decano, Vicedecano, Director de Carrera o Director del Centro de Recursos Tecnológicos y Pedagógicos (CRTP).

La seguridad de la información se logra implementando un conjunto adecuado de controles, que abarca políticas, normas, procedimientos, estructuras organizacionales y funciones de la administración de la información.

Desarrollado por:  Fernando Echavarria	Revisión Dirección del CRTP: Max Arnsdorff	Revisión Dirección de Carrera: Roberto Moreira 28 /02/07	Aprobación: Vicedecano Decano	Código:  PS/001
--	--	---	-------------------------------	-----------------------

	<div style="text-align: center;"> <h1>POLÍTICA DE SEGURIDAD</h1> </div>	<div style="text-align: center;"> <b>Página</b>   <b>2 de 3</b> </div>
	<b>Actualización al 27 de febrero de 2007</b>	

### ***El Delito informático, sus formas y consecuencias.***

El desarrollo de las nuevas tecnologías ha originado el nacimiento de una nueva modalidad delictiva.

Se entiende como **delito informático**, a toda acción consciente, voluntaria y premeditada, que provoca un perjuicio para la Facultad y que conlleva o no un beneficio material para el autor, en cuya comisión intervienen indispensablemente y de forma activa dispositivos normalmente utilizados en las actividades informáticas.

Los delitos informáticos más frecuentes y más reportados son los ataques de Hackers que envían troyanos, gusanos, spyware, etc., a través de las redes corporativas e Internet, los ataques que perpetran los empleados al interior de las empresas, la venta no autorizada o robo de bases de datos, el robo de datos críticos (phishing) con fines ilícitos, etc.

### **3. Importancia de la seguridad de la información**

La información y los procesos, sistemas y redes que le brindan apoyo constituyen importantes recursos de la Facultad.

La Facultad, sus redes y sistemas de información, se enfrentan en forma creciente a amenazas relativas a la seguridad de diversos orígenes, inclusive el fraude asistido por computadora, espionaje, sabotaje, vandalismo, incendio o inundación. Daños tales como los ataques mediante virus informáticos, “hacking” y denegación de servicio se han vuelto más comunes, ambiciosos y crecientemente sofisticados.

La dependencia de las instituciones educativas, y de la Facultad, en particular, con respecto de los sistemas y servicios de información, denota que ellas son vulnerables a las amenazas concernientes a seguridad. La interconexión de las redes públicas y privadas y el uso compartido de los recursos de información, incrementan la dificultad de lograr el control de los accesos.

Por todo lo mencionado anteriormente, la Facultad debe protegerse y proteger sus recursos de información, implementando medidas de seguridad por medio de la instalación y actualización permanente de programas antivirus, instalación de barreras de protección a accesos no autorizados, actualizaciones de software de base o aplicaciones desarrollados por el fabricante, custodia de sus activos de información y aplicando buenas prácticas de seguridad.

Desarrollado por:  Fernando Echavarria	Revisión Dirección del CRTP: Max Arnsdorff	Revisión Dirección de Carrera: Roberto Moreira 28 /02/07	Aprobación: Vicedecano Decano	Código:  PS/001
--	--	---	-------------------------------------	-----------------------

	<div style="text-align: center;"> <h1>POLÍTICA DE SEGURIDAD</h1> </div>	<div style="text-align: center;"> <b>Página</b>   <b>3 de 3</b> </div>
	<b>Actualización al 27 de febrero de 2007</b>	

#### **4. Declaración de la Política**

La Política de Seguridad de la Información debe guiar y demostrar la importancia de la seguridad de la información para los procesos de la Facultad. Los documentos que guíen la seguridad de la información deben ser divulgados, mantenidos y adoptados en toda la Facultad.

El Decano y Vicedecano de la Facultad deben aprobar, instruir la publicación y apoyar la Política de Seguridad de la Información de la Facultad.

El Director del CRTP se hará cargo de la evaluación y mejoramiento continuo de la Política de Seguridad de la Información de la Facultad.

La Política de Seguridad, debe amparar a la Facultad contra fraude informático, destrucción fraudulenta de datos electrónicos, modificaciones y destrucción de datos a través de medios de comunicación, destrucción maliciosa o fraudulenta de datos electrónicos por parte de alguna persona, pérdida, daño o hurto de medios de almacenamiento de datos, daño por introducción de virus informáticos, violación a los controles de seguridad en las comunicaciones, accesos no autorizados y otros.


#### **5. Cumplimiento**

Autoridades, docentes, estudiantes, funcionarios administrativos y toda otra persona ligada de alguna manera a la Facultad están obligados a cumplir la política de seguridad de la información. Los mismos deben comunicar inmediatamente cualquier incidente de seguridad al Encargado del Area de Sistemas y, si es necesario, este empleado comunicará el incidente al Director del CRTP.

La gestión de la seguridad de la información, exige, como mínimo, la participación de todos los empleados de la Facultad. También puede requerir la participación de proveedores, clientes y terceros en general. Asimismo, puede requerirse el asesoramiento experto de organizaciones externas. Los controles de seguridad de la información resultan considerablemente más económicos y eficientes si se incorporan en la etapa de especificación de requerimientos y diseño.

El personal debe basarse en esta política y todas las normas de seguridad generadas por la Facultad y regirse estrictamente bajo las mismas.

Desarrollado por:  Fernando Echavarria	Revisión Dirección del CRTP: Max Arnsdorff	Revisión Dirección de Carrera: Roberto Moreira 28 /02/07	Aprobación: Vicedecano Decano	Código:  PS/001
--	--	---	-------------------------------------	-----------------------

	<div> <div> <b>POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD</b> </div> <div> <b>Actualización al 1 de febrero de 2007</b> </div> </div>	<b>Página</b>  <b>1 de 1</b>
---	---	------------------------------------

## **1. Propósito y Alcance**

Esta política establece los lineamientos de la organización de la seguridad y la administración de la seguridad de la información de la Facultad de Arquitectura, Artes, Diseño y Urbanismo.

Esta política se aplica a todos las autoridades, docentes, estudiantes, funcionarios administrativos y personas relacionadas de alguna manera a la Facultad.

## **2. Declaración de la Política**

La organización de la seguridad debe cubrir los ámbitos de accesos físicos y lógicos, a fin de resguardar los activos de información y los recursos de información de acuerdo a los niveles de criticidad y sensibilidad definidos por la Facultad.

La administración y la implementación de la seguridad de la información estarán a cargo del *Comité de Sistemas* y estará bajo la responsabilidad operativa del Encargado de Sistemas del CRTP quien coordinará dicha implementación con todo el personal de la Facultad.

El Encargado de Sistemas del CRTP tendrá la responsabilidad de estar actualizado en materia de seguridad y de tomar contacto con especialistas en el tema para tener información sobre tendencias de la industria, monitoreo de estándares y métodos de evaluación.


Se debe controlar el acceso al Área de Cómputo de la Facultad por parte de terceros, se debe llevar a cabo una evaluación de riesgos para determinar las incidencias en la seguridad y los requerimientos de control necesarios.

## **3. Cumplimiento**

Para asegurar la apropiada protección de la información y los recursos informáticos, la Facultad deberá definir claramente los roles y responsabilidades relacionados con la seguridad de la información para todo el personal.

La seguridad de la información dentro de la Facultad depende de un enfoque multidisciplinario y de la cooperación entre todas las autoridades, docentes, estudiantes, funcionarios administrativos y personas relacionadas a la Facultad, las cuales son responsables por mantener un ambiente seguro. *El Comité de Sistemas* proporcionará las guías necesarias para la creación de un ambiente seguro, estableciendo las normas de seguridad, aprobando los roles y responsabilidades, y proporcionando coordinación consistente entre los diferentes esfuerzos de seguridad que se establezcan en la Facultad.

Desarrollado por:  Fernando Echavarria	Revisión Dirección del CRTP: Max Arnsdorff	Revisión Dirección de Carrera: Roberto Moreira 28/02/07	Aprobación: Vicedecano Decano	Código:  PS/002
--	--	--	-------------------------------------	-----------------------

	<p style="text-align: center;"><b>NORMA DE INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION</b></p> <p style="text-align: center;">Actualización al 21 de enero de 2007</p>	<p>Página 1 de 2</p>
---	---	--------------------------

## **1. Objetivo**

Establecer los aspectos principales para la Administración de la Información dentro de la Facultad.

## **2. Alcance**

La administración de la seguridad de la información proporciona una estructura ejecutiva sólida adecuada para implementar los procesos de control relacionados con la seguridad de la información.

## **3. Responsables**

Es responsable de cumplir esta norma el Encargado de Cómputo, el Auxiliar de Cómputo y el personal involucrado de las áreas usuarias de la Facultad.

## **4. Definición de la Norma**


La administración de la seguridad de la información debe contemplar la asignación de responsabilidades, asignación de funciones y controles de accesos, para conformar la estructura ejecutiva de control.

La administración de la seguridad de la información es una responsabilidad compartida por todos los miembros de la Facultad. Por consiguiente, debe existir un Comité de Sistemas que garantice la existencia de una clara dirección y un apoyo manifiesto de la dirección a las iniciativas de seguridad.

El Comité, en materia de seguridad, debe tener las siguientes funciones:

- a) Promover la seguridad dentro de la Facultad mediante un adecuado compromiso y una apropiada asignación de recursos.
- b) Revisar, aprobar y elevar políticas de seguridad de sistemas, al Decano y Vicedecano para su correspondiente aprobación;
- c) Ejercer las responsabilidades generales en materia de seguridad de la información;
- d) Monitorear cambios significativos en la exposición de los recursos de información frente a las mayores amenazas;
- e) Revisar y monitorear los incidentes relativos a la seguridad, de acuerdo a los cronogramas establecidos en el Plan de Contingencias y los eventos ocurridos;
- f) Aprobar las principales iniciativas para incrementar la seguridad de la información.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/02.001
--	--	---	---	--------------------------

	<p style="text-align: center;"><b>NORMA DE INFRAESTRUCTURA DE SEGURIDAD DE LA INFORMACION</b></p>	<p>Pagina 2 de 2</p>
	<p style="text-align: center;">Actualización al 21 de enero de 2007</p>	

### **Asignación de responsabilidades en materia de seguridad de la información**

Deben definirse claramente las responsabilidades para la protección de cada uno de los recursos y la implementación de procesos específicos de seguridad.

La política de seguridad de la información (*ver PS/001*) suministra una orientación general acerca de la asignación de funciones de seguridad y responsabilidades dentro de la Facultad. En este sentido, la responsabilidad por la seguridad de la información recae en el Encargado del Area de Computación, el cual debe contar con el apoyo y la aprobación del Comité de Sistemas para la realización de sus actividades.

El Comité de Sistemas debe designar responsables a los propietarios de los recursos de la información, estableciendo claramente las áreas sobre las cuales es responsable y detallando las atribuciones y los niveles de autorización debidamente documentados.

### **Asesoramiento especializado en materia de seguridad de la información**

Es probable que en algún caso se requiera asesoramiento especializado en materia de seguridad. En estos casos, el Encargado del Area de Computación, con la aprobación del Comité de Sistemas debe requerir el apoyo de especialistas externos dependiendo del aspecto de seguridad específico del cual se trate.

### **Cooperación entre organizaciones**

Se deben mantener adecuados contactos con autoridades policiales o de seguridad, organismos reguladores, proveedores de servicios de información y operadores de telecomunicaciones, a fin de garantizar que, en caso de producirse un incidente relativo a la seguridad, puedan tomarse las medidas adecuadas y obtener asesoramiento con prontitud.

### **Revisión independiente de la seguridad de la información**

La implementación de la seguridad de la información debe ser revisada independientemente para garantizar que las prácticas de la Facultad reflejan adecuadamente la política de seguridad, y que ésta es viable y eficaz.

Dicha revisión puede ser llevada a cabo por una empresa externa especializada en revisiones de esta índole.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/02.001
--	--	---	---	--------------------------



	<p align="center"><b>NORMA DE SEGURIDAD FRENTE AL ACCESO POR PARTE DE TERCEROS</b></p> <p align="center"><b>Actualización al 28 de febrero de 2007</b></p>	<p align="center">Pagina 1 de 3</p>
---	--	---

## **1. Objetivo**

Establecer los aspectos principales de la seguridad frente al acceso por parte de terceros a los sistemas de información de la Facultad.

## **2. Alcance**

Esta norma incluye al personal del Area de Computación y el Comité de Sistemas de la Facultad.

## **3. Responsables**

Es responsable de cumplir esta norma todo el personal del Área de Computación de la Facultad.

## **4. Definición de la Norma**

La información puede ponerse en riesgo si el acceso de terceros se produce en el marco de una inadecuada gestión de la seguridad. Cuando existe una necesidad de negocios que involucren una conexión con un sitio externo, debe llevarse a cabo una evaluación de riesgos para identificar los requerimientos de controles específicos. Esta evaluación debe tener en cuenta el tipo de acceso requerido, el valor de la información, los controles empleados por la tercera parte y la incidencia de este acceso en la seguridad de la información de la Facultad.

### ***Identificación de riesgos del acceso de terceras partes***

#### **Tipos de acceso**

El tipo de acceso otorgado a terceras partes es de especial importancia. Los riesgos de acceso a través de una conexión de red son diferentes de los riesgos relativos al acceso físico. Los tipos de acceso que se deben tener en cuenta son:

- a) Acceso físico, a oficinas, salas de cómputo, gabinetes de archivos;
- b) Acceso lógico, a las bases de datos y sistemas de información de la Facultad.

#### **Razones para el acceso**

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/02.002
--	--	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE SEGURIDAD FRENTE AL ACCESO POR PARTE DE TERCEROS</h1>	Pagina 2 de 3
		Actualización al 28 de febrero de 2007

Puede otorgarse acceso a terceros por diversas razones. En el caso de terceros que provean servicios a la Facultad y no estén ubicados dentro de la misma, se les puede otorgar acceso físico y lógico, tales como:

- a) Personal de soporte de hardware y software, quienes necesitan acceso a nivel de sistema o a funciones de las aplicaciones;
- b) Socios comerciales o socios con “riesgo compartido” (“joint ventures”), quienes pueden intercambiar información, acceder a sistemas de información o compartir bases de datos.

### Contratistas

Las terceras partes que estén ubicadas en la Facultad por un período de tiempo determinado según contrato, también pueden originar debilidades en materia de seguridad. Entre las terceras partes en estas condiciones, se encuentran:

- a) Personal de mantenimiento y soporte de hardware y software;
- b) Limpieza, guardia de seguridad y otros servicios de soporte tercerizado;
- c) Pasantías de estudiantes y otras designaciones contingentes de corto plazo;
- d) Consultores.

Es esencial determinar qué controles son necesarios para administrar el acceso de terceras partes a las instalaciones de procesamiento de información. En general, todos los requerimientos de seguridad que resulten de los controles internos o del acceso de terceros, deben estar reflejados en los contratos celebrados con los mismos. Si existe una necesidad específica de confidencialidad de la información, pueden implementarse acuerdos de confidencialidad o no-divulgación (ver *Acuerdos de Confidencialidad*, en la *Norma de Seguridad en la definición de puestos de trabajo y la asignación de recursos NS/4.001*).

### Requerimientos de seguridad en contratos con terceros

Las disposiciones que contemplan el acceso de terceros a las instalaciones de procesamiento de información de la Facultad, deben estar basadas en un contrato formal que contenga todos los requerimientos de seguridad, o haga referencia a los mismos, a fin de asegurar el cumplimiento de las políticas y normas de seguridad de la Facultad. El contrato debe garantizar que no surjan malentendidos entre la Facultad y el proveedor. Se deben considerar las siguientes cláusulas para su inclusión en el contrato:


- a) La política de seguridad de la información;
- b) La protección de activos, con la inclusión de:
  - 1) Procedimientos de protección de los activos de la Facultad, incluyendo información y software;

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/02.002
--	--	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE SEGURIDAD FRENTE AL ACCESO POR PARTE DE TERCEROS</h1> <p style="text-align: center;"><b>Actualización al 28 de febrero de 2007</b></p>	<p>Página <b>3 de 3</b></p>
---	---	---------------------------------

- 2) Procedimientos para determinar si se han comprometido los activos de información;
  - 3) Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o en un momento convenido durante la vigencia del mismo;
  - 4) Integridad y disponibilidad;
  - 5) Restricciones a la copia y divulgación de información;
- c) Una descripción de cada servicio del que podrá disponerse;
- d) El nivel de servicio al que se aspira y los niveles de servicio que se consideran inaceptables;
- e) Disposición que contemple la transferencia de personal cuando corresponda;
- f) Las respectivas obligaciones de las partes con relación al acuerdo;
- g) Responsabilidades con respecto a asuntos legales;
- h) Derechos de propiedad intelectual y asignación de derecho de propiedad intelectual;
- i) Acuerdos de control de acceso que contemplen:
- 1) Los métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario (IDs) y contraseñas de usuarios;
  - 2) Un proceso de autorización de acceso y privilegios de usuarios;
  - 3) Un requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios a implementarse y sus derechos y privilegios con respecto a dicho uso;
- j) La definición de criterios de desempeño comprobables, y el monitoreo y presentación de informes respecto de los mismos;
- k) El derecho a monitorear e impedir la actividad del usuario;
- l) El derecho a auditar responsabilidades contractuales o a contratar a un tercero para la realización de dichas auditorías;
- m) El establecimiento de un proceso gradual para la resolución de problemas;
- n) Responsabilidades relativas a la instalación y el mantenimiento de hardware y software;
- o) Una clara estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos;
- p) Un proceso claro y detallado de gestión de cambios;
- q) Los controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos;
- r) Los métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad;
- s) Los controles que garantizan la protección contra software malicioso;
- t) Las disposiciones con respecto a elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad;
- u) La relación entre proveedores y subcontratistas.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/02.002
--	---	---	---	--------------------------

	<h1 style="text-align: center;">POLÍTICA DE GERENCIA DE ACTIVOS</h1> <p style="text-align: center;">Actualización al 27 de febrero de 2007</p>	<p>Página 1 de 2</p>
---	--	--------------------------

## **1. Propósito y Alcance**

La Política de Gerencia (Clasificación y Control) de Activos, define el marco general para la clasificación y control de los activos de información, establece la protección de los mismos y busca garantizar que los recursos de información reciban un apropiado nivel de protección.

Un activo de información se define como cualquier bien tangible o intangible de propiedad o controlado por la Facultad de Arquitectura, Artes, Diseño y Urbanismo; están incluidos los activos lógicos (la propiedad intelectual y datos) y físicos (las computadoras).

Esta política se aplica a autoridades, docentes, estudiantes, funcionarios administrativos y todo otro personal relacionado a la Facultad.

## **2. Declaración de la Política**

Todos los activos de la Facultad deben ser controlados de manera apropiada. Esto se aplica tanto a los activos físicos como lógicos.


Los activos son importantes para el trabajo de la Facultad y por lo tanto deben protegerse mediante controles adecuados que minimicen el riesgo de daño, interrupción de servicio o divulgación de información.

Toda la información de la Facultad, tanto electrónica como impresa, debe ser clasificada según las normas internas de clasificación y control de activos (Ver *Norma de Clasificación de la Información NS/3.001* y la *Norma de Responsabilidad por la Rendición de los Activos NS/3.002*). La clasificación de la información de la Facultad permitirá contar con niveles de criticidad, sensibilidad y protección predefinidos; asimismo, se deberá contar con procedimientos que permitan controlar cada uno de los niveles según la necesidad de protección de la información y los sistemas.

Adicionalmente, deben definirse, en todos los casos, los propietarios de todos los recursos de información de la Facultad, quienes serán los responsables sobre los mismos.

La información debe ser clasificada para señalar la necesidad, la prioridad y el grado de protección. La información tiene diversos grados de sensibilidad y criticidad. Algunos activos pueden requerir un nivel de protección adicional o un tratamiento especial. Se debe utilizar un sistema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de tratamiento especial.

Desarrollado por:  Fernando Echavarria	Revisión Dirección del CRTP: Max Arnsdorff	Revisión Dirección de Carrera: Roberto Moreira 28/02/07	Aprobación: Vicedecano Decano	Código:  PS/003
--	--	--	-------------------------------	-----------------------

	<div data-bbox="435 224 1193 280" data-label="Section-Header"> <h1>POLÍTICA DE GERENCIA DE ACTIVOS</h1> </div> <div data-bbox="571 347 1054 380" data-label="Text"> <p>Actualización al 27 de febrero de 2007</p> </div>	<div data-bbox="1284 190 1364 219" data-label="Text"> <p>Página</p> </div> <div data-bbox="1284 235 1364 268" data-label="Text"> <p>2 de 2</p> </div>
---	--	---

## 3. Cumplimiento

Todo el personal de la Facultad, así como terceros relacionados con la misma, tiene la obligación de cumplir lo determinado por esta política.

Desarrollado por:  Fernando Echavarria	Revisión Dirección del CRTP: Max Arnsdorff	Revisión Dirección de Carrera: Roberto Moreira 28/02/07	Aprobación: Vicedecano Decano	Código:  PS/003
--	--	--	-------------------------------------	-----------------------

	<p align="center"><b>NORMA PARA LA RESPONSABILIDAD POR RENDICION DE CUENTAS DE LOS ACTIVOS INFORMATICOS</b></p> <p align="center"><b>Actualización al 28 de febrero de 2007</b></p>	<p align="center">Pagina 1 de 1</p>
---	---	---

## **1. Objetivo**

Garantizar la adecuada protección de los activos informáticos de la Facultad, a través de la asignación de responsabilidades de rendición de cuentas de activos, controlados por medio del inventario de los activos.

## **2. Alcance**

La responsabilidad de rendición de cuentas de activos informáticos cubre a todos los usuarios responsables de un activo de la Facultad y cubre todos los activos asociados a los Sistemas de Información. Estos activos son: Recursos de Información; Recursos de Software; Recursos Físicos y Recursos de Servicios.

## **3. Responsables**


Se debe asignar la responsabilidad por los activos y por el mantenimiento de los controles apropiados, la implementación de los controles y su protección, a todo el personal responsable de un activo informático de la Facultad.

## **4. Definición de la Norma**

Para alcanzar una adecuada protección de los activos de información de la Facultad, es necesario considerar lo siguiente:

- Se debe realizar un inventario de los activos informáticos asociados a los sistemas de información de la Facultad, para ayudar a garantizar la vigencia de una protección eficiente de los recursos.
- Identificar los activos y su importancia para la Facultad.
- Asignar niveles de protección con relación a la importancia identificada.
- Cada activo debe ser claramente identificado, al igual que su responsable y ubicación.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/03.001
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA PARA LA CLASIFICACIÓN DE LA INFORMACIÓN</h1> <p style="text-align: center;">Actualización al 26 de abril de 2007</p>	<p>Página</p> <p style="text-align: center;">1 de 3</p>
---	--	---

## **1. Objetivo**

Garantizar que los recursos de información de la Facultad, debidamente inventariados, reciban un apropiado nivel de protección, en base a una cuidadosa clasificación e identificación de prioridades, sensibilidad y criticidad.

## **2. Alcance**

En el entendido de que la información es un recurso que como el resto de los activos de la Facultad tienen un valor, debe protegerse y preservarse, a fin de garantizar buenos niveles de confidencialidad y permitiendo que sea accesible sólo por personal autorizado. La clasificación de la información abarca todos los recursos de información inventariados, de acuerdo a la definida para la Responsabilidad por rendición de cuentas de activos. (Ver. NS/3.001)

## **3. Responsables**


La responsabilidad por la definición de la clasificación de un ítem de información, por ejemplo, un documento, registro de datos, archivo de datos o medio magnético, y por la revisión periódica de dicha clasificación, debe ser asignada al creador o propietario del recurso.

## **4. Definición de la Norma**

A base del registro de todos los recursos de información contenidos en el Inventario de Activos, debe realizarse una clasificación de los mismos, señalando claramente la necesidad de distribución dentro de la Facultad, el nivel de restricción y el grado de incidencia de dicha distribución, el grado de sensibilidad, el nivel de criticidad y el rótulo que identifique el grado de confidencialidad.

En este sentido, deben considerarse los siguientes criterios para la clasificación de los recursos de información.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/03.002
--	--	---	---	--------------------------

	<h1 style="text-align: center;">NORMA PARA LA CLASIFICACIÓN DE LA INFORMACIÓN</h1> <p style="text-align: center;">Actualización al 26 de abril de 2007</p>	<p>Página 2 de 3</p>
---	--	--------------------------

## CLASIFICACIÓN DE RECURSOS DE INFORMACIÓN

Clase	Criterio
<b>Confidencial</b>	Es el recurso de información de máxima restricción y que debe ser protegida de accesos no autorizados y que puedan afectar directamente a la Facultad. Es información que requiere una garantía de exactitud y de integridad mayor que la normal. Es la información a la cual tienen acceso sólo algunos funcionarios de la Facultad y cuyo uso debe estar restringido. Su revelación no autorizada podría afectar de manera adversa a la Facultad (p.ej. identificadores, claves de usuario, código fuente de programas de aplicación, documentación de proyectos etc.)
<b>Privada</b>	Se aplica a la información que es importante para los objetivos de la Facultad, que si no estuvieran disponibles, se perderían o fueras destruidos, tendrían consecuencias graves para la Facultad. Información que está destinada para el uso dentro de la Facultad. (p.ej. datos de notas de alumnos, mensajes de correo electrónico, reportes contables, etc.)
<b>Pública</b>	Son los datos que pueden ser accedidos por el público, pueden ser actualizados y/o eliminados sólo por personal autorizado (por ejemplo, las páginas web de la Facultad, información general, etc.)

### ***Rotulado y manejo de la información***

Es importante definir un procedimiento adecuado para el rotulado y manejo de la información, según el esquema de clasificación establecido en la presente norma. Este procedimiento debe incluir los recursos de información en formatos físicos y electrónicos.


Cada recurso de información debe contener el rótulo correspondiente, en función a su distribución y niveles de criticidad, principalmente para aquellos cuya clase sea Confidencial, y Privado.

Para cada clasificación se deben definir procedimientos de manejo de acuerdo al tipo de actividad de procesamiento de la información:

- a) Copia
- b) Almacenamiento
- c) Transmisión por correo, fax, correo electrónico
- d) Transmisión oral, telefonía fija y móvil, correo de voz, contestadores automáticos
- e) Destrucción

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/03.002
--	--	---	---	--------------------------



	<h1 style="text-align: center;">NORMA PARA LA CLASIFICACIÓN DE LA INFORMACIÓN</h1>	Pagina 3 de 3
	<b>Actualización al 26 de abril de 2007</b>	

Las salidas del Sistema Modelo Informacional y del SICOPRE y otros reportes generados de manera alternativa por los usuarios operativos, que contienen información clasificada como, Confidencial o Privada, deben llevar una etiqueta de clasificación apropiada. Estas salidas pueden ser informes impresos, despliegues por pantalla, medios de comunicación grabados (cintas, discos ópticos, etc.), mensajes electrónicos y archivos para transferencia o intercambio de información.

Las etiquetas físicas generalmente son los medios más apropiados de etiquetado, sin embargo, para medios o documentos electrónicos como documentos Word, planillas Excel, se deben adoptar etiquetados electrónicos.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/03.002
--	---	---	---	--------------------------

	<div> <div> <b>POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS</b> </div> <div> Actualización al 27 de febrero de 2007 </div> </div>	Pagina  1 de 2
---	--	----------------------

## **1. Propósito y Alcance**

La política de seguridad de los recursos humanos busca reducir los riesgos de error humano, robo, fraude o uso inadecuado de las instalaciones, garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, minimizar el daño producido por incidentes y anomalías en materia de seguridad y monitorear dichos incidentes.

Esta política se aplica a autoridades, docentes, estudiantes, funcionarios administrativos y a todo personal asociado de alguna manera a la Facultad de Arquitectura, Artes, Diseño y Urbanismo.

## **2. Declaración de la Política**

Las responsabilidades en materia de seguridad deben ser dadas a conocer en la etapa de designación, incluidas en los contratos y monitoreadas durante el desempeño del individuo como empleado de la Facultad.

Los candidatos a ocupar los puestos de trabajo de la Facultad deben ser adecuadamente seleccionados especialmente si se trata de tareas críticas. Todos los empleados y usuarios externos de las instalaciones de procesamiento de información deben firmar un acuerdo de confidencialidad (no divulgación).

Los usuarios de la Facultad deben estar capacitados en las normas y procedimientos de seguridad y el correcto uso de las instalaciones de procesamiento de información, a fin de minimizar eventuales riesgos de seguridad.

Los incidentes que afectan la seguridad de la Facultad deben ser comunicados mediante los canales adecuados tan pronto como sea posible.

Se debe concientizar a todos los empleados y contratistas de la Facultad acerca de los procedimientos de comunicación de los diferentes tipos de incidentes (violaciones, amenazas, debilidades o anomalías en materia de seguridad) que podrían producir un impacto en la seguridad de los activos de la Facultad. Se debe requerir que los mismos comuniquen cualquier incidente advertido o supuesto al punto de contacto designado tan pronto como sea posible. La Facultad debe establecer un proceso disciplinario formal para tratar con los funcionarios que perpetran violaciones de la seguridad. Para ello se aplicará el Reglamento de Procesos Universitarios vigente en la Facultad, específicamente los Artículos 21, 22, 23 y 24. Para lograr abordar debidamente los incidentes podría ser necesario recolectar evidencia tan pronto como sea posible una vez ocurrido el hecho.

Desarrollado por:  Fernando Echavarria	Revisión Dirección del CRTP: Max Arnsdorff	Revisión Dirección de Carrera: Roberto Moreira 28/02/07	Aprobación: Vicedecano Decano	Código:  PS/004
--	--	--	-------------------------------	-----------------------

	<p style="text-align: center;"><b>POLÍTICA DE SEGURIDAD DE LOS RECURSOS HUMANOS</b></p> <p style="text-align: center;">Actualización al 27 de febrero de 2007</p>	<p>Página 2 de 2</p>
---	---	--------------------------

### **3. Cumplimiento**

La presente política debe ser cumplida por todas las autoridades, docentes, estudiantes, funcionarios administrativos y por todo personal asociado de alguna manera a la Facultad de Arquitectura, Artes, Diseño y Urbanismo.

Desarrollado por:  Fernando Echavarria	Revisión Dirección del CRTP: Max Arnsdorff	Revisión Dirección de Carrera: Roberto Moreira 28/02/07	Aprobación: Vicedecano Decano	Código:  PS/004
--	--	--	-------------------------------------	-----------------------

	<h1 style="text-align: center;">NORMA DE RESPUESTA A INCIDENTES</h1>	Pagina 1 de 2
	Actualización al 10 de marzo de 2007	

## **1. Objetivo**

Minimizar el daño producido por posibles incidentes y anomalías en materia de seguridad.

## **2. Alcance**

Esta norma incluye a todo el personal de la Facultad.

## **3. Responsables**

Es responsable de cumplir esta norma todo el personal de la Facultad.

## **4. Definición de la Norma**

### ***Comunicación de incidentes relativos a la seguridad***

Los incidentes relativos a la seguridad deben comunicarse al Encargado de Sistemas del CRTP o al Director del CRTP, tan pronto como sea posible.

Se debe establecer un procedimiento formal de comunicación, junto con un procedimiento de respuesta a incidentes, que establezca la acción a emprender al recibir un informe sobre incidentes. Todos los empleados y contratistas deben estar al corriente del procedimiento de comunicación de incidentes de seguridad, y deben informar de los mismos tan pronto como sea posible.

Se deben implementar adecuados procesos de retroalimentación para garantizar la notificación de los resultados a las personas que comunican los incidentes una vez tratados y resueltos los mismos. Estos incidentes pueden ser utilizados durante la capacitación a fin de crear conciencia de seguridad en el usuario.

### ***Comunicación de debilidades en materia de seguridad***

El Área de Sistemas debe registrar y comunicar las debilidades o amenazas supuestas u observadas en materia de seguridad, con relación a los sistemas o servicios. Deberán comunicar estos asuntos al Encargado de Sistemas del CRTP o a su proveedor de servicios, en caso de ser necesario, tan pronto como sea posible. Se debe informar a los usuarios que ellos no deben, bajo ninguna circunstancia, intentar probar una supuesta debilidad. Esto se

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/04.003
--	---	---	---	--------------------------

	<b>NORMA DE RESPUESTA A INCIDENTES</b>	<b>Página</b>  <b>2 de 2</b>
	<b>Actualización al 10 de marzo de 2007</b>	

lleva a cabo para su propia protección, debido a que el intentar probar debilidades puede ser interpretado como un potencial mal manejo del sistema.

### ***Comunicación de anomalías del software***

Se deben establecer procedimientos para la comunicación de anomalías del software. Se deben considerar las siguientes acciones:

- Deben advertirse y registrarse los síntomas del problema y los mensajes que aparecen en pantalla;
- La computadora debe ser aislada, si es posible, y debe detenerse el uso de la misma. Se debe alertar de inmediato a la persona pertinente. Si el equipo va a ser examinado, este debe ser desconectado de la red de la Facultad antes de ser activado nuevamente. Los disquetes no deben transferirse a otras computadoras;
- El problema debe ser comunicado inmediatamente al Encargado de Sistemas del CRTP.

Los usuarios no deben quitar el software que supuestamente tiene una anomalía, a menos que estén autorizados a hacerlo. La recuperación debe ser realizada por personal adecuadamente capacitado y experimentado.

### ***Aprendiendo de los incidentes***

Deben implementarse mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información debe utilizarse para identificar incidentes y anomalías recurrentes o de alto impacto. Esto puede señalar la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

### ***Proceso disciplinario***

Debe existir un proceso disciplinario formal para los empleados que violen las políticas, normas y procedimientos de seguridad de la Facultad. Dicho proceso puede servir de factor disuasivo de los empleados que, de no mediar el mismo, podrían ser proclives a pasar por alto las normas de seguridad. Asimismo, este proceso debe garantizar un trato imparcial y correcto hacia los empleados sospechosos de haber cometido violaciones graves o persistentes a la seguridad.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/04.003
--	---	---	---	--------------------------

	<b>NORMA PARA LA SEGURIDAD EN PUESTOS DE TRABAJO</b>	<b>Página</b>  <b>1 de 2</b>
	<b>Actualización al 10 de marzo de 2007</b>	

### **1. Objetivo**

Reducir los riesgos de error humano, robo, fraude o uso inadecuado de instalaciones.

### **2. Alcance**

Esta norma incluye al personal del Area de Sistemas de la Facultad.

### **3. Responsables**

Es responsable de cumplir esta norma el personal del Area de Sistemas, Comité de Sistemas Decano, Vicedecano, Director de Carrera y Director del CRTP de la Facultad.

### **4. Definición de la Norma**

La definición de los puestos de trabajo en el Área de Sistemas, debe ser realizada tomando en cuenta los criterios de selección de personal, los acuerdos de confidencialidad y los términos y condiciones de empleo. Dicha definición debe incluir adicionalmente, las responsabilidades específicas por la protección de cada uno de los activos, o por la ejecución de procesos o actividades de seguridad específicos.

#### ***Selección y política de personal***

A tiempo de seleccionar personal para el Área de Sistemas, se deben llevar a cabo los siguientes controles de verificación:

- a) Disponibilidad de certificados laborales con referencias;
- b) Verificación del currículum vitae del aspirante;
- c) Constatación de las aptitudes académicas y profesionales requeridas;
- d) Verificación independiente de la identidad (carnét de identidad o pasaporte).

Cuando un puesto, por asignación inicial o por promoción, involucra a una persona que tiene acceso a las instalaciones de procesamiento de información, y en particular si éstas manejan información sensible, la Facultad debe llevar a cabo una verificación de riesgo. En el caso de personal con posiciones de alta jerarquía, esta verificación debe repetirse periódicamente.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/04.001
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA PARA LA SEGURIDAD EN PUESTOS DE TRABAJO</h1>	Pagina  2 de 2
Actualización al 10 de marzo de 2007		

Un proceso de selección similar debe llevarse a cabo con contratistas y personal eventual. Cuando éste es provisto a través de una agencia, el contrato celebrado con la misma debe especificar claramente sus responsabilidades, por la selección y los procedimientos de notificación que ésta debe seguir si la selección no ha sido efectuada o si los resultados originan dudas o inquietudes.

El Encargado de Sistemas del CRTP debe realizar la supervisión del personal nuevo e inexperto con autorización para acceder a sistemas sensibles. El trabajo de todo el personal del Área de Sistemas debe estar sujeto a revisión periódica y a procedimientos de aprobación por parte del Encargado de Sistemas del CRTP y del Director del CRTP.

### ***Acuerdos de Confidencialidad***

Los acuerdos de confidencialidad o no divulgación se utilizan para comunicar que la información es confidencial o secreta. Los funcionarios deben firmar un acuerdo de esta índole como parte de sus términos y condiciones iniciales de empleo.

El personal ocasional y los terceros (consultores, auditores, contratistas, etc.) deberán firmar el acuerdo mencionado antes de que se les otorgue acceso a las instalaciones de procesamiento de información.

Los acuerdos de confidencialidad deben ser revisados cuando se producen cambios en los términos y condiciones de empleo o del contrato, en particular cuando el funcionario esté próximo a desvincularse de la Facultad o el plazo del contrato esté por finalizar.

### ***Términos y condiciones de empleo***

Los términos y condiciones de empleo deben establecer la responsabilidad del empleado por la seguridad de la información. Cuando corresponda, estas responsabilidades deben continuar por un período definido una vez finalizada la relación laboral. Se deben especificar las acciones que se emprenderán si el empleado hace caso omiso de los requerimientos de seguridad.

Las responsabilidades y derechos legales del empleado deben ser clarificados e incluidos en los términos y condiciones de empleo.

También se debe incluir la responsabilidad por la clasificación y gestión de los datos del empleador. Cuando corresponda, los términos y condiciones de empleo deben establecer que estas responsabilidades se extienden más allá de los límites de las instalaciones de la Facultad y del horario normal de trabajo.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/04.001
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE CAPACITACION DEL USUARIO</h1>	Pagina 1 de 1
	Actualización al 10 de marzo de 2007	

## **1. Objetivo**

Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad.

## **2. Alcance**

Esta norma incluye a todo el personal de la Facultad.

## **3. Responsables**

Es responsable de cumplir esta norma el Encargado de Sistemas del CRTP con la autorización del Comité de Sistemas de la Facultad, desde el punto de vista de proporcionar la capacitación.

Es responsable de asistir a las sesiones de capacitación todo usuario de la Facultad.

## **4. Definición de la Norma**

Todos los empleados de la Facultad y, cuando sea pertinente, los usuarios externos, deben recibir una adecuada capacitación y actualizaciones periódicas en materia de políticas, normas y procedimientos de seguridad.

Dicha capacitación comprende los requerimientos de seguridad, las responsabilidades legales y controles de seguridad de la Facultad, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información antes de que se les otorgue acceso a la información o a los servicios.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/04.002
--	---	---	---	--------------------------



	<div> <div> <b>POLÍTICA DE SEGURIDAD FÍSICA Y AMBIENTAL</b> </div> <div> <b>Actualización al 27 de febrero de 2007</b> </div> </div>	<b>Página</b>  <b>1 de 1</b>
---	--	------------------------------------

## **1. Propósito y Alcance**

Establecer los aspectos que deben ser considerados para prevenir accesos no autorizados, interferencia a las instalaciones de procesamiento y a la información de la Facultad de Arquitectura, Artes, Diseño y Urbanismo, impedir pérdidas, daños o exposiciones al riesgo de robo, hurto o destrucción de los activos de información, y evitar la interrupción de las actividades de la Facultad.

Esta política se aplica a autoridades, docentes, estudiantes, funcionarios administrativos y a todo personal asociado de alguna manera a la Facultad de Arquitectura, Artes, Diseño y Urbanismo.

## **2. Declaración de la Política**

Las instalaciones de procesamiento de información crítica o sensible de la Facultad deben estar ubicadas en áreas protegidas y resguardadas con controles de acceso apropiados. Deben estar físicamente protegidas contra accesos no autorizados, daños e intrusiones.

Las instalaciones de procesamiento de la información y la información de la Facultad deben ser protegidas contra la divulgación, modificación o robo por parte de personas no autorizadas, debiéndose implementar controles para minimizar pérdidas o daños.

La protección provista debe ser proporcional a los riesgos identificados. El equipamiento de la Facultad debe estar físicamente protegido de las amenazas a la seguridad y los peligros del entorno.

Es necesaria la protección del equipamiento de la Facultad para reducir el riesgo de acceso no autorizado a los datos y para prevenir pérdidas o daños. Esto también debe tener en cuenta la ubicación y disposición del equipamiento de la Facultad. Pueden requerirse controles especiales para prevenir peligros o accesos no autorizados, y para proteger instalaciones de soporte, como la infraestructura de cableado y suministro de energía eléctrica.

## **3. Cumplimiento**

La presente política debe ser cumplida por todos los usuarios, empleados, contratistas y terceros relacionados de alguna manera con la Facultad.

<b>Desarrollado por:</b>  Fernando Echavarria	<b>Revisión Dirección del CRTP:</b> Max Arnsdorff	<b>Revisión Dirección de Carrera:</b> Roberto Moreira 28/02/07	<b>Aprobación:</b> Vicedecano Decano	<b>Código:</b>  PS/005
---	---	---	--	------------------------------

	<p align="center"><b>NORMA DE ESCRITORIOS Y PANTALLAS LIMPIOS</b></p> <p align="center"><b>Actualización al 15 de marzo de 2007</b></p>	<p align="center">Pagina <b>1 de 2</b></p>
---	---	--

### **1. Objetivo**

Impedir la exposición al riesgo de robo de la información o del equipamiento removible empleado en el procesamiento de información de la Facultad.

### **2. Alcance**

Esta norma abarca todos los recursos de información inventariados de la Facultad.

### **3. Responsables**

Es responsable de cumplir esta norma todo el personal de la Facultad.

### **4. Definición de la Norma**

La Facultad debe adoptar los aspectos principales de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y también los principales aspectos relacionados con pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante el horario normal de trabajo y fuera del mismo. Estos aspectos deben contemplar las clasificaciones de seguridad de la información (ver *Norma de Clasificación y Control de Activos NS/3.002*), y los riesgos correspondientes.

Se debe tomar en cuenta que la información que se deja sobre los escritorios también está expuesta a sufrir daños o destrozos en caso de producirse un desastre como incendio, inundación o explosión.

Se deben considerar los siguientes controles:

- Cuando corresponda, los documentos en papel y los medios informáticos deben ser almacenados bajo llave en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
- La información clasificada como sensible, confidencial o crítica de la Facultad debe guardarse bajo llave (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.
- Una vez finalizado el horario normal de trabajo o cuando la persona deje su lugar de trabajo, no debe existir sobre los escritorios ningún documento clasificado como sensible, confidencial o crítico.
- Las computadoras personales, terminales e impresoras no deben dejarse encendidas cuando están desatendidas y las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/05.003
--	---	---	---	--------------------------

	<b>NORMA DE ESCRITORIOS Y PANTALLAS LIMPIOS</b>	<b>Página</b>  <b>2 de 2</b>
	<b>Actualización al 15 de marzo de 2007</b>	

- e) Se deben proteger las maquinas de fax no atendidas.
- f) Las fotocopadoras deben estar bloqueadas (o protegidas de alguna manera, del uso no autorizado) fuera del horario normal de trabajo.
- g) La información sensible, confidencial o crítica, una vez impresa, debe ser retirada de la impresora inmediatamente.

### ***Retiro de bienes***

El equipamiento, la información o el software no deben ser retirados de las oficinas de la Facultad sin autorización. Cuando sea necesario y procedente, los equipos deberán ser desconectados ("logged out") y nuevamente conectados ("logged in") cuando se reingresen. Se deben llevar a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la Facultad. El personal debe conocer la posibilidad de realización de dichas comprobaciones.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/05.003
--	---	---	---	--------------------------

	<b>NORMA DE ÁREAS SEGURAS</b>	<b>Pagina</b>  <b>1 de 3</b>
	<b>Actualización al 15 de marzo de 2007</b>	

## **1. Objetivo**

Impedir accesos no autorizados, daños e interferencia a las instalaciones de procesamiento de información de la Facultad.

## **2. Alcance**

Esta norma incluye a todo el personal de la Facultad.

## **3. Responsables**

Es responsable de cumplir esta norma todo el personal de la Facultad.

## **4. Definición de la Norma**

### ***Perímetro de seguridad física***

La protección física puede llevarse a cabo mediante la creación de diversas barreras físicas alrededor de las instalaciones de procesamiento de información de la Facultad. Cada barrera establece un perímetro de seguridad, cada uno de los cuales incrementa la protección total provista.

La Facultad debe utilizar perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información. Un perímetro de seguridad es algo delimitado por una barrera (una pared, una puerta de acceso controlado con llave o tarjeta, o un escritorio u oficina de recepción atendidos por personas). El emplazamiento y la fortaleza de cada barrera dependerán de los resultados de una evaluación de riesgos.

Se deben considerar e implementar los siguientes lineamientos y controles, según corresponda:

- a) El perímetro de seguridad debe estar claramente definido.
- b) El perímetro de las oficinas que contengan instalaciones de procesamiento de información debe ser físicamente sólido. Las paredes externas del área deben ser de construcción sólida y todas las ventanas que comunican con el exterior, si existen, deben ser adecuadamente protegidas contra accesos no autorizados.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/05.001
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE ÁREAS SEGURAS</h1>	<p style="text-align: center;">Pagina 2 de 3</p>
	<b>Actualización al 15 de marzo de 2007</b>	

- c) Debe existir un área de recepción atendida por personal u otros medios de control de acceso físico a las oficinas. El acceso a las distintas áreas y oficinas debe estar restringido exclusivamente a personal autorizado.
- d) Las barreras físicas deben, si es necesario, extenderse desde el piso hasta el techo, a fin de impedir el ingreso no autorizado.

### ***Controles de acceso físico***

Las áreas protegidas deben ser resguardadas por adecuados controles de acceso que garanticen que sólo se permite el acceso de personal autorizado. Deben tenerse en cuenta los siguientes controles:

- a) Los visitantes de áreas protegidas deben ser supervisados o inspeccionados y la fecha y horario de su ingreso y salida deben ser registrados. Sólo se debe permitir el acceso a los mismos con propósitos específicos y autorizados, instruyendo en dicho momento al visitante sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
- b) El acceso a la información sensible, y a las instalaciones de procesamiento de información, debe ser controlado y limitado exclusivamente a las personas autorizadas.

### ***Protección de oficinas, recintos e instalaciones***

Un área protegida puede ser una oficina cerrada con llave.

Para la selección y el diseño de un área protegida debe tenerse en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También deben tomarse en cuenta las disposiciones y normas en materia de salud y seguridad. Asimismo, se deberán considerar las amenazas a la seguridad que representan los edificios y zonas aledañas (filtración de agua desde otras áreas).

Se deben considerar los siguientes controles:

- a) Las instalaciones clave deben ubicarse en lugares a los cuales no pueda acceder el público en general o los estudiantes.
- b) Las áreas que contienen instalaciones de procesamiento de información deben ser discretas y ofrecer un señalamiento mínimo de su propósito, sin signos obvios, exteriores e interiores, que indiquen la presencia de actividades de procesamiento de información.
- c) Las funciones y el equipamiento de soporte (computadoras personales con acceso a la base de datos del servidor) deben estar ubicados adecuadamente dentro del área protegida para evitar solicitudes de acceso, lo cual podría comprometer la información.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/05.001
--	--	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE ÁREAS SEGURAS</h1> <p style="text-align: center;"><b>Actualización al 15 de marzo de 2007</b></p>	<p style="text-align: center;">Pagina <b>3 de 3</b></p>
---	--	---

- d) Las puertas y ventanas deben estar bloqueadas cuando no hay vigilancia y debe considerarse la posibilidad de agregar protección externa a las ventanas, en particular que se encuentren a nivel del suelo.
- e) Si es que es posible, se deben implementar adecuados sistemas de detección de intrusos. Los mismos deben ser instalados según estándares profesionales y probados periódicamente. Estos sistemas comprenderán todas las puertas exteriores y ventanas accesibles.
- f) Los materiales peligrosos o combustibles, en caso de ser utilizados, deben ser almacenados en lugares seguros a una distancia prudencial de las instalaciones de procesamiento de información. El material de escritorio en cantidad (papelería) no debe ser almacenado dentro del Sala de Servidores.
- g) El equipamiento de sistemas de soporte de reposición de información (en caso de existir) y los medios informáticos de resguardo de información (backups) deben estar situados a una distancia prudencial, para evitar daños ocasionados por eventuales desastres en el sitio principal.

### ***Desarrollo de tareas en áreas protegidas***

Para incrementar la seguridad de un área protegida (Sala de Servidores) pueden requerirse controles y lineamientos adicionales. Esto incluye controles para el personal o terceros que trabajan en el área protegida. Se deberán tener en cuenta los siguientes aspectos:

- a) Se debe evitar el trabajo no controlado en las áreas protegidas, tanto por razones de seguridad como para evitar que se lleven a cabo actividades maliciosas.
- b) El personal del servicio de soporte externo debe tener acceso limitado a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso debe ser autorizado y monitoreado.
- c) A menos que se autorice expresamente, no debe permitirse el ingreso de equipos fotográficos, de video, audio u otro tipo de equipamiento que registre información, a la Sala de Servidores.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/05.001
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA PARA LA SEGURIDAD DEL EQUIPAMIENTO</h1> <p style="text-align: center;">Actualización al 15 de marzo de 2007</p>	<p>Página</p> <p style="text-align: center;">1 de 4</p>
---	---	---

## **1. Objetivo**

La Norma para la Seguridad del Equipamiento, está orientada a impedir o minimizar los daños que puedan originarse a los activos de información, por pérdida o exposiciones al riesgo físico y medioambiental, que puedan causar la interrupción de las actividades de la Facultad.

## **2. Alcance**

Esta norma cubre situaciones dadas en los ámbitos de la protección de los activos de información y la protección del equipamiento, el control y precauciones que deben implementarse respecto al suministro de energía eléctrica, la seguridad en el cableado de las redes eléctricas, telefónicas y de red, el mantenimiento de los equipos, la seguridad de los equipos fuera de las instalaciones de la Facultad, los procesos de baja o reutilización de equipos, principalmente.

## **3. Responsables**

La responsabilidad por la adecuada ejecución de los controles de seguridad física, en lo que hace al equipamiento, es enteramente de cada usuario de la Facultad y debe ser supervisada constantemente por el Encargado de Sistemas del CRTP, quien ante cualquier indicio de incidente crítico, debe tomar las acciones correctivas correspondientes y debe informar sobre los hechos al Comité de Sistemas, quien impondrá las acciones y sanciones correspondientes.

Es de responsabilidad del Encargado de Sistemas del CRTP, ofrecer a las áreas usuarias, todas las garantías de seguridad del equipamiento, considerando cada uno de los aspectos definidos en esta norma.

## **4. Definición de la Norma**

La protección del equipamiento es sumamente importante (incluyendo el equipamiento que se utiliza en forma externa, móvil y portátil) para reducir el acceso no autorizado a los datos y prevenir pérdidas o daños. Para este fin, se deben tomar en cuenta las siguientes consideraciones, al momento de implementar las medidas de seguridad física y ambiental.

### **a) Ubicación y protección del equipamiento**

El equipamiento de sistemas de la Facultad, debe ser ubicado y protegido a fin de reducir los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, tomando en cuenta las siguientes recomendaciones:

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/05.002
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA PARA LA SEGURIDAD DEL EQUIPAMIENTO</h1>	Pagina  2 de 4
	Actualización al 15 de marzo de 2007	

Se deben aislar parcial o totalmente los equipos computacionales, de comunicación y todos los activos de información, de las áreas de trabajo y de atención a clientes de la Facultad, tomando en cuenta el grado de sensibilidad y criticidad de la información que en estos se procesa, para minimizar el acceso innecesario.

El área en la que estén instalados los servidores en los que realizan procesamiento y almacenamiento de información, comunicaciones de red, desarrollo de sistemas, servicios de respaldo y equipos que manejen información sensible o crítica, deben ubicarse en sitios que permitan reducir el riesgo de falta de supervisión durante su uso.

Los servidores, equipamiento de comunicaciones y todo activo de información sensible, deben ser aislados y protegidos para reducir el nivel de riesgo.

Se deben monitorear periódicamente las condiciones ambientales de la Sala de Servidores y de los equipos principales (servidores), a fin prevenir condiciones adversas de funcionamiento.

## **b) Condiciones de Seguridad ambiental**

Se deben adoptar medidas de control y protección para minimizar riesgos de amenazas potenciales, instalando extintores de fuego en áreas visibles y de fácil acceso, detectores de humo para permitir reacciones oportunas, instalar estabilizadores de energía eléctrica y UPS, para reducir posibles alteraciones en el suministro de energía. Todo este equipamiento debe recibir mantenimiento periódico.

Deben ponerse letreros que establezcan las prohibiciones de comer, beber y fumar en las áreas de mayor riesgo, principalmente dentro de las instalaciones de la Sala de Servidores.

Se deben considerar el impacto que producirían desastres en edificaciones aledañas, filtraciones de agua, incendios y otros que puedan afectar a las instalaciones de mayor riesgo de la Sala de Servidores de la Facultad, en la casa matriz y en las agencias.

## **c) Suministro de energía**

El equipamiento debe estar protegido contra fallas en el suministro de energía eléctrica, las mismas que pueden ocurrir eventualmente, periódicamente o con mucha frecuencia, dependiendo del suministro de la zona en la que se encuentran las instalaciones.

Se debe garantizar un suministro regular y controlado de energía, para prevenir desperfectos por sobre-voltajes y bajas de tensión, a fin de cumplir las características

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/05.002
--	--	---	---	--------------------------



	<h1 style="text-align: center;">NORMA PARA LA SEGURIDAD DEL EQUIPAMIENTO</h1>	Pagina  3 de 4
Actualización al 15 de marzo de 2007		

establecidas por los fabricantes de los equipos conectados a la red de suministro eléctrico.

Para asegurar un buen suministro de energía eléctrica se recomienda que se considere la implementación de una toma alterna de suministro, instalación de UPS y un estabilizador de corriente. El Comité de Sistemas, evaluará la necesidad, factibilidad y nivel de riesgo, para elegir una o más de las recomendaciones antes mencionadas.

#### d) Seguridad del Cableado

Los cableados de energía eléctrica y de comunicaciones o de la Red LAN, deben ser protegidos contra interceptación o daños de manera tal que se reduzcan los riesgos.

Las líneas de instalación eléctrica y de transmisión de datos, deben ser tendidas en ductos aislados y subterráneos (siempre que sea posible), o deben estar sujetas a ductos que permitan su protección.

Las líneas del cableado de red deben estar protegidas contra accesos o interceptaciones no autorizadas, evitando que los ductos atraviesen áreas públicas.

Los cables de energía deben estar separados de los de la red, para evitar interferencias.

Se deben realizar barridos periódicos a las líneas de la red LAN, para identificar y desconectar accesos no permitidos o inutilizados, que requieran su anulación definitiva.

#### e) Mantenimiento de Equipos

Deben realizarse mantenimientos periódicos del equipamiento, a fin de asegurar que su disponibilidad e integridad sean permanentes y para prevenir daños mayores.

El servicio de mantenimiento debe estar de acuerdo con las especificaciones del fabricante y puede ser realizado internamente o por medio de la contratación del servicio a terceros, en tal caso, se debe buscar a empresas legalmente establecidas y con experiencia en el mercado.

Únicamente el personal autorizado debe realizar tareas de mantenimiento preventivo o correctivo al equipamiento de la Facultad.

Se debe llevar una bitácora o registro detallado de todas las fallas reportadas, supuestas y reales y de todo el mantenimiento preventivo y correctivo.

Cada vez que sea necesario que un equipo deba salir de la Facultad por motivos de mantenimiento, deben considerarse las medidas de seguridad, principalmente en CPUs, y

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/05.002
--	--	---	---	--------------------------

	<h1 style="text-align: center;">NORMA PARA LA SEGURIDAD DEL EQUIPAMIENTO</h1>	Pagina 4 de 4
Actualización al 15 de marzo de 2007		

medios magnéticos de almacenamiento, a fin de resguardar la información sensible y crítica de la Facultad.

Debe registrarse la entrada y salida de equipamiento fuera de la Facultad, indicando el número de serie, marca y otros datos que permitan identificar el equipo y sus componentes, la fecha y el motivo por el cual salió, nombre y cargo de quién autorizó la salida y del receptor a tiempo de entrada.

#### **f) Seguridad del equipamiento fuera del ámbito de la Facultad**

Se deben considerar los siguientes lineamientos para reducir los riesgos:

- La salida de Servidores y equipos de procesamiento y almacenamiento de información de alto riesgo, debe ser autorizada por el Comité de Sistemas, y debe quedar registrado y refrendado por sus miembros.
- Deberá existir una autorización escrita y respaldada, para permitir la salida de cualquier equipamiento móvil y portátil (computadoras portátiles, etc.), y de dispositivos de almacenamiento.
- Los dispositivos y equipamiento retirados de la Facultad, no deben ser desatendidos en lugares públicos.

#### **g) Baja segura o reutilización de equipamiento**

Se debe minimizar el riesgo de acceso a información sensible y crítica a tiempo de dar de baja o reutilizar un equipamiento.

Los medios de almacenamiento que contienen información sensible, deben ser físicamente destruidos, o sobre escritos en forma segura.

Debe ponerse mucha atención en los componentes de los equipos, principalmente de los medios de almacenamiento fijo o removibles, de los que se deben eliminar físicamente toda la información sensible y el software que cuenta con alguna licencia de funcionamiento.

A tiempo de dar de baja un equipo, es necesario realizar una evaluación de riesgo, a fin de determinar si los medios de almacenamiento dañados, deben ser destruidos, reparados o desechados.

Deben registrarse los eventos de baja de equipamiento, formateo de discos duros, reutilización y desecho de medios magnéticos, a fin de mantener la evidencia del mismo.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/05.002
--	---	---	---	--------------------------

	<p style="text-align: center;"><b>POLÍTICA DE GERENCIA DE LAS COMUNICACIONES Y OPERACIONES</b></p> <p style="text-align: center;">Actualización al 27 de febrero de 2007</p>	<p>Página 1 de 2</p>
---	--	--------------------------

## **1. Propósito y Alcance**

La política de gerencia de las comunicaciones y operaciones pretende garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información de la Facultad de Arquitectura, Artes, Diseño y Urbanismo, minimizar el riesgo de fallas en los sistemas, proteger la integridad del software y la información, mantener la integridad y disponibilidad de los servicios de procesamiento y comunicación de información, garantizar la seguridad de la información en las redes y la protección de la infraestructura de apoyo, así como impedir el daño a los activos y las interrupciones en las actividades de la Facultad.

Esta política se aplica a autoridades, docentes, estudiantes, funcionarios administrativos y toda otra persona relacionadas de algún modo a la Facultad.

## **2. Declaración de la Política**

Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todas las instalaciones de procesamiento de información de la Facultad.

Cuando sea posible, tomando en cuenta la cantidad de personal en el Área de Cómputo, se debe implementar la segregación de funciones en la Facultad cuando corresponda, a fin de reducir el riesgo del uso negligente o mal uso deliberado del sistema.

Se requiere una planificación y preparación anticipada para garantizar la disponibilidad de capacidad y recursos adecuados en la Facultad.

Deben realizarse proyecciones para futuros requerimientos de capacidad, a fin de reducir el riesgo de sobrecarga del sistema. Se deben establecer, documentar y probar los requerimientos operativos de nuevos sistemas para la Facultad antes de su aprobación y uso.

Es necesario tomar precauciones para prevenir y detectar la introducción de software malicioso en la Facultad. El software y las instalaciones de procesamiento de información son vulnerables a la introducción de software malicioso como, por ejemplo, virus informáticos, gusanos ("worms") de red, "troyanos" y bombas lógicas.

Se debe concientizar a los usuarios de la Facultad acerca de los peligros del software no autorizado o malicioso, y el Encargado del Área de Cómputo debe, cuando corresponda, introducir controles especiales para detectar o prevenir la introducción de los mismos. En particular, es esencial que se tomen precauciones para detectar y prevenir virus informáticos en computadoras personales de la Facultad.

Desarrollado por:  Fernando Echavarria	Revisión Dirección del CRTP: Max Arnsdorff	Revisión Dirección de Carrera: Roberto Moreira 1/03/07	Aprobación: Vicedecano Decano	Código:  PS/006
--	--	---	-------------------------------	-----------------------

	<div> <div> <b>POLÍTICA DE GERENCIA DE LAS COMUNICACIONES Y OPERACIONES</b> </div> <div> <b>Actualización al 27 de febrero de 2007</b> </div> </div>	<b>Página</b>  <b>2 de 2</b>
---	--	------------------------------------

Se deben establecer procedimientos de rutina para realizar copias de resguardo de los datos (Backups) y ensayando su restablecimiento oportuno (pruebas de restore), registrando eventos y posibles fallas.

Los medios de almacenamiento de la Facultad deben ser controlados y protegidos físicamente. Se deben establecer procedimientos operativos apropiados para proteger documentos, medios de almacenamiento (cintas, discos, disquetes, etc.), datos de entrada/salida y documentación del sistema contra daño, robo y acceso no autorizado.

### **3. Cumplimiento**

La presente política debe ser cumplida por todos los usuarios, empleados, contratistas y terceros relacionados de alguna manera con la Facultad.

<b>Desarrollado por:</b>  Fernando Echavarria	<b>Revisión Dirección del CRTP:</b> Max Arnsdorff	<b>Revisión Dirección de Carrera:</b> Roberto Moreira 1/03/07	<b>Aprobación:</b> Vicedecano Decano	<b>Código:</b>  PS/006
---	---	--	--	------------------------------

	<h1 style="text-align: center;">NORMA DE INTERCAMBIO DE INFORMACIÓN Y SOFTWARE</h1>	Pagina 1 de 4
	Actualización al 22 de marzo de 2007	

## **1. Objetivo**

Normar el intercambio de información y software evitando la pérdida, modificación o uso inadecuado de la información, que intercambia la Facultad con otras organizaciones, en caso que esto se realice.

## **2. Alcance**

Cubre las atribuciones y controles que debe implementar el Encargado de Sistemas del CRTP en materia de seguridad a tiempo de intercambiar información y software.

## **3. Responsables**

La responsabilidad por garantizar que el intercambio de información y software sea seguro, recae en el Encargado de Sistemas del CRTP y su personal (en caso de existir).

El Director del CRTP y el Comité de Sistemas es responsable de las autorizaciones y del monitoreo de las operaciones de intercambio de información y software.

## **4. Definición de la Norma**

### ***Acuerdos de intercambio de información y software***

La Facultad debe establecer acuerdos formales y por escrito con las organizaciones con quienes realice o vaya a realizar intercambio de información y software, velando por la seguridad de la misma y reflejando el grado de sensibilidad y criticidad de la información, para la Facultad.

Los acuerdos sobre requisitos de seguridad en este sentido, deben considerar lo siguiente:

- a) Se deben establecer los niveles gerenciales y responsables del control y la notificación de transmisiones, envíos y recepciones.
- b) Se debe contar con un procedimiento adecuado para la notificación del emisor, las transmisiones, envíos y recepciones.
- c) El armado de paquetes de información a ser enviada y recibida, debe responder a los acuerdos a los que se llegue con las organizaciones externas, en función a los requerimientos de la Facultad y la homologación con los requerimientos externos, siguiendo estrechamente las Políticas, Normas y Procedimientos de seguridad de la Facultad.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.007
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE INTERCAMBIO DE INFORMACIÓN Y SOFTWARE</h1>	Pagina 2 de 4
Actualización al 22 de marzo de 2007		

- d) En caso de requerir mensajeros (empresas de Courier), se deben realizar acuerdos y contratos formales, que garanticen la seguridad y confidencialidad de la información y el software a ser intercambiado con terceros.
- e) Deben incluirse cláusulas que especifiquen las responsabilidades y obligaciones en caso de pérdida de datos, por parte del emisor y del receptor.
- f) Se debe emplear un sistema de rotulado de información crítica, confidencial o sensible, garantizando que el significado de los rótulos sea inmediatamente comprendido y para que la información sea adecuadamente protegida. (Ver *Norma de Clasificación de la Información NS/3.002*)
- g) Se deben incluir cláusulas sobre la protección de la información y software, y las responsabilidades de la protección de los datos, el cumplimiento del derecho de propiedad intelectual y consideraciones similares.
- h) Se debe especificar que la información tendrá un formato convenido de grabación y lectura, que podrá ser presentado en archivo de texto plano, encriptado, en estructura de datos, etc.
- i) En caso de emplear claves criptográficas, se deben establecer las cláusulas correspondientes para protegerlas y garantizar la seguridad de la información.

### ***Seguridad en los medios de tránsito***

La información puede ser vulnerable a accesos no autorizados, mal uso o alteración durante el transporte físico del medio, cuando se envían a través de servicios postales o de mensajería. Para salvaguardar la información que es enviada a otras organizaciones, como producto del intercambio de información, se deben considerar los siguientes controles:

- a) Utilizar medios de transporte o medios de mensajería confiables.
- b) Se deben adoptar controles especiales, cuando resulte necesario a fin de proteger la información sensible contra divulgación o modificación no autorizada. Tales controles pueden ser:
  - Empleo de recipientes cerrados.
  - Entrega en mano.
  - Embalaje a prueba de apertura no autorizada.
  - En caso de requerirse, se debe emplear firma digital y criterios de encriptación, para garantizar la confidencialidad.

### ***Seguridad del correo electrónico***

#### **a) Riesgos de seguridad**

El correo electrónico, es un medio de comunicación altamente explotado actualmente, es así que su utilidad es de máxima prioridad y su protección requiere una adecuada atención.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.007
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE INTERCAMBIO DE INFORMACIÓN Y SOFTWARE</h1>	Pagina 3 de 4
Actualización al 22 de marzo de 2007		

El correo electrónico conlleva un alto grado de informalidad y vulnerabilidad a las acciones no autorizadas, debido a su estructura y facilidad de acceso. Estos riesgos pueden ser:

- Vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación del servicio.
- Vulnerabilidad a errores producidos por consignación errónea de direcciones y pérdida de confiabilidad y disponibilidad del servicio.
- Implicancia de la publicación externa de listados de personal accesible al público.
- Fallas en el control de accesos remotos a las cuentas de correo de la Facultad.

## b) **Controles de correo electrónico.**

La Facultad debe implementar los controles adecuados, de manera clara y particular, para el uso y explotación de este servicio de comunicación, para lo cual se deben considerar los siguientes tópicos:

- Salvaguardar las operaciones de la Facultad que involucren el uso de correo electrónico, por medio de programas informáticos de protección contra software malicioso, para evitar ataques de virus informáticos, correos interceptados, etc.
- Se deben controlar y proteger los archivos adjuntos de correo electrónico, a fin de resguardar su confidencialidad y evitar accesos no autorizados. En caso de ser necesario, se deben implementar técnicas de criptografía y controles criptográficos.
- Se debe entrenar e instruir a los usuarios de este servicio, cómo y cuando es posible emplearlo y cuándo no.
- Es necesario delegar a cada usuario de este servicio, la responsabilidad por el buen empleo del correo electrónico, a fin de no comprometer la seguridad de la información de la Facultad.
- Se debe implementar la autenticación de los mensajes electrónicos.
- Implementar o aprovechar las ventajas de los programas y software de control de software malicioso, como los antivirus, anti-spam, anti-spyware, etc.

## c) **Seguridad de los sistemas electrónicos de oficina**

La tecnología empleada para el ejercicio de las funciones del personal de la Facultad, referida como sistemas electrónicos de oficina, que involucra a computadoras de escritorio, computación móvil o inalámbrica, red de comunicación telefónica fija o móvil, correo postal, correos de voz, máquinas de fax, palms, etc., debe ser adecuadamente empleada por el personal de la Facultad, con el fin de garantizar la confidencialidad de la información.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.007
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE INTERCAMBIO DE INFORMACIÓN Y SOFTWARE</h1>	Pagina 4 de 4
Actualización al 22 de marzo de 2007		

Es necesario concientizar a todo el personal de la Facultad, sobre las ventajas del empleo de la tecnología y los riesgos en materia de seguridad, que conlleva el mal uso de los recursos. Los usuarios de la tecnología de la información, deben tener conocimiento de las consecuencias de un mal uso de los recursos y del grado de responsabilidad que tienen dentro de la Facultad.

#### **d) Sistemas de acceso público**

Se deben tomar recaudos para proteger la integridad de la información publicada electrónicamente y así prevenir la modificación no autorizada que podría dañar la imagen de la Facultad. Esta información publicada se refiere principalmente a la publicada en el sitio o portal Web de la Facultad.

Los sistemas de publicación electrónica, en particular aquellos que permiten retroalimentación (feedback) o ingreso directo de información, actualizaciones y modificaciones vía FTP, debe ser cuidadosamente controlados, tomando en cuenta lo siguiente:

- La información que se ingresa o publica, debe ser completa, exacta y oportuna.
- La información sensible, debe ser protegida durante los procesos de recolección y almacenamiento.
- El acceso al sistema de publicación, no debe permitir accesos accidentales o forzados a las redes a las cuales se conecta el mismo.

#### **e) Otras formas de intercambio de información**

Otras formas de intercambio de información, son realizadas a través de medios de comunicación de voz, fax y video. La información contenida en dichos medios, puede verse comprometida, por tanto debe concientizarse al personal de la Facultad acerca del uso y discreción en el empleo de dichos medios, tomando en cuenta las siguientes recomendaciones:

- No revelar información sensible vía teléfono fijo o móvil, para evitar el ser escuchado por personas ajenas cercanas en el lado del receptor o por intervenciones en las líneas telefónicas.
- No sostener conversaciones confidenciales en lugares públicos o áreas de la Facultad cuya acústica permita filtrarse información de alto riesgo.
- No dejar mensajes que contengan datos o información crítica en buzones de mensajes de voz, para evitar que terceros no autorizados tengan acceso a la misma.
- El uso de Fax y otros equipos de oficina sujetos de esta norma, deben ser debidamente controlados y su uso debe ser restringido a personal autorizado.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.007
--	---	---	---	--------------------------



	<p><b>NORMA PARA LOS PROCEDIMIENTOS Y RESPONSABILIDADES OPERATIVAS</b></p> <p>Actualización al 16 de marzo de 2007</p>	<p>Página 1 de 3</p>
---	--	--------------------------

## **1. Objetivo**

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información generada por las operaciones de la Facultad.

## **2. Alcance**

Esta norma abarca el establecimiento de las responsabilidades y las características de los procedimientos para la administración y operación de la Sala de Sistemas, donde se procesa la información.

## **3. Responsables**

El Encargado de Sistemas del CRTP, el personal dependiente y el Comité de Sistemas, tiene la responsabilidad de implementar, evaluar y realizar las actualizaciones correspondientes a los procedimientos que garanticen el alcance del objetivo de la presente norma.

## **4. Definición de la Norma**

La Facultad, cuenta con una Sala de Servidores, mismo que debe garantizar que el procesamiento de la información generada a partir de las operaciones de la misma, sea seguro y correcto.

Es altamente necesario que todos los procedimientos operativos y sus cambios sean adecuadamente documentados y reflejarlos en los procedimientos mismos, se deben establecer las responsabilidades y procedimientos que garanticen una pronta recuperación de las operaciones, frente a cualquier incidente, que pueda amenazar la continuidad de las operaciones de la Facultad. Estos y otros aspectos, son establecidos a continuación:

### ***Documentación de los procedimientos operativos***

El Área de Sistemas, debe contar con la documentación adecuada de cada actividad operativa de sistemas, a fin de mantener los procedimientos operativos claramente identificados, en estrecha relación a las políticas de seguridad. Estos procedimientos deben ser tratados como documentos formales, cuyos cambios y adecuaciones, deben ser aprobados por el Comité de Sistemas.

En la definición de los procedimientos, se deben tomar en cuenta los detalles mismos de la operativa de sistemas e incluir mínimamente las siguientes instrucciones:

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.001
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA PARA LOS PROCEDIMIENTOS Y RESPONSABILIDADES OPERATIVAS</h1>	<p style="text-align: center;">Pagina 2 de 3</p>
<b>Actualización al 16 de marzo de 2007</b>		

- a) Definir los pasos e instancias del procesamiento y manejo de la información.
- b) Definir los requerimientos de programación de tareas, incluyendo interdependencias con otros módulos, subsistemas y con otros sistemas, y estableciendo las escalas de tiempo de ejecución, desde las primeras hasta las últimas tareas.
- c) Definir las instrucciones o pasos a seguir para el manejo de errores u otras condiciones excepcionales que podrían surgir de la ejecución de las tareas.
- d) Definir las instrucciones que se deben seguir para el manejo y administración de las salidas, reportes, informes, etc., originados por la operación misma del sistema, respetando los niveles de confidencialidad y criticidad de los recursos de información, su divulgación o destrucción, en caso necesario.
- e) Definir las instrucciones y pasos necesarios para alcanzar la recuperación de las operaciones del sistema, en caso de fallas e incidentes.

Debe prepararse además documentación sobre los procedimientos relacionados con las actividades de mantenimiento del sistema que se refieran a las instalaciones de procesamiento de información y comunicaciones de la Sala de Servidores de la Facultad.

### ***Control de Cambios en las Operaciones***

Se deben controlar los cambios en el Sistema y los cambios en las instalaciones de la Sala de Servidores de la Facultad.


La responsabilidad de la ejecución de los procedimientos operativos de sistemas, es del Encargado de Sistemas del CRTP, quien debe garantizar un control satisfactorio en todos los cambios realizados al software, hardware y a los procedimientos. Es también responsable por la restauración de las operaciones en caso de que los cambios resultasen fallidos.

La responsabilidad del Comité de Sistemas, es la de autorizar y aprobar los cambios propuestos por el Encargado de Sistemas del CRTP, en función de garantizar el correcto y seguro procesamiento de la información.

Para realizar una adecuada implementación y un correcto seguimiento a los cambios, se deben considerar los siguientes controles:

- a) Se debe identificar y registrar cada cambio que resulte significativo.
- b) Se debe realizar una evaluación previa del impacto que genere la implementación de cambios en la operativa.
- c) Los cambios propuestos, deben ser aprobados formalmente por el Comité de Sistemas.
- d) Cada cambio propuesto y aprobado, debe ser comunicado y adecuadamente divulgado al personal que resulte involucrado.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.001
--	---	---	---	--------------------------

	<p><b>NORMA PARA LOS PROCEDIMIENTOS Y RESPONSABILIDADES OPERATIVAS</b></p> <p>Actualización al 16 de marzo de 2007</p>	<p>Página 3 de 3</p>
---	--	--------------------------

### ***Procedimientos de manejo de incidentes***

En este acápite, se define en términos de responsabilidad, la función que debe cumplir el Encargado de Sistemas del CRTP, en materia de definición de un procedimiento de manejo de incidentes (Plan de Contingencias), que permita garantizar una respuesta rápida, eficaz y sistemática frente a la ocurrencia de incidentes relacionados con la seguridad.

En el Plan de Contingencias se deben integrar los siguientes controles:

- a) Identificación de todos los probables tipos de incidentes relativos a la seguridad. (p.ej. fallas en el Sistema; negación de servicio; errores generados por datos incompletos o inexactos; violaciones de la confidencialidad, etc.)
- b) Identificación y análisis de las causas de cada incidente probable.
- c) Recolección de pistas de Auditoría (logs).
- d) Notificación de las acciones de recuperación al Comité de Sistemas y al personal involucrado.
- e) Los procedimientos de recuperación deben contar con controles detallados y formalizados respecto a las violaciones de la seguridad y de corrección de fallas del Sistema.

### ***Separación de Funciones***

La separación o segregación de funciones del Área de Sistemas y de las instalaciones de desarrollo y producción, es un método que reduce la probabilidad de duplicidad de funciones, suplantación de funciones y permite incrementar los niveles de seguridad. En el caso de la Facultad y por la poca cantidad de personal que tiene el Área de Sistemas, se debe evaluar este aspecto el momento que se decida incrementar el personal en el área, esta evaluación debe estar a cargo del Comité de Sistemas.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.001
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA PARA LA PLANIFICACIÓN Y APROBACION DE SISTEMAS</h1> <p style="text-align: center;">Actualización al 16 de marzo de 2007</p>	<p>Página 1 de 2</p>
---	---	--------------------------

## **1. Objetivo**

El objetivo principal es minimizar el riesgo de fallas en los sistemas de la Facultad.

## **2. Alcance**

La presente norma abarca a los sistemas de la Facultad.

## **3. Responsables**

Es responsable de implementar la presente norma el Encargado de Sistemas del CRTP, bajo la supervisión del Director del CRTP y aprobación de las acciones a ejecutar del Comité de Sistemas.

## **4. Definición de la Norma**

### ***Planificación de la Capacidad***

La Planificación de acciones futuras en materia de Sistemas, es de vital importancia, debido a que mínimos cambios en la operativa de sistemas, puede representar grandes alteraciones y cambios en la operativa misma de la Facultad.

Se deben monitorear las demandas de capacidad y realizar proyecciones para futuros requerimientos, a fin de garantizar la disponibilidad del poder de procesamiento y almacenamiento adecuado de los servidores.

### ***Aprobación del Sistema***

En este acápite, se definen los criterios de aprobación para los nuevos sistemas de información, nuevos módulos para el sistema principal, las actualizaciones y nuevas versiones del sistema y los módulos. Dichos criterios son:

- a) Debe documentarse el desempeño y los requerimientos de capacidad de las computadoras.
- b) Se debe contar con un adecuado Plan de Contingencias y recuperación.
- c) Se deben planificar y ejecutar pruebas de los procedimientos operativos de rutina.
- d) Se deben tomar en cuenta las especificaciones del resto de normas de seguridad.
- e) Los procedimientos manuales, si existen, deben reflejar eficacia ante las situaciones emergentes de los cambios.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.002
--	---	---	---	--------------------------

	<b>NORMA PARA LA PLANIFICACIÓN Y APROBACION DE SISTEMAS</b>	Pagina 2 de 2
	Actualización al 16 de marzo de 2007	

- f) Para la aprobación, debe documentarse claramente que los cambios en las nuevas versiones y nuevos sistemas, no interfieren o afectan al resto, especialmente en periodos pico y durante la etapa de inscripción.
- g) Se debe documentar y garantizar que los cambios no afectan la seguridad global de la Facultad, en materia de información.
- h) Deben existir los manuales de usuario y planes de entrenamiento y capacitación de los cambios, nuevas versiones y/o nuevos sistemas.

En todos los casos, la aprobación de cambios al sistema existente, nuevas versiones de los módulos, etc., deben ser analizados y validados con los usuarios finales y aprobados por el Comité de Sistemas, en base a las pruebas que reflejen el cumplimiento de los requerimientos.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.002
--	---	---	---	--------------------------

	<p style="text-align: center;"><b>NORMA PARA LA PROTECCION COTRA SOFTWARE MALICIOSO (VIRUS)</b></p> <p style="text-align: center;">Actualización al 19 de marzo de 2007</p>	<p>Pagina 1 de 4</p>
---	---	--------------------------

## **1. Objetivo**

Proteger la integridad del software y la información de la Facultad, tomando las precauciones adecuadas para prevenir y detectar la introducción de software malicioso, que ponga en riesgo las operaciones globales de la Facultad.

## **2. Alcance**

La presente norma, alcanza al Encargado de Sistemas del CRTP, quien debe diseñar e implementar controles adecuados, y realizar el seguimiento correspondiente. Abarca además, a todo el personal de la Facultad, que interactúa con computadoras de escritorio, portátiles y otros recursos tecnológicos, por medio de los cuales se pueden infiltrar programas o software maliciosos.

## **3. Responsables**

La responsabilidad de diseñar, implementar y realizar el mantenimiento a los controles de protección contra software malicioso, es del Encargado de Sistemas del CRTP, y las áreas usuarias deben cumplir dichos controles, a fin de prevenir y proteger a la Facultad de software malicioso.

El Comité de Sistemas, es el responsable de monitorear periódicamente que los controles son efectivos, en base a los informes del Encargado de Sistemas del CRTP.

## **4. Definición de la Norma**

El software y las instalaciones de procesamiento de información de la Facultad, pueden ser vulnerables a la introducción de software malicioso, si no se aplican las medidas necesarias para reducir el riesgo por medio de la implementación y aplicación de controles adecuados.

Se entiende por *software malicioso*, a cualquier programa instalado o adquirido de alguna manera, que ponga en riesgo la seguridad de la información de la Facultad. Estos programas pueden ser virus informáticos, gusanos, troyanos y bombas lógicas.

### ***Controles contra Software Malicioso***

Se deben implementar controles de detección y prevención para la protección contra software malicioso y procedimientos adecuados de concientización de los usuarios, que se basará en los principios de seguridad, controles de cambios de acceso al sistema y gestión de cambios.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.003
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA PARA LA PROTECCION COTRA SOFTWARE MALICIOSO (VIRUS)</h1>	<p>Pagina 2 de 4</p>
	<p style="text-align: center;">Actualización al 19 de marzo de 2007</p>	

El Encargado de Sistemas del CRTP, deberá implementar mínimamente los siguientes controles, a fin de minimizar el riesgo.

a) **Control de Uso Autorizado de Software**

Se debe controlar que en los equipos de la Facultad exista solamente el software autorizado por el Comité de Sistemas, en base al análisis realizado con relación al software que es necesario para desarrollar el trabajo y las actividades normales del personal de la Facultad, a fin de reducir el riesgo de intrusión de software malicioso en las instalaciones de la Facultad, tomando en cuenta el Derecho Propietario y las leyes de Propiedad Intelectual.

b) **Control en la obtención de archivos y software**

Debe ponerse adecuado control en la obtención de archivos y software a través de redes externas, medios magnéticos (discos ópticos, cintas magnéticas, disquetes, USB Flash Memory, etc.), Internet, correos electrónicos y archivos enlazados y la red local, sea de instalación física o inalámbrica.

Deben señalarse con la mayor precisión posible, las medidas de protección a tomarse, las responsabilidades y las acciones correctivas inmediatas.

Es preciso que se controle el cumplimiento de lo establecido para la aplicación de la *Norma de Seguridad de los Procesos de Desarrollo y Soporte*.

c) **Instalación y actualizaciones de Software de detección (Antivirus, Cortafuegos, etc.)**

En respuesta a la Política general de Seguridad de la Facultad, y en atención a las medidas de seguridad que se deben implementar ante ataques de Virus informáticos, programas maliciosos como Troyanos, Gusanos y otros, que pueden ser adquiridos por cualquier medio directa o indirectamente, es altamente necesario tener versiones actualizadas de programas de detección y prevención de este tipo de ataques.

Se deben instalar versiones actualizadas de programas antivirus que cuenten con el soporte técnico correspondiente y que permitan proteger los servidores, las comunicaciones, las estaciones de trabajo, los equipos portátiles, etc. de las amenazas de virus y software malicioso.

La configuración de tales programas, debe permitir realizar actualizaciones de motores de detección y archivos o bases de definiciones de virus informáticos conocidos, tal que pueda realizarse por lo menos una vez cada día.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.003
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA PARA LA PROTECCION COTRA SOFTWARE MALICIOSO (VIRUS)</h1>	Pagina  3 de 4
	Actualización al 19 de marzo de 2007	

Los directorios donde se encuentren archivos infectados en cuarentena, no deben contener elementos vigentes por más de un día y deben ser vaciados de manera segura.

Se deben tomar las medidas necesarias para que los mecanismos de detección permanente y en tiempo real estén activos todo el tiempo, para proteger correos electrónicos, ataques de red, secuencias de comandos, etc.

Se debe contar con un registro de los eventos de análisis parcial o completo, realizados en cada recurso de hardware que lo requiera.

**d) Verificación de existencia de virus en medios magnéticos**

Se debe realizar un control adecuado y verificación de la existencia de virus informáticos en programas, archivos, correos electrónicos, etc., que sean recibidos en medios electromagnéticos, ópticos y digitales, cuyo origen sea incierto o no autorizado, antes de su uso.

Se debe entrenar adecuadamente a todo el personal, sobre el procedimiento de protección contra software malicioso y poner énfasis en el cuidado de realizar los análisis de antivirus correspondientes.

**e) Verificación de archivos adjuntos en correos electrónicos y archivos descargados de Internet.**

Se deben realizar las verificaciones adecuadas y ajustar la configuración de los programas de protección antivirus y de software malicioso, a fin de detectar la presencia de virus u otros programas maliciosos, que estén incluidos como archivos adjuntos de correos electrónicos y de archivos descargados vía Internet.


Esta verificación debe llevarse a cabo en todas las estaciones de trabajo, equipos portátiles, servidores y otros, que tengan conexión a Internet o que presten servicios de correo electrónico.

**f) Contingencias y recuperación**

Se deben incluir estos controles en la elaboración del Plan de Contingencias, a fin de reducir el riesgo y minimizar la probabilidad de ocurrencia de incidentes, de modo tal que pueda evaluarse tempranamente los efectos e identificar las prontas correcciones.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.003
--	---	---	---	--------------------------



	<p style="text-align: center;"><b>NORMA PARA LA PROTECCION COTRA SOFTWARE MALICIOSO (VIRUS)</b></p> <p style="text-align: center;">Actualización al 19 de marzo de 2007</p>	<p>Pagina 4 de 4</p>
---	---	--------------------------

g) **Difusión de información sobre software malicioso**

Deben emitirse y publicarse al interior de la Facultad, boletines periódicos con información exacta, confiable y fidedigna, relativa a software malicioso, sus consecuencias, las fuentes de información y las acciones que se deben tomar para prevenir desastres.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.003
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE MANTENIMIENTO Y DISPONIBILIDAD DE LOS SERVICIOS</h1> <p style="text-align: center;">Actualización al 20 de marzo de 2007</p>	<p>Página 1 de 2</p>
---	---	--------------------------

## **1. Objetivo**

El objetivo es el de mantener la integridad y disponibilidad de los servicios de procesamiento de información y las comunicaciones de la Facultad.

## **2. Alcance**

Esta norma abarca al Encargado de Sistemas del CRTP y sus dependientes (en caso de existir), quienes deben ejecutar los procedimientos de resguardo y restauración de la información, el mantenimiento y continuidad de las comunicaciones y las operaciones de los Sistemas de la Facultad, para poder brindar la integridad y disponibilidad esperadas.

## **3. Responsables**

La responsabilidad de realizar las copias de respaldo de los datos, archivos, etc., es del Encargado de Sistemas del CRTP, quien además debe mantener un registro de los eventos, fallas y el monitoreo de la Sala de Servidores.

## **4. Definición de la Norma**

Se deben establecer procesos de rutina para llevar a cabo la estrategia de resguardo y restauración, para lo cual se establece lo siguiente:

### ***Resguardo de la Información***

Se deben realizar periódicamente copias de resguardo de la información y el software esenciales para la Facultad. Se debe contar con adecuadas instalaciones de resguardo para garantizar que toda la información y el software esencial de la Facultad puede recuperarse una vez ocurrido un desastre o falla de los dispositivos. Las disposiciones para el resguardo de cada uno de los sistemas deben ser probadas periódicamente para garantizar que cumplen con los requerimientos necesarios para garantizar la seguridad y continuidad de las operaciones. Se deben tener en cuenta los siguientes controles:

- a) Los respaldos obtenidos de los sistemas más importantes de la Facultad, se deben almacenar en áreas restringidas y de alta seguridad, poniendo, en la medida de lo posible, una copia en un lugar externo a las instalaciones de la Facultad.
- b) Los medios de resguardo deben ser revisados periódicamente, a fin de garantizar la confiabilidad de los mismos.
- c) Los procedimientos de resguardo y restauración deben verificarse y probarse con cierta periodicidad, a fin de ajustar y afinar los tiempos requeridos en procedimientos operativos.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.004
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE MANTENIMIENTO Y DISPONIBILIDAD DE LOS SERVICIOS</h1>	Pagina  2 de 2
Actualización al 20 de marzo de 2007		

Se debe determinar el período de resguardo de la información esencial para la Facultad, y también los requerimientos de copias de archivos que serán resguardados en forma permanente.

### ***Registro de actividades del personal operativo***

El personal operativo debe mantener un registro de sus actividades. Los registros deben incluir mínimamente:

- a) Hora de inicio y cierre del sistema o módulo.
- b) Errores detectados en el Sistema y medidas correctivas tomadas.
- c) Confirmación del manejo correcto de archivos de datos y salidas.
- d) Nombre de la persona que realiza las actualizaciones del registro.

Los registros de actividades del personal operativo deben estar sujetos a verificaciones periódicas e independientes con relación a los procedimientos operativos.

### ***Registro de Fallas***

Las fallas encontradas por los usuarios, deben ser registradas, documentadas y comunicadas al Encargado de Sistemas del CRTP, para que sean corregidas. Estas fallas pueden referirse a problemas con el procesamiento de los datos y fallas en los sistemas de comunicaciones.

Se deben realizar los siguientes controles, para garantizar que el servicio de procesamiento y comunicaciones sea íntegro y esté disponible:

- a) Revisar los registros de fallas, a fin de reflejar que han sido resueltas de acuerdo a los requerimientos del usuario.
- b) Revisar las medidas correctivas para garantizar que los controles no fueron comprometidos.
- c) Verificar que las medidas adoptadas fueron debidamente autorizadas por el Comité de Sistemas.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.004
--	---	---	---	--------------------------

	<b>NORMA DE GESTIÓN DE LA RED</b>	Página <b>1 de 2</b>
	Actualización al 20 de marzo de 2007	

## **1. Objetivo**

El objetivo de esta norma es el de asegurar y salvaguardar la información de las redes y la protección de la infraestructura de soporte de la Facultad

## **2. Alcance**

La gestión de la red involucra a todo el personal de la Facultad, terceros involucrados, y especialmente al Encargado de Sistemas del CRTP, quien debe implementar los mejores controles para garantizar que la información que fluye por la red (local, remota, inalámbrica, etc.) esté a salvo de cambios no autorizados.

## **3. Responsables**

Es responsable por implementar los controles y realizar el monitoreo correspondiente, el Encargado de Sistemas del CRTP, además de todo el personal de la Facultad y terceros involucrados, quienes deben cumplir todas las políticas y normas de seguridad.

El Encargado de Sistemas del CRTP, es responsable por salvaguardar todo el equipo de red y comunicaciones de la Sala de Servidores de la Facultad.

Todos los funcionarios de la Facultad, son responsables por mantener la seguridad y el buen empleo de los equipos de trabajo y sus conexiones a la red.

## **4. Definición de la Norma**

La gestión de la red y las comunicaciones, requiere que se definan los controles necesarios y adecuados para lograr los mejores niveles de seguridad de los datos y la protección de los servicios.

En general, para elaborar los controles adecuados, se deben considerar los siguientes aspectos:

- Se debe separar claramente las responsabilidades operativas de las redes y telecomunicaciones, de la operación de las estaciones de trabajo.
- Se deben establecer responsabilidades para la gestión y protección de los equipos remotos (en caso de existir).
- Se deben mantener la disponibilidad y operabilidad de los servicios de red y computadoras conectadas.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.005
--	---	---	---	--------------------------

	<p align="center"><b>NORMA DE GESTIÓN DE LA RED</b></p> <p align="center"><b>Actualización al 20 de marzo de 2007</b></p>	<p align="center">Pagina <b>2 de 2</b></p>
---	---	--

- d) Las actividades del Encargado de Sistemas del CRTP, deben orientarse a optimizar los servicios y garantizar que los controles se aplican uniformemente en toda la Facultad.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.005
--	---	---	---	--------------------------

	<p align="center"><b>NORMA DE GESTIÓN Y SEGURIDAD DE LOS MEDIOS DE ALMACENAMIENTO</b></p> <p align="center">Actualización al 22 de marzo de 2007</p>	<p align="center">Pagina 1 de 3</p>
---	--	---

## **1. Objetivo**

Impedir que los activos de información sean dañados y por consiguiente, evitar interrupciones en las actividades tecnológicas de la Facultad.

## **2. Alcance**

Todo el personal de la Facultad, debe ser conciente de la necesidad de proteger los activos de información, sean estos físicos o lógicos.

## **3. Responsables**

La responsabilidad por proporcionar a todo el personal las pautas necesarias para proteger los activos de información, es del Encargado de Sistemas del CRTP.

Todo el personal de la Facultad es responsable por proteger y precautelar la integridad de los activos de información, con el objetivo claro de evitar interrupciones de las operaciones, debido a fallas ocasionadas por la falta de cuidados en la explotación de los recursos de información.

## **4. Definición de la Norma**


Los medios de almacenamiento, deben ser controlados y protegidos físicamente, para evitar el acceso no autorizado a la información contenida en los mismos, que puede ser muy sensible y por tanto ocasionar interrupciones en las operaciones de la Facultad.

### ***Gestión de medios informáticos removibles***

Deben existir procedimientos para la gestión de medios informáticos removibles, tales como cintas, discos ópticos, flash memory, o disquetes, tomando en cuenta los siguientes lineamientos:

- a) Si el contenido de los medios removibles ya no es requerido, debe borrarse o eliminarse, antes de que dichos medios sean reutilizados.
- b) Se debe requerir autorización para retirar cualquier medio de la Facultad y se debe realizar un registro de todos los retiros a fin de mantener un detalle completo. Esta autorización debe ser otorgada por el Encargado de Sistemas del CRTP, el Director del CRTP o del Comité de Sistemas, de acuerdo al bien a ser retirado.
- c) Todos los medios informáticos deben resguardarse en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.006
--	---	---	---	--------------------------

	<p align="center"><b>NORMA DE GESTIÓN Y SEGURIDAD DE LOS MEDIOS DE ALMACENAMIENTO</b></p>	<p align="center">Pagina 2 de 3</p>
<p align="center">Actualización al 22 de marzo de 2007</p>		

### ***Eliminación de Medios Informáticos***

Cuando ya no son requeridos, los medios informáticos deben eliminarse de manera segura. Si los mismos no se eliminan cuidadosamente, la información sensible puede filtrarse a personas ajenas a la organización. Se deben establecer procedimientos formales para la eliminación segura de los medios informáticos, a fin de minimizar este riesgo. Deben considerarse los siguientes controles:

- a) Los medios que contienen información sensible deben ser almacenados y eliminados de manera segura, por ejemplo, incinerándolos o rompiéndolos en pequeños trozos, o eliminando los datos y utilizando los medios en otra aplicación dentro de la Facultad.
- b) El siguiente listado identifica ítems que podrían requerir una eliminación segura:
  1. Documentos en papel
  2. Informes de salida
  3. Cintas magnéticas
  4. Discos removibles
  5. Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor)
  6. Listados de programas
  7. Datos de prueba
  8. Documentación del sistema
- c) Puede resultar más fácil disponer que todos los medios sean recolectados y eliminados de manera segura, antes que intentar separar los ítems sensibles.
- d) Muchas organizaciones ofrecen servicios de recolección y eliminación de papeles, equipos y medios. Se debe seleccionar cuidadosamente a un contratista apto con adecuados controles y experiencia, en caso de ser requerido.
- e) Cuando sea posible, se debe registrar la eliminación de los ítems sensibles, a fin de mantener una pista de auditoría.

Al acumular medios para su eliminación, se debe considerar el efecto de acumulación, que puede ocasionar que una gran cantidad de información no clasificada se torne más sensible que una pequeña cantidad de información clasificada.

### ***Procedimientos de Manejo de la Información***

Se debe controlar el manejo y almacenamiento de la información para protegerla contra su uso inadecuado o divulgación no autorizada. Dichos controles, deben estar ligados estrictamente a las especificaciones de la *Norma de Clasificación de la Información NS/3.002*.

Se deben tomar en cuenta los siguientes controles adicionales:

- a) Se debe administrar y rotular cada uno de los medios.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.006
--	---	---	---	--------------------------

	<p align="center"><b>NORMA DE GESTIÓN Y SEGURIDAD DE LOS MEDIOS DE ALMACENAMIENTO</b></p> <p align="center"><b>Actualización al 22 de marzo de 2007</b></p>	<p align="center">Pagina <b>3 de 3</b></p>
---	---	--

- b) Se debe restringir el acceso a la información, al personal no autorizado.
- c) Se deben considerar las especificaciones de almacenamiento de medios de información en ambientes adecuados.
- d) Se deben respetar los niveles de clasificación de información en el proceso de distribución de datos.
- e) Se deben marcar y etiquetar las copias de los medios de información, sean magnéticos, ópticos o impresos a fin de que puedan ser advertidas por el receptor.

### ***Seguridad de la Documentación del Sistema***

La documentación del sistema puede contener cierta cantidad de información sensible de procesos, aplicaciones, procedimientos informáticos, estructuras de datos, procesos de autorización, entre otros.

Para asegurar que dicha información sea protegida, deben considerarse los siguientes controles:

- a) La documentación del Sistema debe ser almacenada en un lugar seguro. Es recomendable que sea almacenada de la misma manera que las copias de respaldo.
- b) Sólo pueden acceder a la documentación de los sistemas, el Encargado de Sistemas del CRTP, el Director del CRTP y el Comité de Sistemas.
- c) En caso de ser requerida la participación de terceros, la documentación del sistema, debe ser tratada de manera sensible y de alta confidencialidad.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/06.006
--	---	---	---	--------------------------



	<div> <b>POLÍTICA DE CONTROL DE ACCESOS</b> </div> <div> <b>Actualización al 27 de febrero de 2007</b> </div>	<div> <b>Página</b>   <b>1 de 2</b> </div>
---	---	--

## **1. Propósito y Alcance**

El propósito de la Política de Control de Accesos es el de controlar el acceso a la información de la Facultad de Arquitectura, Artes, Diseño y Urbanismo, impedir el acceso no autorizado a los sistemas de información, proteger los servicios de red, evitar los accesos no autorizados al computador, eliminar el acceso no autorizado a la información contenida en los sistemas de información, detectar actividades no autorizadas, así como garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remotas.

Esta política se aplica a autoridades, docentes, estudiantes, funcionarios administrativos y toda otra persona relacionadas de algún modo a la Facultad.

## **2. Declaración de la Política**

El acceso a la información y los procesos principales de la Facultad deben ser controlados sobre la base de los requerimientos de seguridad y del objetivo de la Facultad.

Se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas y servicios de información de la Facultad.

Los procedimientos deben comprender todas las etapas del ciclo de vida de los accesos de usuario, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren acceso a los sistemas y servicios de información de la Facultad. Se debe conceder especial atención, cuando corresponda, a la necesidad de controlar la asignación de derechos de acceso especial, que permiten a los usuarios privilegiados (programadores, administradores del sistema, etc.) pasar por alto los controles de sistema.

Se debe concientizar a los usuarios de la Facultad acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

Se debe controlar el acceso a los servicios de red de la Facultad, tanto internos como externos. Esto es necesario para garantizar que los usuarios de la Facultad que tengan acceso a las redes y a los servicios de red no comprometan la seguridad de estos servicios, garantizando:

- interfaces adecuadas entre la red de la Facultad y las redes de otras organizaciones, o redes públicas.
- mecanismos de autenticación apropiados para usuarios y equipamiento.
- control de acceso de usuarios a los servicios de información.

Desarrollado por:  Fernando Echavarria	Revisión Dirección del CRTP: Max Arnsdorff	Revisión Dirección de Carrera: Roberto Moreira 28/02/07	Aprobación: Vicedecano Decano	Código:  PS/007
--	--	--	-------------------------------	-----------------------

	<h1 style="text-align: center;">POLÍTICA DE CONTROL DE ACCESOS</h1> <p style="text-align: center;"><b>Actualización al 27 de febrero de 2007</b></p>	<p style="text-align: center;">Pagina 2 de 2</p>
---	--	--

Los mecanismos de seguridad a nivel del sistema operativo de la Facultad deben ser utilizados para restringir el acceso a los recursos del computador. Estas instalaciones deben tener la capacidad de llevar a cabo lo siguiente:

- a) identificar y verificar la identidad y, si fuera necesario, la terminal o ubicación de cada usuario autorizado de la Facultad.
- b) registrar los accesos exitosos y fallidos a los sistemas de la Facultad.
- c) suministrar medios de autenticación apropiados; si se utiliza un sistema de administración de contraseñas, éste debe asegurar la calidad de las mismas.
- d) cuando sea apropiado, restringir el tiempo de conexión de los usuarios.

El acceso lógico al software y a la información de la Facultad debe estar limitado a los usuarios autorizados. Los sistemas de aplicación deben:

- a) controlar el acceso de usuarios a la información y a las funciones de los sistemas de aplicación, de acuerdo con las normas de control de accesos definidas por la Facultad.
- b) brindar protección contra el acceso no autorizado de utilitarios y software del sistema operativo que tengan la capacidad de pasar por alto los controles de sistemas o aplicaciones.
- c) no comprometer la seguridad de otros sistemas con los que se comparten recursos de información.
- d) tener la capacidad de otorgar acceso a la información de la Facultad únicamente al propietario, a otros usuarios autorizados mediante designación formal, o a grupos definidos de usuarios.

Los sistemas de la Facultad deben ser monitoreados para detectar desviaciones con relación a los accesos autorizados y registrar eventos para suministrar evidencia en caso de producirse incidentes relativos a la seguridad.

El monitoreo de los sistemas de la Facultad debe permitir comprobar la eficacia de los controles adoptados y verificar la conformidad con las normas de acceso.

### **3. Cumplimiento**

La presente política debe ser cumplida por todos los usuarios, empleados, contratistas y terceros relacionados de alguna manera con la Facultad.

Desarrollado por:  Fernando Echavarria	Revisión Dirección del CRTP: Max Arnsdorff	Revisión Dirección de Carrera: Roberto Moreira 28/02/07	Aprobación: Vicedecano Decano	Código:  PS/007
--	--	--	-------------------------------	-----------------------

	<h1 style="text-align: center;">NORMA DE MONITOREO DEL ACCESO Y USO DE LOS SISTEMAS (LOG'S)</h1> <p style="text-align: center;">Actualización al 29 de marzo de 2007</p>	<p>Página 1 de 2</p>
---	--	--------------------------

## **1. Objetivo**

Establecer los lineamientos para detectar actividades no autorizadas en el acceso y uso de los sistemas de información de la Facultad.

## **2. Alcance**

Esta norma incluye a todos los sistemas de información de la Facultad.

## **3. Responsables**

Es responsable del registro de logs de auditoría sobre el monitoreo para el acceso y uso de los sistemas de información, el Encargado de Sistemas del CRTP.

## **4. Definición de la Norma**

Deben generarse registros de auditoría (logs) que contengan excepciones y otros eventos relativos a la seguridad, considerados necesarios. Estos deben mantenerse durante un período definido para acceder los mismos durante futuras revisiones o cuando se detecta un cambio no autorizado en el sistema.

Los registros de auditoría deben incluir, al menos, los siguientes aspectos:

- a) Identificación de usuario (ID)
- b) Fecha y hora del hecho.
- c) Identificación de la estación de trabajo, si es posible.
- d) Registro de intentos fallidos de acceso al sistema de gestión.
- e) Registro de intentos fallidos de acceso a datos y otros recursos, si es posible.
- f) Registro de cambios realizados en el sistema de gestión.

### ***Monitoreo del uso de los sistemas***

Deben tomarse en cuenta los siguientes aspectos para realizar el monitoreo del uso de los sistemas de información de la Facultad:

- a) Acceso no autorizado, en caso de presentarse.
- b) Todas las operaciones con privilegios especiales.
- c) Intentos de acceso no autorizado.
- d) Alertas o fallas del sistema.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/07.007
--	---	---	---	--------------------------

	<p><b>NORMA DE MONITOREO DEL ACCESO Y USO DE LOS SISTEMAS (LOG'S)</b></p> <p><b>Actualización al 29 de marzo de 2007</b></p>	<p>Página 2 de 2</p>
---	--	--------------------------

Se debe revisar periódicamente el resultado de las actividades de monitoreo. La frecuencia de la revisión debe depender de los riesgos involucrados. Entre los factores de riesgo que deben considerarse, se encuentran los siguientes:

- a) La criticidad de los procesos de aplicaciones.
- b) El valor, la sensibilidad o criticidad de la información involucrada.
- c) La experiencia acumulada en materia de infiltración y uso inadecuado de los sistemas.

### **Registro y revisión de eventos**

Al asignar la responsabilidad por la revisión de registros, se debe considerar una separación de funciones entre quienes emprenden la revisión y quienes están siendo monitoreados.

Se debe prestar especial atención a la seguridad de la herramienta de registro, debido a que si se accede a la misma en forma no autorizada, pueden existir variaciones en dichos registros.

### **Sincronización de relojes**

La correcta configuración de los relojes de las computadoras es importante para garantizar la exactitud de los registros de auditoría que pueden requerirse para revisiones o como evidencia en casos disciplinarios.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/07.007
--	---	---	---	--------------------------

	<b>NORMA DE REQUERIMIENTO PARA EL CONTROL DE ACCESOS</b>	Pagina 1 de 2
Actualización al 22 de marzo de 2007		

### **1. Objetivo**

Definir el marco para establecer los requerimientos de la Facultad, en relación al control de acceso a la información.

### **2. Alcance**

Esta norma abarca a todos los sistemas e información de la Facultad.

### **3. Responsables**

Es responsable de cumplir esta norma todo el personal del Área de Sistemas de la Facultad.

### **4. Definición de la Norma**

Se deben definir y documentar los requerimientos de la Facultad para el control de accesos. Las reglas y derechos del control de accesos, para cada usuario o grupo de usuarios, deben ser claramente establecidos. Se debe otorgar a los usuarios y proveedores de servicio una clara enunciación de los requerimientos que deberán satisfacer los controles de acceso.

Se debe incluir lo siguiente:

- a) Requerimientos de seguridad de cada una de las aplicaciones.
- b) Identificación de toda información relacionada con las aplicaciones.
- c) Las normas de divulgación de información y los niveles de seguridad y la clasificación de información (Ver *Norma de Clasificación de la Información NS/3.002*).
- d) Coherencia entre las normas de control de acceso y de clasificación de información de los diferentes sistemas y redes (Ver *Norma de Clasificación de la Información NS/3.002*, *Norma de Control de Acceso a la red NS/7.004*, *Norma de Control de Accesos al Sistema Operativo NS/7.005* y *Norma de Control de acceso a las aplicaciones NS/7.006*).
- e) Legislación aplicable y obligaciones contractuales con respecto a la protección del acceso a datos y servicios.
- f) Perfiles de acceso de usuarios estándar, comunes a cada categoría de puestos de trabajo.
- g) Gestión de derechos de acceso en un ambiente distribuido y de red el cual reconoce todos los tipos de conexiones disponibles.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/07.001
--	--	---	---	--------------------------

	<b>NORMA DE REQUERIMIENTO PARA EL CONTROL DE ACCESOS</b>	Pagina 2 de 2
Actualización al 22 de marzo de 2007		

### ***Reglas de control de acceso***

Al especificar las reglas de control de acceso, se debe considerar cuidadosamente lo siguiente:

- a) Diferenciar entre reglas que siempre deben imponerse y reglas optativas o condicionales.
- b) Establecer reglas sobre la base de la premisa “Qué debe estar generalmente prohibido a menos que se permita expresamente”, antes que la regla más débil “Todo esta generalmente permitido a menos que se prohíba expresamente”.
- c) Los cambios en los rótulos de información que son iniciados automáticamente por los sistemas de procesamiento de información y aquellos iniciados por el usuario según su criterio.
- d) Los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos iniciados por el Encargado de Sistemas del CRTP.
- e) Las reglas que requieren la aprobación del Encargado de Sistemas del CRTP o de otros antes de entrar en vigencia y aquellas que no.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/07.001
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE GESTIÓN DE ACCESOS DE USUARIOS</h1>	Pagina 1 de 3
Actualización al 22 de marzo de 2007		

## **1. Objetivo**

Establecer los lineamientos para una adecuada gestión de accesos e impedir el acceso no autorizado a los sistemas de información de la Facultad.

## **2. Alcance**

Esta norma abarca a todos los sistemas, información y usuarios de los sistemas de información de la Facultad.

## **3. Responsables**

Es responsable de cumplir esta norma todo el personal del Área de Sistemas de la Facultad.

El Encargado de Sistemas del CRTP y el personal de sistemas (en caso de existir), es responsable de la adecuada gestión de los accesos de los usuarios de la Facultad.

## **4. Definición de la Norma**

### ***Registro de usuarios***

Debe existir un procedimiento formal de registro y borrado de usuarios para otorgar acceso a todos los sistemas y servicios de información de la Facultad.

El acceso a servicios de información debe ser controlado a través de un proceso formal de registro de usuarios, el cual debe incluir los siguientes aspectos:

- a) Utilizar IDs (Identificadores de Usuario) únicos de manera que se pueda vincular y hacer responsables a los usuarios por sus acciones. Utilizar el primer dígito del nombre seguido del apellido de la persona, en todos los casos.
- b) Verificar que el usuario tiene autorización del responsable del sistema para el uso del sistema o servicio de información. También será necesaria una aprobación de derechos de acceso por parte del responsable del área.
- c) Verificar que el nivel de acceso otorgado es adecuado para el propósito de la Facultad y es coherente con la política de seguridad de la Facultad.
- d) Entregar a los usuarios un detalle escrito de sus derechos de acceso.
- e) Requerir que los usuarios firmen declaraciones señalando que comprenden las condiciones para el acceso.
- f) Garantizar que el Área de Sistemas no otorga acceso hasta que se hayan completado los procedimientos de autorización.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/07.002
--	---	---	---	--------------------------

	<b>NORMA DE GESTIÓN DE ACCESOS DE USUARIOS</b>	<b>Página</b>  <b>2 de 3</b>
	<b>Actualización al 22 de marzo de 2007</b>	

- g) Mantener un registro formal de todas las personas registradas para utilizar el servicio.
- h) Cancelar inmediatamente los derechos de accesos de los usuarios que cambiaron sus tareas o se desvincularon de la Facultad.
- i) Evitar tener IDs y cuentas de usuarios redundantes. En caso de presentarse el caso, utilizar adicionalmente la letra del segundo nombre o del segundo apellido para identificar al usuario.

Se debe considerar la inclusión de cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o las personas que prestan un servicio intentan accesos no autorizados.

### ***Gestión de privilegios***

Se debe limitar y controlar la asignación y uso de privilegios (cualquier característica o servicio de un sistema de información que permita que el usuario pase por alto los controles de sistemas o aplicaciones). El uso inadecuado de los privilegios del sistema resulta frecuentemente el más importante factor que contribuye a la falta de los sistemas a los que se ha accedido ilegalmente.

Los sistemas deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes aspectos:

- a) Deben identificarse los privilegios asociados a cada producto del sistema (sistema operativo, sistema de gestión de base de datos y aplicaciones).
- b) Los privilegios deben asignarse al personal sobre las bases de la necesidad de uso.
- c) Se debe mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso de autorización.
- d) Se debe promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

### ***Gestión de contraseñas de usuarios***

Las contraseñas constituyen el primer medio de validación de la identidad de un usuario para acceder a un sistema o servicio de información. La asignación de contraseñas debe controlarse a través de un proceso de gestión formal, mediante el cual debe llevarse a cabo lo siguiente:

- a) Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/07.002
--	---	---	---	--------------------------



	<b>NORMA DE GESTIÓN DE ACCESOS DE USUARIOS</b>	Pagina 3 de 3
Actualización al 22 de marzo de 2007		

- b) Garantizar que los usuarios mantengan sus propias contraseñas, que se provea inicialmente a los mismos de una contraseña provisoria, que deberán cambiar de inmediato.

Las contraseñas nunca deben ser almacenadas en sistemas informáticos sin protección.

#### ***Revisión de derechos de acceso de usuario***

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Encargado de Sistemas del CRTP conjuntamente el Director del CRTP debe llevar a cabo un proceso formal a intervalos regulares, a fin de revisar los derechos de acceso de los usuarios, de manera tal que:

- a) Los derechos de acceso de los usuarios se revisen a intervalos regulares (12 meses) y después de cualquier cambio.
- b) Las autorizaciones de privilegios especiales de derechos de acceso se revisen a intervalos más frecuentes (6 meses).
- c) Las asignaciones de privilegios se verifiquen a intervalos regulares, a fin de garantizar que no se obtengan privilegios no autorizados.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/07.002
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE RESPONSABILIDAD DE USUARIOS (CONTRASEÑAS)</h1>	<p>Página 1 de 2</p>
<p style="text-align: center;">Actualización al 22 de marzo de 2007</p>		

## **1. Objetivo**

Establecer los aspectos a ser tomados en cuenta en la selección y uso de contraseñas (password).

## **2. Alcance**

Esta norma abarca a todo el personal de la Facultad que deba hacer uso de una cuenta de usuario y una contraseña para ingresar a la red y/o a un Sistema Aplicativo.

## **3. Responsables**

Es responsable del cumplimiento de dicha norma todo usuario que utilice una cuenta de acceso y contraseña para ingresar a los sistemas de la Facultad.

## **4. Definición de la Norma**

### ***Uso de contraseñas***

Las contraseñas constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, servicios o sistemas de procesamiento de información. Pueden ser estos accesos a la red o a algún sistema de aplicación.

Los siguientes aspectos deben ser de conocimiento de los usuarios:

- a) Mantener la contraseña en secreto.
- b) Evitar mantener un registro escrito en papel de las contraseñas, a menos que este pueda ser almacenado en forma segura.
- c) Cambiar las contraseñas siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.
- d) Seleccionar contraseñas de calidad, con las siguientes características:
  1. La longitud debe ser de 8 caracteres como mínimo.
  2. Debe contener por lo menos un carácter especial (+, -, \*, /, @, \_, -).
  3. Debe contener por lo menos una letra mayúscula.
  4. Deben ser fáciles de recordar.
  5. No deben basarse en datos fácilmente deducibles, por ejemplo nombres, números telefónicos, fechas de nacimiento, etc.
  6. No deben tener caracteres idénticos consecutivos.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/07.003
--	--	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE RESPONSABILIDAD DE USUARIOS (CONTRASEÑAS)</h1>	Pagina 2 de 2
Actualización al 22 de marzo de 2007		

- e) Cambiar las contraseñas a intervalos regulares, evitando la reutilización de viejas contraseñas controlando que no se repitan las 3 últimas utilizadas.
- f) Obligar el cambio de contraseña asignada en el primer inicio de sesión ("log on")
- g) No incluir contraseñas en los procesos automatizados de inicio de sesión.
- h) No compartir las contraseñas individuales de usuario.

En caso de presentarse evidencias sospechosas de intentos de utilización de las cuentas de usuarios, la persona debe realizar el cambio de contraseña inmediatamente.

### ***Equipos desatendidos en áreas de usuarios***

Los usuarios deben garantizar que los equipos desatendidos sean protegidos adecuadamente. Los equipos instalados en áreas de usuarios, por ejemplo, estaciones de trabajo o servidores de archivos, pueden requerir una protección específica contra accesos no autorizados, cuando se encuentran desatendidos durante un período extenso. Se debe concientizar a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus responsabilidades por la implementación de dicha protección. Se debe notificar a los usuarios que deben cumplir con los siguientes puntos:

- a) Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla resguardado por contraseña.
- b) Llevar a cabo el procedimiento de salida de todos los sistemas cuando finaliza la sesión (no sólo apagar la PC).
- c) Proteger las PC contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso, cuando no se utilizan.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/07.003
--	---	---	---	--------------------------

	<p align="center"><b>NORMA DE CONTROL DE ACCESO A LA RED</b></p> <p align="center">Actualización al 22 de marzo de 2007</p>	<p align="center">Pagina 1 de 2</p>
---	---	---

### **1. Objetivo**

Proteger la red y los servicios de red de la Facultad.

### **2. Alcance**

Esta norma incluye a todo el personal de la Facultad y eventuales debidamente autorizados, que hagan uso de la red de computadoras y sus servicios.

### **3. Responsables**

Son responsables de su cumplimiento todos los usuarios que utilicen la red de la Facultad.

### **4. Definición de la Norma**

Es importante que todos los usuarios cuenten con accesos directos a los servicios autorizados dentro de la red de la Facultad, cualquier conexión no segura debe ser restringida debido a que puede afectar a toda la Facultad.

El control se debe aplicar a los sistemas de aplicación o módulos individuales, clasificados como sensibles, confidenciales o críticos, en todas las instalaciones de la Facultad.

El control se debe ejercer sobre el uso de la red y sus servicios, y debe comprender:

- a) Las redes y servicios de red a los cuales se permite el acceso.
- b) Procedimientos de autorización para determinar los permisos de acceso a los usuarios.
- c) Controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

Se debe controlar el camino desde la terminal de usuario hasta el servicio de red. Las redes están diseñadas para permitir el máximo alcance de distribución de recurso y flexibilidad. Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones o para el uso no autorizado de los servicios de información. Estos riesgos pueden reducirse mediante la incorporación de controles, que limiten la ruta entre el equipo del usuario y los servicios habilitados en la red, a los cuales los usuarios están autorizados para su acceso. El crear un camino forzoso de ingreso es una buena práctica que debe utilizarse en caso de ser necesario.

El objetivo de un camino forzoso es evitar que los usuarios seleccionen rutas fuera de la trazada entre la terminal de usuario y los servicios a los cuales el mismo está autorizado a

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/07.004
--	--	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE CONTROL DE ACCESO A LA RED</h1>	Pagina 2 de 2
Actualización al 22 de marzo de 2007		

acceder. Limitando las opciones de ruteo en cada punto de la red, a través de elecciones predefinidas, se pueden ejercer puntos de control como:

- a) Gateways a sistemas de aplicación específicos y a usuarios externos de la red.
- b) Limitar opciones de menú y submenú de cada usuario.
- c) Evitar la navegación ilimitada por la red.
- d) Controlar las comunicaciones con origen y destino autorizado a través de firewalls.
- e) Restringir el acceso a redes, estableciendo dominios lógicos separados, por ejemplo, redes privadas virtuales para grupos de usuarios dentro de la Fundación.

El acceso de usuarios remotos debe estar sujeto a la autenticación y a la aprobación del Comité de Sistemas, debido a que estos son potencialmente peligrosos para los accesos no autorizados.

Existen diferentes métodos de autenticación, algunos brindan un mayor nivel de protección que otros, por ejemplo, los métodos basados en el uso de técnicas criptográficas puede proveer una fuerte autenticación. Es importante determinar mediante una evaluación de riesgos el nivel de protección requerido para la Facultad.

Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación de la Facultad. Por consiguiente las conexiones remotas a sistemas informáticos, deben ser autenticadas y previamente autorizadas.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/07.004
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE CONTROL DE ACCESO AL SISTEMA OPERATIVO</h1>	<p>Página 1 de 3</p>
	<p style="text-align: center;">Actualización al 29 de marzo de 2007</p>	

## **1. Objetivo**

Proteger los servidores, las estaciones de trabajo y equipos de computación para evitar el acceso no autorizado a los Sistemas Operativos.

## **2. Alcance**

La presente norma afecta a todos los empleados de la Facultad y terceros que tengan acceso a los activos físicos de información.

## **3. Responsables**

Son responsables de su cumplimiento todos los usuarios que tengan acceso a los servidores de la Facultad o a las estaciones de trabajo.

## **4. Definición de la Norma**

### ***Identificación de estaciones de trabajo***

Se debe tener en cuenta la identificación automática de estaciones de trabajo para autenticar conexiones a ubicaciones específicas y equipamiento portátil. Dicha identificación es importante cuando se restringe el ingreso a equipos específicos, y las autorizaciones que se tienen sobre los equipos. Es necesario aplicar la protección física, a fin de mantener la seguridad del identificador de la misma.

### ***Control de conexión de estaciones de trabajo***

El control de conexión al Sistema Operativo Microsoft Windows XP, debe minimizar la oportunidad de acceso no autorizado, divulgar la mínima información posible acerca del sistema, evitando así proveer de asistencia innecesaria a un usuario no autorizado.

El proceso de identificación debe contemplar:

- a) Definir perfiles y políticas de usuario en el Sistema Operativo.
- b) No desplegar identificadores de sistemas o aplicaciones hasta que se haya llevado a cabo exitosamente el proceso de conexión.
- c) Evitar procesos de ayuda para impedir la asistencia a un usuario no autorizado durante el proceso de conexión.
- d) Validar la información únicamente cuando se hayan completado los datos de entrada. Si surge un error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/07.005
--	--	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE CONTROL DE ACCESO AL SISTEMA OPERATIVO</h1>	Pagina 2 de 3
Actualización al 29 de marzo de 2007		

- e) Limitar el número de conexiones no exitosas permitidas a 3, registrando los intentos no exitosos, implementando una demora obligatoria antes de permitir otros intentos de identificación o rechazar otros intentos sin autorización específica, o en su caso, deshabilitando la conexión.
- f) Desplegar la información de fecha y hora de conexión exitosa anterior y detalles de los intentos de conexión no exitosos desde la última conexión exitosa, al completarse una conexión exitosa.

### ***Identificación y autenticación de los usuarios***

Todos los usuarios, así como el personal de sistemas, deben tener un identificador único (ID de usuario) solamente para uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad.

Los identificadores de usuario no deben dar ningún indicio del nivel de privilegio, entendiéndose como privilegio, el nivel de autorización y libertad de acción que es asignado por medio del Sistema Operativo.

Existen diversos procedimientos de autenticación, los cuales pueden ser utilizados para sustentar la identidad del usuario. Las contraseñas constituyen un medio muy común para proveer la identificación y autenticación sobre la base de un secreto que sólo conoce el usuario.

### ***Sistema de gestión de contraseñas***

Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático. Los sistemas de gestión de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad.

Las contraseñas deben ser seleccionadas y mantenidas por los usuarios de la Facultad.

Un buen sistema de gestión de contraseñas debe:

- a) Imponer el uso de contraseñas para determinar responsabilidades.
- b) Permitir que los usuarios seleccionen y cambien sus propias contraseñas e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
- c) Imponer una selección de contraseñas de calidad.
- d) Imponer cambios en las contraseñas.
- e) Obligar al cambio de contraseñas en su primer procedimiento de identificación.
- f) Mantener un registro de las contraseñas previas utilizadas por el usuario, y evitar la reutilización de las mismas.
- g) No mostrar las contraseñas en pantalla cuando estas sean ingresadas.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/07.005
--	--	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE CONTROL DE ACCESO AL SISTEMA OPERATIVO</h1>	Pagina 3 de 3
Actualización al 29 de marzo de 2007		

- h) Almacenar en forma separada los archivos de contraseñas y los datos de sistema de aplicación.
- i) Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.
- j) Modificar las contraseñas predeterminadas por el proveedor una vez instalada la aplicación.
- k) Debe elaborarse un procedimiento de creación, modificación, eliminación y resguardo de contraseñas que permita mantener esta información sensible en lugares de alta seguridad de Facultad.

### ***Uso de utilitarios sensitivos de sistema***

La mayoría de las instalaciones informáticas tienen uno o más programas utilitarios sensitivos que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Si se presenta el caso, es esencial que su uso, en la Facultad, sea limitado y minuciosamente controlado. Se deben considerar los siguientes controles:

- a) Uso de procedimientos de autenticación para utilitarios sensitivos del sistema.
- b) Limitación de uso de utilitarios sensitivos del sistema a la cantidad mínima viable de usuarios autorizados.
- c) Autorización para uso de utilitarios sensitivos de sistema según roles definidos en el Sistema Operativo Windows.
- d) Limitación de disponibilidad de utilitarios sensitivos de sistema.
- e) Registro de todo uso de utilitarios sensitivos del sistema.
- f) Remoción o inhabilitación de todo el software basado en utilitarios sensitivos y software de sistema innecesarios.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/07.005
--	---	---	---	--------------------------



	<h1 style="text-align: center;">NORMA DE CONTROL DE ACCESO A LAS APLICACIONES</h1> <p style="text-align: center;">Actualización al 29 de marzo de 2007</p>	<p>Página 1 de 1</p>
---	--	--------------------------

## **1. Objetivo**

Establecer los lineamientos para controlar el acceso a las aplicaciones impidiendo el acceso no autorizado a la información contenida en los sistemas de información de la Facultad.

## **2. Alcance**

La presente norma afecta a todo el personal de la Facultad que haga uso de los sistemas informáticos de la misma.

## **3. Responsables**

Son responsables de su cumplimiento todos los funcionarios de la Facultad que utilizan los sistemas informáticos para el cumplimiento de sus funciones.

## **4. Definición de la Norma**

### ***Restricciones del acceso a la información***

Los usuarios de los sistemas de aplicación, con inclusión del personal de apoyo, deben tener acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la política de control de acceso definida (*Ver Política de Control de Accesos PS/007*), y sobre la base de requerimientos de cada aplicación.

Para brindar apoyo a los requerimientos de limitación de accesos se debe tener en cuenta los siguientes controles:

- a) Asignación de menús adecuados para el manejo de la información.
- b) Restricción del conocimiento de los usuarios acerca de la información o funciones de los sistemas a los cuales no sean autorizados a acceder, con la adecuada edición de funciones de usuarios.
- c) Control de los derechos de acceso de los usuarios a lectura, escritura, supresión y ejecución.
- d) Garantizar que las salidas (outputs) de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las ubicaciones autorizadas, revisando periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/07.006
--	---	---	---	--------------------------

	<p style="text-align: center;"><b>POLÍTICA DE SISTEMAS DE INFORMACIÓN, ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO</b></p> <p style="text-align: center;">Actualización al 27 de febrero de 2007</p>	<p>Página  1 de 2</p>
---	--	-------------------------------

## **1. Propósito y Alcance**

Busca asegurar, que los procesos de adquisición, desarrollo y mantenimiento de sistemas, incorporen todos los aspectos de seguridad en los sistemas de información de la Facultad de Arquitectura, Artes, Diseño y Urbanismo. Asimismo, prevenir la pérdida, modificaciones o uso inadecuado de los datos del usuario en los sistemas de aplicación, salvaguardando así la confidencialidad, autenticidad e integridad de la información y garantizando que los proyectos de desarrollo y actividades de mantenimiento de sistemas se lleven a cabo de manera segura.

Esta política se aplica a autoridades, docentes, estudiantes, funcionarios administrativos y a terceros responsables de realizar tareas de planificación, desarrollo y mantenimiento de los sistemas de información.

## **2. Declaración de la Política**

Las etapas de Análisis, Relevamiento de requerimientos y Diseño de los Sistemas, son de muy alta sensibilidad respecto a la definición de las características de seguridad que se deben garantizar, de ahí que, los requerimientos de seguridad deben ser identificados y aprobados antes del desarrollo de los sistemas de información de la Facultad. En el caso de tener ya un sistema desarrollado, se deben hacer los ajustes necesarios para garantizar los requerimientos de seguridad.

Todos los requerimientos de seguridad en la Facultad, deben ser identificados en la fase de Análisis y determinación de requerimientos de un proyecto de desarrollo y deben ser justificados, aprobados y documentados como una parte de la totalidad del proyecto de un sistema de información.

Se deben diseñar en los sistemas de aplicación de la Facultad, controles apropiados y pistas de auditoria o registros de actividad. Esto debe incluir la validación de datos de entrada, procesamiento interno y salida de datos.

Todos los sistemas de información desarrollados por el Área de Computación y aquellos adquiridos de terceros, deben responder a una metodología de desarrollo y deben ser sometidos a una evaluación en base a normas de calidad de software.

Deben utilizarse, en la Facultad, sistemas y técnicas criptográficas para la protección de la información que se considera en estado de riesgo y para la cual otros controles no suministran una adecuada protección.

Desarrollado por:  Fernando Echavarria	Revisión Dirección del CRTP: Max Arnsdorff	Revisión Dirección de Carrera: Roberto Moreira 1/03/07	Aprobación: Vicedecano Decano	Código:  PS/008
--	--	---	-------------------------------	-----------------------

	<p style="text-align: center;"><b>POLÍTICA DE SISTEMAS DE INFORMACIÓN, ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO</b></p> <p style="text-align: center;"><b>Actualización al 27 de febrero de 2007</b></p>	<p><b>Página</b> <b>2 de 2</b></p>
---	---	--

Se debe controlar el acceso a los archivos de los sistemas de la Facultad. El mantenimiento de la integridad del sistema debe ser responsabilidad de la función usuaria o grupo de desarrollo a quien pertenece el software o sistema de aplicación.

Se deben controlar estrictamente los entornos de desarrollo de proyectos y el soporte o mantenimiento a los mismos. Los funcionarios responsables de los sistemas de aplicación de la Facultad también son responsables de la seguridad de los ambientes de desarrollo y mantenimiento de proyectos informáticos. Los funcionarios responsables deben garantizar que todos los cambios propuestos para el sistema sean revisados, a fin de comprobar que los mismos no comprometen la seguridad del sistema o del ambiente operativo.

Todos los sistemas de información desarrollados por o para la Facultad, deben contar con la documentación técnica y de usuario formalmente desarrollada y aprobada por las instancias correspondientes, para garantizar la posibilidad de mantenimiento y el correcto uso por parte de los usuarios de los sistemas de información.

### **3. Cumplimiento**

La presente política debe ser cumplida principalmente por el personal del Área de Computación, involucrado en las tareas de desarrollo y mantenimiento de sistemas de información y por todos los usuarios, empleados, contratistas y terceros relacionados de alguna manera con la Facultad.

Desarrollado por:  Fernando Echavarria	Revisión Dirección del CRTP: Max Arnsdorff	Revisión Dirección de Carrera: Roberto Moreira 1/03/07	Aprobación: Vicedecano Decano	Código:  PS/008
--	--	---	-------------------------------	-----------------------

	<p align="center"><b>NORMA DE SEGURIDAD DE LOS PROCESOS DE DESARROLLO Y SOPORTE</b></p> <p align="center"><b>Actualización al 4 de abril de 2007</b></p>	<p align="center">Pagina <b>1 de 3</b></p>
---	--	--

## **1. Objetivo**

Establecer los lineamientos para mantener la seguridad del software y la información de los sistemas de aplicación de la Facultad.

## **2. Alcance**

Esta norma abarca al personal involucrado en el desarrollo de sistemas, a fin de controlar estrictamente el entorno en el cual se desarrollan y se realizan las actualizaciones del o los sistemas en producción.

## **3. Responsables**

El directo responsable por mantener la seguridad del software y el soporte, es el Encargado de Sistemas del CRTP, quien debe garantizar que todos los cambios propuestos en los Sistemas en producción, sean revisados y se compruebe que los mismos no comprometen la seguridad del sistema ni las operaciones de la Facultad.

## **4. Definición de la Norma**

Los sistemas de información de la Facultad pueden llegar a requerir cambios sustanciales en determinado momento, debido a diversos motivos que surjan de los requerimientos propios de los usuarios, de las condiciones de la Universidad o de las estrategias de la Facultad.

Para minimizar la alteración de los sistemas de información, se debe establecer un control que permita tener un adecuado seguimiento a los cambios, que garanticen el cumplimiento de las normas y procedimientos de seguridad y que el personal de desarrollo y programación debe respetar.

Se debe garantizar que los programadores sólo tengan acceso a aquellas partes del sistema necesarias para el desempeño de sus tareas, en base a los controles cruzados previstos para el pase a producción de los sistemas y cambios, y la autorización correspondiente del Comité de Sistemas.

Si los cambios a ser implementados afectaran las operaciones de la Facultad, antes de ponerlos en marcha se debe difundir, divulgar y entrenar al personal operativo involucrado, para reducir impactos no deseados en la continuidad de las operaciones de la Facultad.

Para reducir los efectos no deseados, garantizar los niveles de seguridad y otros aspectos mencionados anteriormente, se debe incluir en el control, lo siguiente:

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/08.005
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE SEGURIDAD DE LOS PROCESOS DE DESARROLLO Y SOPORTE</h1>	Pagina 2 de 3
Actualización al 4 de abril de 2007		

- a) Se debe mantener un registro de los niveles de autorización acordados.
- b) Verificar que los cambios propuestos por los usuarios están debidamente autorizados.
- c) Se deben revisar los procedimientos y controles, para garantizar que no serán comprometidos por los cambios.
- d) Identificar y documentar todo el software, información, entidades de bases de datos y el hardware que se requiere.
- e) Obtener aprobaciones formales para las propuestas detalladas, antes de dar inicio a los cambios.
- f) Se debe obtener la satisfacción formal de los usuarios involucrados, antes de implementar o pasar a producción los cambios.
- g) Se deben seguir los lineamientos de pase a producción, a fin de garantizar que las operaciones normales de la Facultad, no sean interrumpidas por el cambio a ser implementado, tomando en cuenta los tiempos más adecuados para la ejecución de dicha tarea.
- h) Cada cambio concluido, debe ser documentado y se debe actualizar la documentación de los sistemas o módulos involucrados, manuales de usuario, técnicos, etc., archivando y actualizando la documentación anterior.
- i) Se debe mantener un adecuado control de versiones, en tal caso, es necesario realizar las copias de respaldo necesarias, antes de la puesta en marcha de los cambios.
- j) Se deben mantener pistas de auditoría de todas las solicitudes de cambios y las acciones adoptadas en cada caso.

### ***Revisión técnica de los cambios en el sistema operativo***

En caso de requerirse realizar cambios de sistema operativo en el servidor de producción, sea por la reinstalación del sistema operativo, instalación de una nueva versión, o parches de actualización, los sistemas de información deben ser revisados y probados, para garantizar que dichos cambios no afecten las operaciones en el momento de ser ejecutados.

Las pruebas deben ser realizadas en el servidor de desarrollo, con la intervención de usuarios en escenarios de prueba que reflejen una simulación real, a fin de obtener la satisfacción de los mismos, ante los cambios a ser realizados.

### ***Pase a Producción***

En caso de requerir instalar en el servidor de producción, nuevos sistemas de información, actualizaciones, adecuaciones, modificaciones, instalaciones de parches del sistema de información, entre otros, efectuados en el servidor de desarrollo, se debe tener en cuenta que una vez que se hayan probado y respaldado formalmente el éxito de las pruebas por parte de los usuarios, las implementaciones deben ser pasadas al servidor de producción.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/08.005
--	---	---	---	--------------------------

	<p align="center"><b>NORMA DE SEGURIDAD DE LOS PROCESOS DE DESARROLLO Y SOPORTE</b></p> <p align="center"><b>Actualización al 4 de abril de 2007</b></p>	<p align="center">Pagina <b>3 de 3</b></p>
---	--	--

Una vez realizadas las pruebas y ajustes correspondientes y en caso de resultar factible la implementación del cambio y nuevo software en el servidor de producción, el mismo debe ser realizado por el Encargado de Sistemas del CRTP, bajo la supervisión del Director del CRTP, para garantizar que las acciones estén libres de posible fraude informático o errores involuntarios ocasionados en áreas del servidor de producción.

### ***Restricción del cambio en los paquetes del software***

En caso de requerir cambios en los módulos de los sistemas de la Facultad, se deben analizar diferentes aspectos y enfatizar en los efectos de riesgo en materia de seguridad y en las consecuencias económicas que los mismos pueden ocasionar. Dichos aspectos a considerar son:

- a) Se debe evaluar el riesgo de compromiso de los procesos y controles incorporados.
- b) Se debe obtener la justificación del requerimiento por parte de los usuarios involucrados y la autorización correspondiente.
- c) En caso de tratarse de proveedores de software, evaluar la posibilidad de obtener los cambios requeridos y el impacto económico.
- d) El impacto de asumir la responsabilidad del mantenimiento futuro del sistema, en caso de productos adquiridos de terceros y del software propio.

Si los cambios son esenciales, se debe hacer una copia de respaldo de la versión original o anterior y realizar los cambios sobre ésta, misma que debe estar claramente identificada.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/08.005
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE REQUERIMIENTO DE SEGURIDAD DE LOS SISTEMAS</h1>	Pagina  1 de 1
Actualización al 4 de abril de 2007		

## **1. Objetivo**

Asegurar que los Sistemas de Información de la Facultad contemplan aspectos de Seguridad.

## **2. Alcance**

Esta norma abarca todos los sistemas de información de la Facultad.

## **3. Responsables**

Es responsable de la seguridad el Encargado de Sistemas del CRTP debiendo considerar su importancia en la fase de requerimiento de un proyecto. Asimismo los responsables de las áreas usuarias que solicitan el proyecto, si se diera el caso.

## **4. Definición de la Norma**

Considerar un Sistema de Información seguro, ya sea en su infraestructura, en la aplicación de sistemas asimilados o aplicaciones desarrolladas internamente es de crucial importancia para la Facultad. Su enfoque debe ser priorizado en la fase de requerimiento de un nuevo proyecto, y los requerimientos de seguridad deben ser identificados y justificados, aprobados y documentados como una parte de la totalidad del caso del tratamiento del Sistema.

### ***Análisis y especificaciones de los requerimientos de seguridad***

Los requerimientos de nuevas aplicaciones o mejoras a los sistemas existentes deben especificar la necesidad de controles. Tales especificaciones deben considerar los controles automáticos a incorporar al sistema y la necesidad de controles manuales de apoyo. Se deben aplicar consideraciones similares para evaluar paquetes de software para nuevas aplicaciones.

Los requerimientos de seguridad y los controles, deben reflejar el costo comercial o costo horas/hombre de los recursos de información involucrados y el potencial daño al negocio que pudiera resultar de una falla o falta de seguridad. El marco para analizar los requerimientos de seguridad e identificar los controles que los satisfagan son la evaluación y la gestión de riesgo.

Los controles establecidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/08.001
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE SEGURIDAD EN LOS SISTEMAS DE APLICACION</h1>	Pagina 1 de 3
	Actualización al 4 de abril de 2007	

## **1. Objetivo**

Establecer los mecanismos de seguridad en los sistemas de aplicación de la Facultad para prevenir la pérdida, modificaciones o uso inadecuado de los datos del usuario en los sistemas de aplicación.

## **2. Alcance**

Esta norma incluye todos los sistemas de aplicación de la Facultad.

## **3. Responsables**

El Encargado de Sistemas del CRTP es responsable de la verificación de la utilización de herramientas de control en los sistemas de aplicación.

## **4. Definición de la Norma**

Sistemas de aplicación son los sistemas ya implementados.

Las herramientas de control que deben ser incluidas en dichos sistemas son las pistas de auditoría o registros de actividad, registrando las validaciones de datos de entrada, procesamiento interno y salidas de datos.

Pueden ser necesarios controles adicionales para sistemas que procesan o tienen impacto en recursos sensitivos, valiosos o críticos de la Facultad. Tales controles deben ser determinados sobre la clase de requerimientos de seguridad y evaluación de riesgo.

### ***Validación de datos de entrada***

Los datos de entrada en las aplicaciones deben ser validados para asegurar que son correctos y apropiados. Los controles deben ser aplicados a las entradas de las transacciones, datos de referencia y tablas de parámetros. Se debe considerar los siguientes controles:

- a) Controles de entrada para detectar los siguientes errores:
  - a. Valores fuera de rango.
  - b. Caracteres inválidos en campos de datos.
  - c. Datos faltantes o incompletos.
  - d. Volúmenes de datos que exceden los límites superiores e inferiores determinados.
  - e. Controles de datos no autorizados o inconsistentes.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/08.002
--	---	---	---	--------------------------



	<h1 style="text-align: center;">NORMA DE SEGURIDAD EN LOS SISTEMAS DE APLICACION</h1>	Pagina 2 de 3
	Actualización al 4 de abril de 2007	

- b) Revisión periódica de los contenidos de campos clave o archivos de datos para confirmar su validez e integridad.
- c) Inspección de los documentos de entrada para detectar cambios no autorizados en los datos de entrada.
- d) Procedimientos para responder a errores de validación.
- e) Procedimientos para determinar la autenticidad de los datos.
- f) Determinación de las responsabilidades de todo el personal involucrado en el proceso de entrada de datos.

### ***Controles de Procesamiento interno***

Los datos que han sido correctamente ingresados pueden contaminarse al procesar errores o a través de actos deliberados. Los controles de validación deben ser incorporados a los sistemas para detectar tal corrupción. El diseño de aplicaciones debe asegurar que las restricciones se implementen para minimizar los riesgos de fallas de procesamiento, evitando una pérdida de integridad. Se debe considerar como áreas de riesgo a:

- a) El uso y localización dentro de los programas de funciones de adición y borrado para cambios en los datos.
- b) Procedimientos para prevenir la ejecución de programas fuera de secuencia o fallas en procesamientos previos.
- c) El uso de programas correctos para recuperación de fallas, a fin de garantizar el procesamiento correcto de los datos.

Los controles requeridos dependerán de la naturaleza de la aplicación y del impacto de eventuales alteraciones de datos. Entre los ejemplos de verificaciones que pueden ser incorporados se encuentran los siguientes:

- a) Controles de sesión o de lote, utilizados para conciliaciones después de actualizaciones de transacciones.
- b) *Controles de balance, para comparar balances de apertura frente a balances de cierre anteriores, por ejemplo:*
  - a. *Controles ejecución a ejecución.*
  - b. *Totales de actualización de archivos*
  - c. *Controles programa a programa*
- c) Validación de datos de entrada.
- d) Verificación de la integridad de los datos o software transferidos entre computadoras centrales y remotas.
- e) Totales de control de registros y archivos.
- f) Verificaciones para garantizar que las aplicaciones se ejecutan en el momento correcto.
- g) Comprobaciones para garantizar que los programas se ejecutan en el orden correcto y si tienen falla, estos se detienen hasta resolver el problema.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/08.002
--	--	---	---	--------------------------

	<p style="text-align: center;"><b>NORMA DE SEGURIDAD EN LOS SISTEMAS DE APLICACION</b></p> <p style="text-align: center;">Actualización al 4 de abril de 2007</p>	<p>Página 3 de 3</p>
---	---	--------------------------

### ***Validación de datos de salida***

La salida de datos de un sistema de aplicación debe ser validada para garantizar que el procesamiento de la información almacenada sea correcto y adecuado a las circunstancias. Normalmente, los sistemas se construyen suponiendo que si se ha llevado a cabo una validación, verificación y prueba apropiada, la salida siempre será la correcta. Esto no siempre se cumple. La validación de salidas puede incluir:

- a) Comprobación de la relación y veracidad entre los datos estimables y los obtenidos.
- b) Control de conciliación de datos para asegurar que el procesamiento fue correcto.
- c) Provisión de información suficiente, para que el lector o sistema de procesamiento subsiguiente determine la exactitud, totalidad, precisión y clasificación de la información.
- d) Procesamiento para responder a las pruebas de validación de salidas.
- e) Definición de las responsabilidades de todo el personal involucrado en el proceso de salida de datos.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/08.002
--	---	---	---	--------------------------

	<b>NORMA DE CONTROLES CRİPTOGRAFICOS</b>	<b>Pagina</b>  <b>1 de 3</b>
	<b>Actualización al 4 de abril de 2007</b>	

## **1. Objetivo**

Establecer los lineamientos que permitan proteger la confidencialidad, autenticidad o integridad de la información de la Facultad.

## **2. Alcance**

Esta norma incluye a todos los sistemas de gestión de la Facultad, que generen información que requiera ser intercambiada con otras organizaciones.

## **3. Responsables**

Es responsable de su estudio y aplicación en los casos que así lo necesiten el Encargado de Sistemas del CRTP. Los propietarios de información tienen la responsabilidad de identificar los procesos de información que necesiten de dicha técnica.

## **4. Definición de la Norma**

Las técnicas criptográficas de protección de la información, que es considerada en estado de riesgo, deben ser aplicadas cuando otros controles no suministran una adecuada protección.

### ***Utilización de controles criptográficos***

Decidir si una solución criptográfica es apropiada, debe ser visto como parte de un proceso más amplio de evaluación de riesgos y selección de controles, para determinar el nivel de protección que debe darse a la información. Esta evaluación puede utilizarse posteriormente para determinar si un control criptográfico es adecuado, determinando que tipo de control debe aplicarse y con qué propósito acorde a los procesos de la Facultad.

La Facultad debe utilizar los controles criptográficos para la protección de su información.

Al desarrollar los controles criptográficos se debe considerar:

- El enfoque respecto al uso de controles criptográficos, tomando en cuenta los principios generales según los cuales debe protegerse la información de la Facultad.
- El enfoque respecto a la gestión de claves, con inclusión de los métodos para administrar la recuperación de la información cifrada en caso de pérdida, compromiso o daño de claves, con la definición de responsabilidades y funciones respecto a la implementación de dichos controles y la gestión de claves.
- El nivel apropiado de protección criptográfica.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/08.003
--	---	---	---	--------------------------

	<b>NORMA DE CONTROLES CRIPTOGRAFICOS</b>	<b>Pagina</b>  <b>2 de 3</b>
	<b>Actualización al 4 de abril de 2007</b>	

### ***Cifrado***

El cifrado es una técnica criptográfica que puede utilizarse para proteger la confidencialidad de la información. Se debe tener en cuenta para la protección de información sensible, confidencial o crítica, a ser intercambiada con otras organizaciones.

Mediante una evaluación de riesgo se debe identificar el nivel requerido de protección de la información.

### ***Firma digital***

Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos. Pueden aplicarse a cualquier tipo de documento que se procese electrónicamente.

Pueden implementarse utilizando una técnica criptográfica sobre la base de un par de claves relacionadas de manera única, donde una clave se utiliza para crear una firma (la clave privada) y la otra, para verificarla (la clave pública). Se deben tomar recaudos para proteger la confidencialidad de la clave privada. Esta clave debe mantenerse en secreto dado que una persona que tenga acceso a esta clave puede firmar documentos, falsificando la firma del propietario de la clave. Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.

El Comité de Sistemas debe decidir y aprobar el uso de Firmas Digitales.

### ***Gestión de Claves***

#### **Protección de claves criptográficas**

La gestión de claves criptográficas es esencial para el uso eficaz de las técnicas criptográficas.

Cualquier compromiso o pérdida de claves criptográficas, puede conducir a comprometer la confidencialidad, autenticidad, integridad y por tanto la seguridad de la información.

### **Métodos**

Un sistema de gestión de claves debe estar basado en un conjunto de métodos seguros para realizar uno o varios de los siguientes aspectos:

- a) Generar claves para diferentes sistemas criptográficos.


Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/08.003
--	---	---	---	--------------------------

	<b>NORMA DE CONTROLES CRIPTOGRAFICOS</b>	<b>Pagina 3 de 3</b>
<b>Actualización al 4 de abril de 2007</b>		

- b) En caso de ser necesario, generar y obtener certificados de clave pública.
- c) Distribuir claves a los usuarios que corresponda, incluyendo cómo deben activarse las claves cuando se reciben.
- d) Cambiar o actualizar claves, incluyendo reglas sobre cuándo y cómo deben cambiarse las claves.
- e) Revocar claves incluyendo cómo deben retirarse o desactivarse las mismas.
- f) Archivar claves.
- g) Destruir claves.
- h) Registrar claves.

A fin de reducir la probabilidad de compromiso, las claves deben ser utilizadas sólo por un período limitado de tiempo.

<b>Desarrollado por:</b>  Fernando Echavarria	<b>Revisión: Encargado de Sistemas del CRTP:</b> Edson Quispe	<b>Revisión: Dirección del CRTP:</b> Max Arnsdorff	<b>Aprobación:</b> Dirección de Carrera: Roberto Moreira	<b>Código:</b>  NS/08.003
---	--	--	--	---------------------------------

	<h1 style="text-align: center;">NORMA DE SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA</h1>	Pagina 1 de 2
	Actualización al 4 de abril de 2007	

## **1. Objetivo**

Proporcionar los lineamientos necesarios para garantizar que los proyectos y actividades de soporte de Tecnología de la Información se lleven a cabo de manera segura en la Facultad.

## **2. Alcance**

El Encargado de Sistemas del CRTP, el personal de sistemas y las áreas usuarias, deben apoyar a que se cumplan las recomendaciones de seguridad de los archivos del sistema.

## **3. Responsables**

Es responsable de garantizar la seguridad de los archivos del sistema, el Encargado de Sistemas del CRTP, quien definirá los niveles de acceso y permisos sobre los mismos.

El mantenimiento de la integridad del sistema es responsabilidad del Encargado de Sistemas del CRTP y de los usuarios del sistema.

## **4. Definición de la Norma**


Para realizar el control de los archivos del sistema, se deben considerar las siguientes disposiciones:

### ***Control del software operativo***

Se debe proveer un control para la implementación de software, en los módulos del sistema que está en producción, a fin de minimizar el riesgo de alteración, para lo cual se considerará:

- a) La actualización de las librerías de programas de los módulos del sistema, debe ser realizada cuando sea necesario por el Encargado de Sistemas del CRTP.
- b) Los sistemas en producción, deben mantener únicamente código ejecutable en el Servidor de Producción.
- c) El código fuente de los sistemas de información, no se debe ejecutar o pasar a producción, en tanto no se tenga evidencia del éxito de las pruebas, de la aceptación de los usuarios involucrados y de la aprobación y autorización del Comité de Sistemas.
- d) Se debe mantener un registro de auditoría de todas las actualizaciones de librerías, programas y el sistema en general.
- e) Las versiones anteriores de los sistemas actualizados, deben ser guardadas y respaldadas, como medida de contingencia.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/08.004
--	---	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA</h1>	Pagina 2 de 2
Actualización al 4 de abril de 2007		

Toda decisión tomada con relación a actualizaciones de los sistemas, debe considerar las recomendaciones de seguridad de las políticas y normas establecidas por la Facultad.

Los parches de software, deben aplicarse cuando se evidencie que aquello ayudará a reducir las fallas en materia de seguridad.

### ***Protección de los datos de prueba del sistema***

Los datos de prueba, deben ser protegidos y controlados, ya que las pruebas de aceptación del sistema probado, por lo general requiere volúmenes grandes de información de prueba y que deben ser lo más cercanos posible a los datos reales u operativos.

Se debe evitar utilizar en las pruebas, bases de datos que contenga información personal. En tal caso se debe antes despersonalizar dicha información.

Para proteger los datos, cuando estos son empleados para fines de prueba, deben considerarse los siguientes controles:


- a) El procedimiento de Control de Accesos, que se aplique los Sistema de Información en producción, deben aplicarse también en las pruebas de las actualizaciones.
- b) El Director del CRTP, debe autorizar cada vez que se requiera copiar información operativa al servidor de desarrollo, para fines de prueba.
- c) Cada vez que se haya evidenciado el éxito de las pruebas, la información operativa empleada, debe ser eliminada para evitar accesos no autorizados.
- d) La copia y uso de la información operacional debe ser registrada a fin de contar con pistas de auditoría en este sentido.

### ***Control de acceso a las librerías de programas fuente***

A fin de reducir la probabilidad de alteración de programas fuente, se debe delegar la responsabilidad del acceso a dichos programas al Encargado de Sistemas del CRTP y se deben adoptar los siguientes controles:

- a) Los programas fuente, deben almacenarse únicamente en el Servidor de Desarrollo y nunca en el de Producción.
- b) Únicamente el Encargado de Sistemas del CRTP debe tener acceso a los programas fuente.
- c) Las bibliotecas y programas en desarrollo no deben ser almacenadas en el mismo servidor que los sistemas en operación.
- d) Las versiones pasadas de los programas fuente, se deben almacenar en lugares seguros y con una clara identificación y etiquetado, indicando fechas y horas precisas en las que estaban en producción.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/08.004
--	---	---	---	--------------------------

	<p style="text-align: center;"><b>POLÍTICA DE GERENCIA DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN</b></p> <p style="text-align: center;"><b>Actualización al 27 de febrero de 2007</b></p>	<p>Página  1 de 1</p>
---	---	-------------------------------

## **1. Propósito y Alcance**

La política de gerencia de incidentes de la seguridad de la información pretende contrarrestar las interrupciones de las actividades operativas y proteger los procesos críticos de la Facultad de Arquitectura, Artes, Diseño y Urbanismo, de los efectos de fallas significativas o desastres.

Esta política se aplica a autoridades, docentes, estudiantes, funcionarios administrativos y toda otra persona relacionadas de algún modo a la Facultad.

## **2. Declaración de la Política**

Se debe implementar en la Facultad un Plan de Contingencias para reducir la interrupción ocasionada por desastres y fallas de seguridad (que pueden ser el resultado de desastres naturales, accidentes, fallas en el equipamiento, o acciones deliberadas) a un nivel aceptable mediante una combinación de controles preventivos y de recuperación.

Se deben analizar las consecuencias de desastres, fallas de seguridad e interrupciones de los servicios de la Facultad, para el análisis de riesgo a ser incluido en el Plan de Contingencias, y de esta manera garantizar que los procesos principales de la Facultad puedan restablecerse dentro de los plazos requeridos. Dicho plan debe mantenerse en vigencia y transformarse en una parte integral del resto de los procesos de administración y gestión.


La gestión de la continuidad de los procesos y sistemas principales de la Facultad debe incluir controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables.

## **3. Cumplimiento**

La presente política debe ser cumplida por todos los usuarios, empleados, contratistas y terceros relacionados de alguna manera con Facultad.

Desarrollado por:  Fernando Echavarria	Revisión Dirección del CRTP: Max Arnsdorff	Revisión Dirección de Carrera: Roberto Moreira 1/03/07	Aprobación: Vicedecano Decano	Código:  PS/009
--	--	---	-------------------------------	-----------------------



	<div style="text-align: center;"> <h1>NORMA DE ELABORACION DEL PLAN DE CONTINGENCIAS</h1> </div> <div style="text-align: center;"> <p>Actualización al 15 de abril de 2007</p> </div>	<div style="text-align: center;"> <p>Página</p> <p>1 de 4</p> </div>
---	---	--

## **1. Objetivo**

La norma para la elaboración del Plan de Contingencias del Área de Sistemas de la Facultad, establece las especificaciones y lineamientos que permiten minimizar los riesgos y facilitan la recuperación rápida de las operaciones de sistemas, frente a interrupciones originadas por fallas significativas de seguridad o desastres, como lo establece la *Política de Gerencia de Incidentes de la Seguridad de la Información PS/009*.

## **2. Alcance**

Está dirigida a contar con un instrumento de análisis y reducción de riesgos, consecuencias frente a los posibles incidentes dañinos, sean estos provocados o naturales, la reanudación oportuna de las operaciones indispensables aplicando el plan, y una estimación de tiempos y costos en base a la simulación de recuperación, resultado de las pruebas, mantenimiento y reevaluación del plan de contingencias.

## **3. Responsables**

Es responsable de la planificación, administración, divulgación y ejecución de los controles de seguridad el Encargado de Sistemas del CRTP y el personal del área de Sistemas (en caso de contar con el mismo).


La aprobación y seguimiento al plan de contingencia, será de responsabilidad del Comité de Sistemas, quien deberá realizar una evaluación periódica del cumplimiento de las medidas de seguridad y los controles implementados para tal efecto. El Comité de Sistemas, podrá designar y delegar estas funciones a un Oficial de Seguridad en caso de contar con uno.

## **4. Definición de la Norma**

Se debe implementar un proceso controlado para el desarrollo y mantenimiento de la continuidad de las operaciones del Área de Sistemas, contemplando principalmente el grado de comprensión de los riesgos a los que se enfrenta la Facultad; comprensión del impacto que ocasionan las interrupciones y la planificación de una estrategia realista de protección y de reacción oportuna.

Para garantizar el cumplimiento de los controles, inicialmente se debe realizar un Diagnóstico, el cual será dirigido a evaluar la situación inicial de la seguridad del entorno, en relación a los controles, procesos y procedimientos establecidos.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/09.001
--	--	---	---	--------------------------

	<h1 style="text-align: center;">NORMA DE ELABORACION DEL PLAN DE CONTINGENCIAS</h1>	<p>Página</p> <p style="text-align: center;">2 de 4</p>
<p style="text-align: center;">Actualización al 15 de abril de 2007</p>		

La continuidad de las operaciones del Área de Sistemas de la Facultad se basa en la identificación de los eventos que puedan ocasionar interrupciones y su correspondiente análisis de riesgo.

Identificados los eventos de riesgo, se debe elaborar el Plan, para definir el marco global y el alcance de la planificación.

### ***Elaboración del Plan de Contingencias***

El propósito de desarrollar el Plan de Contingencias, es el de mantener o restablecer las operaciones del Área de Sistemas de la Facultad en el plazo mínimo determinado, una vez ocurrida una interrupción o falla en los procesos críticos de la misma.

En la elaboración del Plan de Contingencia deben considerarse mínimamente los siguientes aspectos:


- a) Identificar los servicios críticos.
- b) Identificar claramente los riesgos.
- c) Analizar la probabilidad de ocurrencia y el nivel de impacto de los mismos.
- d) Identificar con claridad los procedimientos de emergencia y las acciones que mitiguen los riesgos.
- e) Conformar grupos de empleados para emergencias y apoyo.
- f) Delegar las responsabilidades y funciones a los grupos de contingencia.

La Estructura del Plan de contingencias responde al siguiente esquema de contenido:

1. Objetivo
2. Alcance
3. Definición de responsabilidades
4. Términos y Definiciones
5. Identificación de Servicios del Área de Sistemas
6. Identificación de riesgos y servicios críticos
7. Matriz de riesgos
8. Procedimientos de emergencia y recuperación
  - 8.1. Prevención de emergencias
    - 8.1.1. Capacitación
    - 8.1.2. Identificación de emergencias
    - 8.1.3. Respuestas a las emergencias
    - 8.1.4. Evaluación de daños
  - 8.2. Recuperación
    - 8.2.1. Plan detallado

### **ANEXOS**

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/09.001
--	---	---	---	--------------------------

	<div style="text-align: center;"> <h1>NORMA DE ELABORACION DEL PLAN DE CONTINGENCIAS</h1> </div>	<div style="text-align: center;"> <p>Página</p> <p>3 de 4</p> </div>
	<p>Actualización al 15 de abril de 2007</p>	

## ***Implementación del Plan de Contingencias***

Para implementar los procedimientos de emergencia, a fin de permitir la recuperación y restablecimiento de las operaciones del Área de Sistemas de la Facultad en los plazos requeridos, se deben considerar los siguientes aspectos:

- a) Documentar adecuadamente los procedimientos de emergencia y recuperación.
- b) Capacitar y entrenar a los grupos de emergencia y apoyo, y a todo el personal involucrado, en materia de procedimientos y procesos de emergencia.
- c) Mantener un registro histórico de las pruebas y actualizaciones de los procedimientos de emergencia.

## ***Prueba, mantenimiento y reevaluación del Plan de Contingencias***

El Plan de Contingencias debe ser probado por lo menos una vez al año a fin de identificar fallas, suposiciones incorrectas o cambios que pudieran producirse entre las pruebas.

Se deben divulgar los cambios para que los involucrados estén al corriente de las actualizaciones del plan, sus funciones y responsabilidades.

La identificación de cambios aún no reflejados en el Plan de Contingencias debe seguir una adecuada actualización del plan. Este proceso formal de control de cambios garantiza que se difundan las actualizaciones y que el nuevo plan sea sometido a prueba.

Para evaluar y garantizar que el plan sea viable deben realizarse:


- a) Pruebas de discusión de diversos escenarios.
- b) Simulaciones, tomando en cuenta los eventos de riesgo.
- c) Pruebas de recuperación de los aspectos críticos identificados.
- d) Ensayos completos, probando que todos los elementos involucrados tengan pleno conocimiento del plan.
- e) Mantener un registro histórico de las pruebas y actualizaciones de los procedimientos de emergencia.

## ***Documentación del Plan de Contingencias***

La documentación necesaria del Plan de Contingencias debe contener:

- a) Última versión del Plan de Contingencias actualizado, debidamente escrito y aprobado por el Comité de Sistemas.
- b) Los procedimientos de recuperación de las operaciones.
- c) El registro de distribución y conocimiento del plan entre los involucrados.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/09.001
--	--	---	---	--------------------------

	<div data-bbox="427 230 1198 324" data-label="Section-Header"> <h1>NORMA DE ELABORACION DEL PLAN DE CONTINGENCIAS</h1> </div> <div data-bbox="582 347 1038 378" data-label="Text"> <p>Actualización al 15 de abril de 2007</p> </div>	<div data-bbox="1276 185 1362 212" data-label="Text"> <p>Pagina</p> </div> <div data-bbox="1273 235 1364 264" data-label="Text"> <p>4 de 4</p> </div>
---	---	---

Documentación de respaldo.

- a) El cronograma de pruebas.
- b) Documentación completa de los entrenamientos y las pruebas realizadas, los resultados y las acciones a tomar.
- c) Evaluación de los incidentes registrados que necesitaron la ejecución real del plan o de alguna acción correctiva y de recuperación y su incidencia.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/09.001
--	---	---	---	--------------------------

	<div style="text-align: center;"> <h1>POLÍTICA DE CUMPLIMIENTO</h1> </div>	<div style="text-align: center;"> <b>Página</b>   <b>1 de 1</b> </div>
	<b>Actualización al 27 de febrero de 2007</b>	

## **1. Propósito y Alcance**

La política de cumplimiento pretende impedir infracciones y violaciones de las leyes, de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos, y de los requisitos de seguridad, adicionalmente busca garantizar la compatibilidad de los sistemas con las políticas y normas de seguridad de la Facultad de Arquitectura, Artes, Diseño y Urbanismo, además de optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

Esta política se aplica a autoridades, docentes, estudiantes, funcionarios administrativos y toda otra persona relacionadas de algún modo a la Facultad.

## **2. Declaración de la Política**

El diseño, operación, uso y gestión de los sistemas de información pueden estar sujetos a requisitos de seguridad legal, normativa y contractual.

Se debe procurar asesoramiento sobre requisitos legales específicos por parte de los asesores jurídicos de la organización, o de abogados convenientemente calificados.

La seguridad de los sistemas de información debe revisarse periódicamente. Dichas revisiones deben llevarse a cabo con referencia a las políticas de seguridad pertinentes y las plataformas técnicas y sistemas de información deben ser auditados para verificar su compatibilidad con los estándares (normas) de implementación de seguridad.


Deben existir controles que protejan los sistemas de operaciones y las herramientas de auditoría en el transcurso de las auditorías de sistemas.

Asimismo, se requiere una protección adecuada para salvaguardar la integridad y evitar el uso inadecuado de las herramientas de auditoría.

## **3. Cumplimiento**

La presente política debe ser cumplida por todos los usuarios, empleados, contratistas y terceros relacionados de alguna manera con la Facultad.

Desarrollado por:  Fernando Echavarria	Revisión Dirección del CRTP: Max Arnsdorff	Revisión Dirección de Carrera: Roberto Moreira  1/03/07	Aprobación: Vicedecano Decano	Código:  PS/010
--	--	---	-------------------------------------	-----------------------

	<p align="center"><b>NORMA DE CONSIDERACIONES DE AUDITORIA Y AUDITORIA DE SISTEMAS</b></p> <p align="center"><b>Actualización al 15 de abril de 2007</b></p>	<p align="center">Pagina <b>1 de 2</b></p>
---	--	--

### **1. Objetivo**

Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.

### **2. Alcance**

Todos los sistemas de información con los que cuenta la Facultad, así como el Area de Sistemas del CRTP en general esta sujeta a esta norma.

### **3. Responsables**

El Comité de Sistemas es responsable por hacer cumplir la presente norma.

### **4. Definición de la Norma**

Anualmente, el Decano de la Facultad debe solicitar la contratación de una empresa de Auditoría Externa, para una revisión independiente en la cual se evalúen aspectos relacionados con la Auditoría de Sistemas


Deben existir controles que protejan los sistemas de operaciones y las herramientas de auditoría en el transcurso de las auditorías de sistemas. Asimismo, se requiere una protección adecuada para salvaguardar la integridad y evitar el uso inadecuado de las herramientas de auditoría.

#### ***Controles de auditoria de sistemas***

Los requerimientos y actividades de auditoría que involucran verificaciones de los sistemas operacionales deben ser cuidadosamente planificados y acordados a fin de minimizar el riesgo de interrupción de los procesos más importantes. Se deben contemplar los siguientes aspectos:

- a) Los requerimientos de auditoría deben ser acordados con la Dirección de Carrera;
- b) El alcance de las verificaciones debe ser acordado y controlado;
- c) Las verificaciones deben estar limitadas a un acceso de sólo lectura del software de datos;
- d) El acceso que no sea de sólo lectura solamente debe permitirse para copias aisladas de archivos del sistema, las cuales deben ser eliminadas una vez finalizada la auditoría;
- e) Los recursos de TI para realizar las verificaciones deben estar explícitamente identificados y puestos a disposición;

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/10.003
--	---	---	---	--------------------------

	<p align="center"><b>NORMA DE CONSIDERACIONES DE AUDITORIA Y AUDITORIA DE SISTEMAS</b></p> <p align="center"><b>Actualización al 15 de abril de 2007</b></p>	<p align="center">Pagina 2 de 2</p>
---	--	---

- f) Los requerimientos para procedimientos especiales o adicionales deben estar identificados y acordados;
- g) Todos los accesos deben ser monitoreados y registrados a fin de generar una pista de referencia;
- h) Todos los procedimientos, requerimientos y responsabilidades deben documentarse.

***Protección de herramientas de auditoría de sistemas***

Se debe proteger el acceso a las herramientas de auditoría de sistemas, por ejemplo, archivos de datos o software, a fin de evitar su mal uso o compromiso. Dichas herramientas deben estar separadas de los sistemas operacionales y de desarrollo y no deben almacenarse en bibliotecas de cintas o en áreas de usuarios, a menos que se les otorgue un nivel adecuado de protección adicional.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/10.003
--	---	---	---	--------------------------

	<p align="center"><b>NORMA DE CUMPLIMIENTO DE REQUISITOS LEGALES</b></p> <p align="center"><b>Actualización al 15 de abril de 2007</b></p>	<p align="center">Pagina <b>1 de 2</b></p>
---	--	--

### **1. Objetivo**

Impedir infracciones y violaciones de las leyes, de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos, y de los requisitos de seguridad establecidos por la Facultad.

### **2. Alcance**

Todo el personal de la Facultad, esta en la obligación de dar cumplimiento exacto a lo establecido en la presente norma.

### **3. Responsables**

El Encargado de Sistemas del CRTP y el Comité de Sistemas, son responsables de monitorear el cumplimiento de la presente norma.

### **4. Definición de la Norma**

El diseño, operación, uso y gestión de los sistemas de información pueden estar sujetos a requisitos de seguridad legal, normativa y contractual.

Se debe procurar asesoramiento sobre requisitos legales específicos por parte de los asesores jurídicos de la Facultad, o de abogados convenientemente calificados.

Se deben definir y documentar claramente todos los requisitos legales, normativos y contractuales pertinentes par cada sistema de información, en caso de ser aplicable. Del mismo modo deben definirse y documentarse los controles específicos y las responsabilidades individuales para cumplir con dichos requisitos.

### ***Derechos de propiedad intelectual (DPI)***

Se deben implementar procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material respecto del cual puedan existir derechos de propiedad intelectual, como derechos de diseño o marcas registradas. La infracción de derechos de autor (derecho de propiedad intelectual) puede tener como resultado acciones legales que podrían derivar en demandas penales.

Los requisitos legales, normativos y contractuales pueden poner restricciones a la copia de material que constituya propiedad de una empresa. En particular, pueden requerir que sólo

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/10.001
--	---	---	---	--------------------------



	<h2 style="text-align: center;">NORMA DE CUMPLIMIENTO DE REQUISITOS LEGALES</h2>	<p style="text-align: center;">Pagina 2 de 2</p>
<p style="text-align: center;">Actualización al 15 de abril de 2007</p>		

pueda utilizarse material desarrollado por la Facultad, o material autorizado o suministrado a la misma por la empresa que ha realizado el desarrollo.

Los productos de software que constituyan propiedad de una empresa se suministran normalmente bajo un acuerdo de licencia que limita el uso de los productos a equipos específicos y puede limitar la copia a la creación de copias de resguardo solamente. Se deben considerar los siguientes controles:

- a) Publicación de una norma de cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software;
- b) Emisión de normas para la adquisición de productos de software;
- c) Mantenimiento de la concientización respecto de la adquisición y derecho de propiedad intelectual de software, y notificación de la determinación de tomar acciones disciplinarias contra el personal que incurra en el cumplimiento de las mismas;
- d) Mantenimiento adecuado y registro de activos;
- e) Mantenimiento de pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.;
- f) Implementación de controles para garantizar que no se exceda el número máximo permitido de usuarios (si es que es necesario);
- g) Comprobaciones para verificar que sólo se instalan productos con licencia y software autorizado;
- h) Mantenimiento de licencias por parte de personal autorizado;
- i) Utilización de herramientas de auditoría adecuadas;

### ***Prevención del uso inadecuado de los recursos de procesamiento de información***

Los recursos de procesamiento de información de una organización se suministran con propósitos de negocio. La Dirección debe autorizar el uso que se da a los mismos. La utilización de estos recursos con propósitos no autorizados o ajenos a la operativa, sin la aprobación de la Dirección, debe ser considerada como uso indebido. Si dicha actividad es identificada mediante monitoreo u otros medios, se debe notificar al Director de Carrera para que se tomen las acciones disciplinarias que correspondan.

Es esencial que todos los usuarios estén al corriente del alcance preciso del acceso permitido. Esto puede lograrse, por ejemplo, otorgando a los usuarios una autorización escrita, una copia de la cual debería ser firmada por los mismos y retenida en forma segura por la Facultad. Los empleados deben ser advertidos de la prohibición de todo acceso que no esté expresamente autorizado.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/10.001
--	---	---	---	--------------------------

	<p align="center"><b>NORMA DE REVISIONES DE POLÍTICA DE SEGURIDAD Y COMPATIBILIDAD TECNICA</b></p> <p align="center"><b>Actualización al 15 de abril de 2007</b></p>	<p align="center">Pagina 1 de 2</p>
---	--	---

## **1. Objetivo**

El objetivo de la presente norma es garantizar la compatibilidad de los sistemas con las políticas y normas de seguridad de la Facultad.

## **2. Alcance**

Todos los sistemas de información con los que cuenta la Facultad deben cumplir la presente norma.

## **3. Responsables**

El Encargado de Sistemas del CRTP y el Comité de Sistemas, son responsables del cumplimiento de la presente norma.

## **4. Definición de la Norma**

La seguridad de los sistemas de información debe revisarse periódicamente. Dichas revisiones deben llevarse a cabo con referencia a las políticas de seguridad pertinente y las plataformas técnicas y sistemas de información deben ser auditados para verificar su compatibilidad con las normas de seguridad.

La gerencia debe garantizar que se lleven a cabo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad. Asimismo, se debe considerar la implementación de una revisión periódica de todas las áreas de la Facultad para garantizar el cumplimiento de las políticas y normas de seguridad. Entre las áreas a revisar deben incluirse las siguientes:

- a) Sistemas de información;
- b) Proveedores de sistemas;
- c) Propietarios de información y de recursos de información;
- d) Usuarios;
- e) Directores.

Los propietarios de los sistemas de información (*ver NS/3.001 Responsabilidad por Rendición de Cuentas de los Activos*) deben apoyar la revisión periódica de la conformidad de sus sistemas con las políticas, normas y otros requisitos de seguridad aplicables.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/10.002
--	---	---	---	--------------------------

	<p align="center"><b>NORMA DE REVISIONES DE POLÍTICA DE SEGURIDAD Y COMPATIBILIDAD TECNICA</b></p> <p align="center"><b>Actualización al 15 de abril de 2007</b></p>	<p align="center">Pagina 2 de 2</p>
---	--	---


### ***Verificación de la compatibilidad técnica***

Se debe verificar periódicamente la compatibilidad de los sistemas de información con las normas de implementación de la seguridad. La verificación de la compatibilidad técnica comprende la revisión de los sistemas operacionales a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados. Este tipo de verificación de cumplimiento requiere asistencia técnica especializada. Debe ser realizada manualmente (si es necesario, con el apoyo de adecuadas herramientas de software) por un ingeniero en sistemas experimentado.

La verificación de compatibilidad también puede comprender pruebas de penetración, las cuales podrían ser realizadas por expertos independientes contratados específicamente con este propósito. Esto puede resultar útil para la detección de vulnerabilidades en el sistema y para verificar la eficacia de los controles con relación a la prevención de accesos no autorizados posibilitados por las mismas. Se deben tomar recaudos en caso de que una prueba de penetración exitosa pueda comprometer la seguridad del sistema e inadvertidamente permita explotar otras vulnerabilidades.

Las verificaciones de compatibilidad técnica sólo deben ser realizadas por personas competentes y autorizadas o bajo la supervisión de las mismas.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  NS/10.002
--	---	---	---	--------------------------

	<b>PLAN DE CONTINGENCIAS (ANEXOS)</b>	<b>Página</b> <b>1 de 7</b>
	<b>Actualización al 8 de abril de 2007</b>	

## ANEXO 1 Listado de los Grupos de Emergencia y Apoyo


### GRUPO DE EMERGENCIA PARA LA EJECUCION DEL PLAN DE CONTINGENCIAS

Paterno	Materno	Nombres	Dirección	Teléfono

### GRUPO DE APOYO PARA LA EJECUCION DEL PLAN DE CONTINGENCIAS

Paterno	Materno	Nombres	Dirección	Teléfono

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL.A / 001
--	--	---	---	---------------------------

	<b>PLAN DE CONTINGENCIAS (ANEXOS)</b>	<b>Página</b>  <b>2 de 7</b>
	<b>Actualización al 8 de abril de 2007</b>	

## ANEXO 2 Lista de Teléfonos de Emergencia

### TELÉFONOS DE EMERGENCIA

INSTITUCIÓN DE EMERGENCIA	TELÉFONO
Radio Patrulla	110
Ambulancias	118
Bomberos	119
PAC	120
Reten de Emergencias de la HAM de La Paz	134
Grupo de Rescate	138
ELECTROPAZ	2333300
CRUZ ROJA BOLIVIANA	2227818
HOSPITAL DE CLINICAS	2229180
TRANSITO LA PAZ	2371224
POLICIA CAMINERA	2211214
EPSAS	2211222
SAR ILLIMANI FAB	2844040
HOSPITAL DEL NIÑO	2245154
AEROPUERTO	2810140
TRANSITO EL ALTO	2845059

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL.A / 001
--	--	---	---	---------------------------

**Actualización al 8 de abril de 2007**

### ANEXO 3      Formulario de Registro de Capacitación


## REGISTRO DE CAPACITACIÓN

[illegible]

## Capacitador

## Encargado de Sistemas del CRTP


Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL.A / 001
--	--	---	---	---------------------------

	<b>PLAN DE CONTINGENCIAS (ANEXOS)</b>	<b>Página 4 de 7</b>
	<b>Actualización al 8 de abril de 2007</b>	

#### **ANEXO 4 Forma de registro de llamada de amenaza de Bomba**

REPORTER DE AMENAZA DE BOMBA							
<b>a) Escriba literalmente las palabras de la persona que llama.</b> Si fuese posible indague datos sobre la ubicación del dispositivo, forma, lugar en la que la instalaron, a qué grupo representa, etc.							
<b>b) Inmediatamente cuelgue el auricular, registre los siguientes datos.</b> Registre los datos que recuerde y los datos del teléfono al cual ingresó la llamada.							
Número de Teléfono:							
Fecha y Hora de recepción:							
Tiempo de llamada:							
Por la voz identifique:		<b>Varón</b>	Sí	No	<b>Mujer</b>	Sí	No
<b>c) Otros comentarios u observaciones.</b>							
<b>d) Registre sus datos personales.</b>							
Nombre del Empleado:							
Cargo en la Fundación:							
Número telefónico personal:							

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL.A / 001
--	---	---	---	---------------------------


	<b>PLAN DE CONTINGENCIAS (ANEXOS)</b>	<b>Pagina 5 de 7</b>
	<b>Actualización al 8 de abril de 2007</b>	

## ANEXO 5 Forma de registro de llamada de amenaza telefónica

REPORTER DE AMENAZA TELEFÓNICA							
<b>a) Escriba literalmente las palabras de la persona que llama.</b> Si fuese posible indague más datos sobre la persona que llama y el origen de la llamada, ciudad, país, etc.							
<b>b) Inmediatamente cuelgue el auricular, registre los siguientes datos.</b> Registre los datos que recuerde y los datos del teléfono al cual ingresó la llamada.							
Número de Teléfono:							
Fecha y Hora de recepción:							
Tiempo de llamada:							
Por la voz identifique:		<b>Varón</b>	Sí	No	<b>Mujer</b>	Sí	No
<b>c) Otros comentarios u observaciones.</b>							
<b>d) Registre sus datos personales.</b>							
Nombre del Empleado:							
Cargo en la Fundación:							
Número telefónico personal:							

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL.A / 001
--	---	---	---	---------------------------




	<b>PLAN DE CONTINGENCIAS (ANEXOS)</b>	<b>Página 6 de 7</b>
	<b>Actualización al 8 de abril de 2007</b>	

## ANEXO 6    Formulario de Registro de Incidentes

REGISTRO DE INCIDENTES			
<b>Nombre del Involucrado:</b>	<b>Fecha del incidente:</b>	<b>Hr. Inicio:</b>	<b>Hr. Fin:</b>
<b>Área en la que se produjo:</b>			
<b>Tipo de Incidente</b>	<b>Descripción del incidente</b>		
a)    Incidente Natural.			
b)    Incidente del entorno.			
c)    Incidente Humano.			
<b>Consecuencias identificadas, acciones, reacciones adoptadas y observaciones:</b>  <div style="border: 1px solid black; height: 150px; margin-top: 5px;"></div>			
<i>En caso necesario adjunte las hojas que requiera.</i>			

Personal involucrado	Administrador de Sistemas
----------------------	---------------------------

Desarrollado por:	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL.A / 001
Fernando Echavarria				

	<h2 style="text-align: center;">PLAN DE CONTINGENCIAS (ANEXOS)</h2>	<b>Página</b> <b>7 de 7</b>
	<b>Actualización al 8 de abril de 2007</b>	

### ANEXO 7    Formulario de Registro de Pruebas del Plan de Contingencias

REGISTRO DE PRUEBAS DEL PLAN DE CONTINGENCIAS			
Nombre del Involucrado:	Fecha de la prueba :	Hr. Inicio:	Hr. Fin:
<b>Area :</b>			
<b>Contingencia probada</b>		<b>Función realizada</b>	
a)	Identificación de emergencias		
b)	Respuesta a emergencias		
c)	Evacuación total		
d)	Evacuación parcial		
e)	Identificación de equipo de emergencia.		
f)	Revisión de guías telefónicas		
g)	Llamadas telefónicas		
h)	Rescate		
i)	Primeros Auxilios		
<b>Observaciones:</b>  <i>En caso necesario adjunte las hojas que requiera.</i>			

Personal involucrado

Encargado de Sistemas del CRTP

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL.A / 001
--	---	---	---	---------------------------

	<b>PROCEDIMIENTO PARA INVENTARIO DE ACTIVOS (HD, SW)</b>	Página 1 de 2
	Actualización al 2 de mayo de 2007	

### Levantamiento de inventario de software Cliente

#### Detalle del procedimiento


No.	Detalle de las actividades	Responsable
1	Utilizando el "Formulario de Inventario de Software Cliente", realizar el levantamiento del software instalado en cada una de las PCs de los usuarios.	Técnico de Sist. del CRTP
2	Clasificar el software de acuerdo a su uso, indicando si es para cliente o Servidor.	Técnico de Sist. del CRTP
3	Verificar la existencia de licencias e instaladores, una vez concluido el levantamiento.	Técnico de Sist. del CRTP
4	Elaborar un informe para presentación al Comité de Sistemas, adjuntando el inventario de software servidor.	Técnico de Sist. del CRTP

### Levantamiento de inventario de software Servidor

#### Detalle del procedimiento

No.	Detalle de las actividades	Responsable
1	Utilizando el "Formulario de Inventario de Software Servidor", realizar el levantamiento del software instalado en cada uno de los Servidores.	Técnico de Sist. del CRTP
2	Verificar la existencia de licencias e instaladores, una vez concluido el levantamiento.	Técnico de Sist. del CRTP
3	Elaborar un informe para presentación al Comité de Sistemas, adjuntando el inventario de software servidor.	Técnico de Sist. del CRTP

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PR/ 3.01.01
--	---	---	---	----------------------------

	<h2 style="text-align: center;">PROCEDIMIENTO PARA INVENTARIO DE ACTIVOS (HD, SW)</h2>	Pagina 2 de 2
Actualización al 2 de mayo de 2007		

### Levantamiento de inventario de hardware

#### Detalle del procedimiento

No.	Detalle de las actividades	Responsable
1	Apoyado en el Inventario de Activos Fijos de la Facultad, realizar el levantamiento del inventario de hardware.	Técnico de Sist. del CRTP
2	Utilizando el “Formulario de Inventario de Hardware”, realizar el levantamiento del inventario.	Técnico de Sist. del CRTP
3	Elaborar un informe para presentación al Comité de Sistemas, adjuntando el inventario de hardware.	Técnico de Sist. del CRTP
4	Aprovechando el levantamiento del inventario de hardware, será importante evaluar el estado del equipo para planificar el mantenimiento preventivo y correctivo de cada uno.	Técnico de Sist. del CRTP

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PR/ 3.01.01
--	---	---	---	----------------------------

	<b>PROCEDIMIENTO PARA LA CLASIFICACIÓN Y ROTULADO DE INFORMACION</b>	<b>Página</b>  <b>1 de 2</b>
	<b>Actualización al 2 de mayo de 2007</b>	

## **Clasificación de la Información**

El presente procedimiento abarca toda la información generada, procesada y compartida por los usuarios los cuales son propietarios de la información, independientemente del medio de almacenamiento o difusión de la misma.

### **Definiciones**

**Usuario Propietario:** Toda la información y los recursos de información, son de propiedad de la Facultad. El término propietario de la información, se refiere al usuario que la genera, procesa y comparte al interior o exterior de la Facultad y que es producto de las operaciones.

**Recurso o Activo de Información:** Son todos los Informes, reportes manuales, reportes del sistema, registro de datos, etc., impresos o almacenados en algún medio magnético como un CD, Flash Memory, disquete, cinta, etc.

### **Detalle del procedimiento**

<b>No.</b>	<b>Detalle de las actividades</b>	<b>Responsable</b>
1	Utilizando el "Formulario de Inventario de Recursos de Información", elaborar el inventario de recursos de información, tomando en cuenta toda la información procesada por cada usuario así como los reportes generados como resultado del trabajo.	Usuario Propietario
2	En base al cuadro de clasificación de la información ( <i>Ver Norma de Clasificación de la Información NS/3.002</i> ) clasificar cada recurso identificado en el inventario, indicando el grado de criticidad de la información.	Usuario Propietario
3	Revisar, verificar y aprobar el inventario elaborado por el usuario propietario	Jefe de Area
4	En caso de identificar recursos de información generados por el Sistema Modelo Informacional, elaborar el requerimiento correspondiente para la actualización del rotulo en el Sistema.	Usuario Propietario por medio del Jefe de Area

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PR/ 3.02.01
--	---	---	---	----------------------------

	<p style="text-align: center;"><b>PROCEDIMIENTO PARA LA CLASIFICACIÓN Y ROTULADO DE INFORMACION</b></p> <p style="text-align: center;">Actualización al 2 de mayo de 2007</p>	<p>Página 2 de 2</p>
---	---	--------------------------

### Rotulado de la Información

Para el rotulado de la información contenida en medios físicos impresos o electrónicos, se debe seguir el siguiente procedimiento, mismo que parte del entendido de que cada recurso de información ha sido debidamente catalogado y clasificado.

### **Detalle del procedimiento**

No.	Detalle de las actividades	Responsable								
1	Identificar, en el inventario de recursos de información, el rótulo del recurso de información.	Usuario Propietario								
2	Elaborar la etiqueta y rotularla en base a los datos obtenidos del “Inventario de Recursos de Información”	Usuario Propietario								
3	Los rótulos para cada tipo de clasificación son: <table><tr><th>Clasificación</th><th>Rotulado</th></tr><tr><td>Confidencial</td><td>CONFIDENCIAL</td></tr><tr><td>Privada</td><td>SOLO USO INTERNO</td></tr><tr><td>Pública</td><td>Sin rótulo</td></tr></table>	Clasificación	Rotulado	Confidencial	CONFIDENCIAL	Privada	SOLO USO INTERNO	Pública	Sin rótulo	Usuario Propietario
Clasificación	Rotulado									
Confidencial	CONFIDENCIAL									
Privada	SOLO USO INTERNO									
Pública	Sin rótulo									

### **Almacenamiento de información**

Los medios impresos y/o electrónicos que contienen información clasificada como confidencial y privada, deben ser almacenados en lugares seguros, de acuerdo a las normas establecidas para la protección de los activos de información, en tal sentido, debe evitarse el acceso de personas no autorizadas a las áreas de archivo físico y resguardo de dichos medios. Los medios magnéticos, deben ser celosamente resguardados en cajas de seguridad o bajo llave.

El acceso a los medios de almacenamiento electrónico de información confidencial y privada, debe controlarse por medio de contraseñas y es de responsabilidad de cada usuario propietario verificar dicha restricción.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PR/ 3.02.01
--	--	---	---	----------------------------

	<h1 style="text-align: center;">PROCEDIMIENTO DE ACCESO A LA SALA DE SERVIDORES</h1>	Pagina  1 de 2
Actualización al 2 de mayo de 2007		

## **Acceso de personal de Sistemas del CRTP**

Es importante recalcar que la puerta de vidrio que da acceso a la Sala de Servidores debe mantenerse cerrada con llave todo el tiempo y ninguna persona debe realizar trabajo permanente en dicho ambiente.

Adicionalmente en dicho ambiente sólo deben encontrarse los dos servidores y los equipos de comunicación.

El acceso del personal de Sistemas del CRTP sólo debe efectuarse cuando existe un trabajo específico que realizar en el servidor o con los equipos de comunicación, semanalmente para realizar la verificación del correcto funcionamiento del equipamiento o cuando se presenta algún problema con uno de los servidores o con las comunicaciones.

### **Detalle del procedimiento**

No.	Detalle de las actividades	Responsable
1	Hacer uso de una de las llaves que se encuentra en poder del Encargado de Sistemas del CRTP, del Director del CRTP o del Técnico de Sistemas del CRTP.	Encargado de Sist. del CRTP
2	Realizar el trabajo específico o solucionar el problema presentado.	Encargado de Sist. del CRTP
3	Abandonar el ambiente y cerrar con llave la puerta de vidrio.	Encargado de Sist. del CRTP

## **Acceso de terceros a la Sala de Servidores**

El acceso de terceros a la Sala de Servidores debe efectuarse únicamente cuando se requiere realizar un trabajo específico o el tercero desea realizar una visita a dicho ambiente.

Los terceros pueden ser, entre otros, consultores, auditores, proveedores, técnicos, etc.

En todos los casos los terceros deben ser acompañados por el Encargado de Sistemas del CRTP.

### **Requisitos de Seguridad**

Es importante tomar cierto tipo de precauciones con el objetivo de precautelar la seguridad física de los servidores y de los equipos de comunicación.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PR/ 5.01.01
--	---	---	---	----------------------------

	<h2 style="text-align: center;">PROCEDIMIENTO DE ACCESO A LA SALA DE SERVIDORES</h2>	Pagina 2 de 2
Actualización al 2 de mayo de 2007		

El Encargado de Sistemas del CRTP debe exigir que el personal que ingresa a la Sala de Servidores, cumpla los siguientes requisitos mínimos:

- No ingresar a la Sala de Servidores con alimentos o bebidas
- No está permitido fumar en el ambiente
- El personal que realiza mantenimiento al hardware debe llevar una pulsera antiestática
- No utilizar teléfonos celulares en el interior de la Sala de Servidores

### Detalle del procedimiento

No.	Detalle de las actividades	Responsable
1	Hacer uso de una de las llaves que se encuentra en poder del Encargado de Sistemas del CRTP, del Director del CRTP o del Técnico de Sistemas del CRTP.	Encargado de Sist. del CRTP
2	Antes de ingresar, hacer que el tercero llene el “Libro de Visitas a la Sala de Servidores”, incluyendo la información necesaria.	Encargado de Sist. del CRTP
3	Registrar el trabajo realizado por el tercero.	Encargado de Sist. del CRTP
4	Acompañar en todo momento al personal que fue autorizado para ingresar a la Sala de Servidores.	Encargado de Sist. del CRTP
5	Cerrar con llave la puerta de la Sala de Servidores.	Encargado de Sist. del CRTP
6	Registrar la hora de salida y firmar el “Libro de Visitas a la Sala de Servidores.	Encargado de Sist. del CRTP

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PR/ 5.01.01
--	---	---	---	----------------------------





# PROCEDIMIENTO DE ESCRITORIOS Y PANTALLAS LIMPIOS

Página

1 de 2

Actualización al 3 de mayo de 2007

## Escritorios Limpios

### Detalle del procedimiento

No.	Detalle de las actividades	Responsable
1	Diariamente, al inicio de las actividades, verificar que sobre el escritorio no exista ningún documento clasificado como confidencial o privado, impreso o en medio magnético. En caso de existir alguno, y de no ser utilizado de inmediato, guardar en lugar seguro.	Usuario
2	Si abandona su escritorio por un lapso mayor a los 15 minutos, asegúrese de dejar resguardada la información clasificada como confidencial o privada.	Usuario
3	Si necesita abandonar su escritorio por un lapso mayor de tiempo, asegúrese de guardar documentos impresos, medios magnéticos y equipos portátil a fin de resguardar la seguridad de dichos recursos y evitar el acceso no autorizado a los mismos.	Usuario
4	Antes de retirarse de la oficina al final de la jornada, verifique que todos los documentos impresos, equipo portátil y medios magnéticos que contengan información clasificada como confidencial o privada, haya sido protegida en un lugar seguro y, si es posible, bajo llave.	Usuario
5	Asimismo, verifique que los dispositivos de lectura como disqueteras o lectores de CD se encuentran vacíos y que no existan dispositivos removibles como unidades de flash memory o pen drive utilizados durante la jornada en las ranuras de conexión USB.	Usuario

## Pantallas limpias

### Detalle del procedimiento

No.	Detalle de las actividades	Responsable
1	Verifique que su computadora cuenta con una protección de contraseña en el momento de encenderla. En caso de no contar con una, solicite al Encargado de Sistemas del CRTP que se proteja su equipo con una contraseña de encendido.	Usuario
2	En caso de recibir la solicitud, configurar el equipo para que este cuente con una contraseña de encendido.	Encargado de Sist. del CRTP

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PR/ 5.03.01
--	---	---	---	----------------------------



## PROCEDIMIENTO DE ESCRITORIOS Y PANTALLAS LIMPIOS


Página

2 de 2

Actualización al 3 de mayo de 2007

3	Verifique que su computadora tiene activado un protector de pantalla o descansa pantallas protegido por contraseña.	Usuario
4	Las computadoras deben tener activado un protector de pantalla, protegido con contraseña. Para usuarios normales, el tiempo de inactividad antes que se active el protector deberá ser de 15 minutos.	Encargado de Sist. del CRTP
5	En caso de requerir ausentarse de la Facultad, el personal debe apagar computadora y los periféricos, asegurándose de seguir el procedimiento de escritorios limpios, definido en este mismo documento.	Usuario

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PR/ 5.03.01
--	---	---	---	----------------------------

	<p align="center"><b>PROCEDIMIENTO PARA EL REGISTRO SEMANAL DE LA SALA DE SERVIDORES</b></p> <p align="center">Actualización al 3 de mayo de 2007</p>	<p align="center">Pagina 1 de 1</p>
---	---	---

### **Registro semanal de la Sala de Servidores**

#### **Detalle del procedimiento**

No.	Detalle de las actividades	Responsable
1	Todos los lunes al inicio del día, revisar cada uno de los componentes de hardware instalados en la Sala de Servidores.	Encargado de Sist. del CRTP
2	Revisar el correcto funcionamiento del Servidor Principal.	Encargado de Sist. del CRTP
3	Revisar el correcto funcionamiento del Servidor NAT.	Encargado de Sist. del CRTP
4	Revisar el correcto funcionamiento del MODEM.	Encargado de Sist. del CRTP
5	Revisar el correcto funcionamiento de los switches (7).	Encargado de Sist. del CRTP
6	Registrar el estado de cada componente en el "Formulario de Registro Semanal".	Encargado de Sist. del CRTP

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PR/ 6.01.01
--	---	---	---	----------------------------

	<b>PROCEDIMIENTO PARA SOLICITUD DE TRABAJO AL AREA DE SISTEMAS DEL CRTP</b>	<b>Página</b>  <b>1 de 1</b>
	<b>Actualización al 2 de mayo de 2007</b>	

### **Solicitud de Trabajo al Area de Sistemas del CRTP**


Para requerimientos como Alta de Usuario, Nuevo Módulo, Alta de Rol, Modificación de Notas, y Cambio en Inscripción, el formulario debe estar autorizado por el Director de Carrera.

No debe realizarse ningún trabajo de los mencionados anteriormente si es que el usuario no realizó el requerimiento utilizando para ello el "Formulario de Requerimientos a Sistemas del CRTP".

#### **Detalle del procedimiento**

<b>No.</b>	<b>Detalle de las actividades</b>	<b>Responsable</b>
1	Llenar el "Formulario de Requerimientos a Sistemas del CRTP" incluyendo la información necesaria y recabando la firma del Jefe de Area o Autoridad Universitaria.	Usuario Jefe de Area Director de Carrera
2	Asignación al Técnico de Sistemas, en caso de tratarse de temas relacionados con el soporte o falla en equipos PC de usuario.	Encargado de Sist. del CRTP
3	En caso de tratarse de temas relacionados con el Sistema, el Encargado de Sistemas del CRTP es el responsable por el trabajo.	Encargado de Sist. del CRTP
4	Llenar el "Formulario de Requerimiento a Sistemas del CRTP", en la parte relacionada con "Detalle del trabajo técnico requerido".	Encargado de Sist. del CRTP
5	Poner en conocimiento del Director del CRTP, sobre el requerimiento específico.	Encargado de Sist. del CRTP
6	Establecer plazos de acuerdo al tipo de requerimiento utilizando el Formulario de Requerimiento a Sistemas del CRTP, en la parte "Fecha de realización".	Encargado de Sist. del CRTP
7	Una vez concluido el trabajo requerido, llenar el Formulario de Requerimiento a Sistemas del CRTP, en la parte final incluyendo la "Fecha de cierre" y recabando la "Firma del usuario" que requirió el trabajo en señal de conformidad.	Encargado de Sist. del CRTP

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PR/ 6.01.02
--	---	---	---	----------------------------

	<p style="text-align: center;"><b>PROCEDIMIENTO PARA LA ADMINISTRACION DE COPIAS DE RESPALDO (BACKUP)</b></p> <p style="text-align: center;">Actualización al 27 de abril de 2007</p>	<p>Página 1 de 5</p>
---	---	--------------------------

### Copia de Respaldo de la Base de Datos

Periodicidad:


En época de inscripciones (febrero, marzo, junio y julio), se debe obtener copias diarias.

En época regular (demás meses), se debe obtener copias semanales.

### **Detalle del procedimiento**

No.	Detalle de las actividades	Responsable
1	Ingresar al servidor, mediante el programa de aplicación PUTTY instalado en el servidor de pruebas.	Encargado de Sist. del CRTP
2	Elegir "mi" (máscara que tiene guardado el IP del servidor)	Encargado de Sist. del CRTP
3	Ingresar con el usuario "root" digitando el password de administrador.	Encargado de Sist. del CRTP
4	En el prompt del sistema operativo, digitar el comando "mc" (manager commander)	Encargado de Sist. del CRTP
5	Ingresar a la carpeta "sistema"	Encargado de Sist. del CRTP
6	Dentro de la carpeta "sistema" ingresar a carpeta "basedatos"	Encargado de Sist. del CRTP
7	<p>Ejecutar el script "backup", creado internamente. El mismo obtiene el backup y lo comprime. El nombre que debe ser asignado al archivo debe tener el siguiente formato:</p> <p style="text-align: center;">faadu_arqui AAAA-MM-DD-HHMiMi.tar.bz2</p> <p>AAAA: Año MM: Mes DD: Día HH: Hora MiMi: Minuto</p>	Encargado de Sist. del CRTP
8	Esperar aproximadamente tres minutos hasta que el script realice el trabajo de obtención y comprima el archivo	Encargado de Sist. del CRTP
9	Llenar el formulario de "Registro de generación de backup".	Encargado de Sist. del CRTP

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PR/ 6.06.01
--	---	---	---	----------------------------

	<p style="text-align: center;"><b>PROCEDIMIENTO PARA LA ADMINISTRACION DE COPIAS DE RESPALDO (BACKUP)</b></p> <p style="text-align: center;">Actualización al 27 de abril de 2007</p>	<p>Página 2 de 5</p>
---	---	--------------------------

### Backup externo

En época de inscripciones (febrero, marzo, junio y julio) debe obtenerse una copia externa (en CD) de manera semanal, dejando la sesión abierta hasta completar la capacidad del medio magnético (CD aprox. 700 MB).

En época regular (demás meses del año) debe obtenerse una copia externa (en CD) de manera mensual, dejando la sesión abierta hasta completar la capacidad del medio magnético (CD aprox. 700 MB).

Una vez generada la copia externa, se debe llenar el formulario "Registro de Medios Magnéticos de Backups".

Nota: Actualmente el espacio que ocupa la base de datos comprimida es de 5 MB.

### Copia de Respaldo sólo en caso de requerir pruebas específicas con la Base de Datos

Periodicidad:

Esta copia debe ser obtenida sólo en caso de requerir pruebas específicas con la Base de Datos, en consecuencia, no existe una periodicidad establecida.

### Detalle del procedimiento

No.	Detalle de las actividades	Responsable
1	Ingresar al servidor, mediante el programa de aplicación PUTTY instalado en el servidor de pruebas.	Encargado de Sist. del CRTP
2	Elegir "mi" (máscara que tiene guardado el IP del servidor)	Encargado de Sist. del CRTP
3	Ingresar con el usuario "root" digitando el password de administrador.	Encargado de Sist. del CRTP
4	En el prompt del sistema operativo, digitar el comando "mc" (manager commander)	Encargado de Sist. del CRTP
5	Ingresar a la carpeta "sistema"	Encargado de Sist. del CRTP
6	Dentro de la carpeta "sistema" ingresar a carpeta "basedatos"	Encargado de Sist. del CRTP
7	Ejecutar el comando "pg_dump", con el nombre de la base de datos	Encargado de

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PR/ 6.06.01
--	---	---	---	----------------------------

	<p style="text-align: center;"><b>PROCEDIMIENTO PARA LA ADMINISTRACION DE COPIAS DE RESPALDO (BACKUP)</b></p> <p style="text-align: center;">Actualización al 27 de abril de 2007</p>	<p>Página 3 de 5</p>
---	---	--------------------------

	<p>(faadu_arqui), asignando un nombre a la base de datos con el siguiente formato:</p> <p style="text-align: center;">base_arqui AAAA-MM-DD-HHMiMi.dump</p> <p>AAAA: Año MM: Mes DD: Día HH: Hora MiMi: Minuto</p>	Sist. del CRTP
8	Esperar aproximadamente tres minutos hasta que el comando realice el trabajo de obtención del archivo	Encargado de Sist. del CRTP
9	Llenar el formulario de "Registro de generación de backup".	Encargado de Sist. del CRTP

### Backup externo

Luego de obtener la copia de respaldo, cuando se presenta la necesidad de realizar pruebas específicas de la base de datos, debe obtenerse una copia externa (en CD), dejando la sesión abierta hasta completar la capacidad del medio magnético (CD aprox. 700 MB).

Una vez generada la copia externa, se debe llenar el formulario "Registro de Medios Magnéticos de Backups".

Nota: Actualmente el espacio que ocupa la base de datos con el comando mencionado es de 50 MB.

### Copia de Respaldo del Sistema Modelo Informacional

Periodicidad:

Esta copia debe ser obtenida sólo en caso de existir cambios en el Sistema Informacional, en consecuencia, no existe una periodicidad establecida.

### Detalle del procedimiento

No.	Detalle de las actividades	Responsable
1	Ingresar al servidor, mediante el programa de aplicación PUTTY instalado en el servidor de pruebas.	Encargado de Sist. del CRTP
Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff  Aprobación: Dirección de Carrera: Roberto Moreira  Código:  PR/ 6.06.01



## PROCEDIMIENTO PARA LA ADMINISTRACION DE COPIAS DE RESPALDO (BACKUP)

Página

4 de 5

Actualización al 27 de abril de 2007


2	Elegir "mi" (máscara que tiene guardado el IP del servidor)	Encargado de Sist. del CRTP
3	Ingresar con el usuario "root" digitando el password de administrador.	Encargado de Sist. del CRTP
4	En el prompt del sistema operativo, digitar el comando "mc" (manager commander)	Encargado de Sist. del CRTP
5	Ingresar a la carpeta "sistema"	Encargado de Sist. del CRTP
6	<p>Copiar la versión anterior del sistema con la fecha de utilización en la carpeta "sistemas_old", con el formato:</p> <p style="text-align: center;">sis_final - DD-MM-AA</p> <p>DD: Día MM: Mes AA: Año</p>	Encargado de Sist. del CRTP
7	En la carpeta "sis_final" se compila la nueva versión del programa, una vez realizadas las pruebas necesarias.	Encargado de Sist. del CRTP
8	<p>Generar la copia de la última versión del sistema (comprimido aprox. 23 MB) con el siguiente formato de nombre:</p> <p style="text-align: center;">academico_DD-MM-AA</p> <p>DD: Día MM: Mes AA: Año</p> <p>Utilizar un CD sólo para guardar las versiones del Sistema Modelo Informativo.</p>	Encargado de Sist. del CRTP
9	Llenar el formulario de "Registro de generación de backup".	Encargado de Sist. del CRTP

### Backup externo

Una vez generada la copia de respaldo, grabar el archivo del Sistema en un CD expresamente dedicado a las versiones del Sistema Modelo Informativo, dejando sesión abierta hasta completar la capacidad del medio magnético (CD aprox. 700 MB).

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PR/ 6.06.01
--	---	---	---	----------------------------



	<p style="text-align: center;"><b>PROCEDIMIENTO PARA LA ADMINISTRACION DE COPIAS DE RESPALDO (BACKUP)</b></p> <p style="text-align: center;">Actualización al 27 de abril de 2007</p>	<p>Página 5 de 5</p>
---	---	--------------------------

Una vez generada la copia externa, se debe llenar el formulario “Registro de Medios Magnéticos de Backups”.

### **Etiquetado y Custodia**

No.	Detalle de las actividades	Responsable
1	<p><b>Etiqueta</b></p> <p>La etiqueta de los medios magnéticos (CD) en los cuales se obtengan las copias de respaldo, deben tener el siguiente formato:</p> <p style="text-align: center;">Nombre + Mes + Año</p> <p>La misma debe ser escrita con un marcador especial para CDs.</p> <p>El Nombre debe ser llenado de acuerdo al tipo de copia externa: Base de datos, Sistema, etc.</p>	Encargado de Sist. del CRTP
	<p><b>Custodia</b></p>	
2	Una vez obtenida la copia de respaldo externa en CD, el mismo debe ser resguardado en uno de los casilleros existentes actualmente en el Ambiente de Sistemas	Encargado de Sist. del CRTP
3	Llenar el formulario de “Registro de Medios Magnéticos de Backups”.	Encargado de Sist. del CRTP

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PR/ 6.06.01
--	---	---	---	----------------------------

	<b>PROCEDIMIENTO PARA LA ADMINISTRACION DE USUARIOS</b>	<b>Pagina</b>  <b>1 de 2</b>
	<b>Actualización al 4 de mayo de 2007</b>	

## **Alta de Usuarios**

Para que el Encargado de Sistemas del CRTP pueda proceder al alta de un nuevo usuario en el Sistema Modelo Informacional, es necesaria la presentación del “Formulario de Requerimientos a Sistemas del CRTP”, firmado y autorizado por el Director de Carrera.

### **Detalle del procedimiento**

<b>No.</b>	<b>Detalle de las actividades</b>	<b>Responsable</b>
1	Llenar el Formulario de Requerimientos a Sistemas del CRTP incluyendo la información necesaria para el alta del nuevo usuario.	Director de Carrera
2	Recabar datos generales del usuario: Nombre, Carnet de Identidad, Cargo, Funciones generales.	Encargado de Sist. del CRTP
3	Generar el usuario con la inicial del nombre y el apellido. En caso de existir un homónimo incluir la inicial del segundo apellido.	Encargado de Sist. del CRTP
4	Generar la contraseña (password) para el usuario utilizando su Número de Carnet de Identidad.	Encargado de Sist. del CRTP
5	Ingresa al Sistema Modelo Informacional con la contraseña de Sistemas.	Encargado de Sist. del CRTP
6	Ingresa en el Menú a la opción “Administrar Usuarios”.	Encargado de Sist. del CRTP
7	En el título de “Agregar usuario”, incluir la información relacionada con:  Id de usuario: (Identificador de usuario) Usuario: (Nombre de usuario) Clave: (Inicialmente el password asignado por sistemas) Repita la clave: (Reiterar la anterior) Correo: (Correo electrónico personal del usuario) Recordatorio: (Algún dato especial para recordar la clave) Facultad: (Arquitectura y Artes) Carrera: (Arquitectura)	Encargado de Sist. del CRTP
8	En la misma pantalla, en el título de “Agregar rol a usuario”, incluir la siguiente información:  Seleccione: (Elegir un usuario existente) Rol de usuario: (Elegir entre los diez roles existentes, de acuerdo al requerimiento y al tipo de trabajo que realizará el usuario) Fecha de expiración: (Actualmente está establecido que el periodo	Encargado de Sist. del CRTP

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PR/ 7.02.01
--	---	---	---	----------------------------

	<b>PROCEDIMIENTO PARA LA ADMINISTRACION DE USUARIOS</b>	<b>Pagina</b>  <b>2 de 2</b>
	<b>Actualización al 4 de mayo de 2007</b>	

	de expiración sea de un año calendario)	
--	---	--


### **Baja de Usuario**

Para que el Encargado de Sistemas del CRTP pueda proceder a la baja de un usuario en el Sistema Modelo Informacional, es necesaria la presentación del “Formulario de Requerimientos a Sistemas del CRTP”, firmado y autorizado por el Director de Carrera.

### **Detalle del procedimiento**

<b>No.</b>	<b>Detalle de las actividades</b>	<b>Responsable</b>
1	Llenar el Formulario de Requerimientos a Sistemas del CRTP incluyendo, la fecha en la que se debe dar de baja al usuario y el motivo por el cual se solicita la baja, utilizando el espacio con el título “Explique detalladamente su requerimiento”.	Director de Carrera
2	Ingresar al Sistema Modelo Informacional con la contraseña de Sistemas.	Encargado de Sist. del CRTP
3	Ingresar en el Menú a la opción “Administrar Usuarios”.	Encargado de Sist. del CRTP
4	En el título de “Agregar rol a usuario”, en el punto referido a “Fecha de expiración” incluir la fecha de baja del usuario (fecha que el usuario quedará inhabilitado)	Encargado de Sist. del CRTP

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PR/ 7.02.01
--	---	---	---	----------------------------

	<b>PROCEDIMIENTO PARA LA ADMINISTRACION DE ROLES</b>	<b>Página</b>  <b>1 de 2</b>
	<b>Actualización al 2 de mayo de 2007</b>	


### **Alta de nuevo Rol**

Para que el Encargado de Sistemas del CRTP pueda proceder al alta de un nuevo rol en el Sistema Modelo Informacional, es necesaria la presentación del “Formulario de Requerimientos a Sistemas del CRTP”, firmado y autorizado por el Director de Carrera.

### **Detalle del procedimiento**

<b>No.</b>	<b>Detalle de las actividades</b>	<b>Responsable</b>
1	Llenar el Formulario de Requerimientos a Sistemas del CRTP incluyendo la información necesaria para el alta del nuevo rol.	Director de Carrera
2	Ingresar al Sistema Modelo Informacional con la contraseña de Sistemas.	Encargado de Sist. del CRTP
3	Ingresar al Menú “Administrar Roles”.	Encargado de Sist. del CRTP
4	En el título de “Agregar nuevo rol”, incluir la siguiente información:  Código rol: (Nombre del rol) Rol: (Nombre del rol) Descripción: (En caso de requerir más detalle sobre el nuevo rol)	Encargado de Sist. del CRTP
5	Ingresar al Menú “Administrar Enlaces”.	Encargado de Sist. del CRTP
6	En el título de “Agregar nuevo enlace”, incluir información sobre:  Categoría: Nombre del enlace: Ruta del enlace: Posición en la categoría: Imagen:	Encargado de Sist. del CRTP
7	Ingresar al Menú “Administrar Menues”.	Encargado de Sist. del CRTP
8	En el título “Agregar nuevo menú”, incluir la siguiente información:  Seleccione usuario: (Elegir un usuario existente) Roles del usuario: (Elegir el nuevo rol agregado en el sistema) Seleccione categoría: (Seleccionar la categoría requerida)	Encargado de Sist. del CRTP
9	En la misma pantalla existen dos menús: “Enlaces de la categoría”,	Encargado de

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PR/ 7.02.02
--	---	---	---	----------------------------

	<b>PROCEDIMIENTO PARA LA ADMINISTRACION DE ROLES</b>	<b>Pagina</b> <b>2 de 2</b>
	<b>Actualización al 2 de mayo de 2007</b>	

	y “Enlaces permitidos para el usuario”.  Para agregar los enlaces requeridos al nuevo rol, es necesario marcar en el menú “Enlaces de la categoría” los enlaces que serán utilizados por el nuevo rol en el Sistema.	Sist. del CRTP
--	--	----------------

### **Modificación de Rol**

Para que el Encargado de Sistemas del CRTP pueda proceder a la modificación de un rol en el Sistema Modelo Informacional, es necesaria la presentación del “Formulario de Requerimientos a Sistemas del CRTP”, firmado y autorizado por el Director de Carrera.

#### **Detalle del procedimiento**

<b>No.</b>	<b>Detalle de las actividades</b>	<b>Responsable</b>
1	Llenar el Formulario de Requerimientos a Sistemas del CRTP incluyendo la información necesaria para el alta del nuevo usuario.	Director de Carrera
2	Ingresa al Sistema Modelo Informacional con la contraseña de Sistemas.	Encargado de Sist. del CRTP
3	Ingresa al Menú “Administrar Menues”.	Encargado de Sist. del CRTP
4	En el título “Agregar nuevo menú”, incluir la siguiente información:  Seleccione usuario: (Elegir un usuario existente) Roles del usuario: (Elegir el rol a ser modificado) Seleccione categoría: (Seleccionar la categoría requerida)	Encargado de Sist. del CRTP
5	En la misma pantalla existen dos menús: “Enlaces de la categoría”, y “Enlaces permitidos para el usuario”.  Para modificar los enlaces requeridos al nuevo rol, es necesario marcar en el menú “Enlaces de la categoría” los enlaces que serán utilizados por el rol en el Sistema.	Encargado de Sist. del CRTP

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PR/ 7.02.02
--	---	---	---	----------------------------

	<b>PROCEDIMIENTO PARA LA ADMINISTRACION DE PROYECTOS</b>	<b>Pagina</b>  <b>1 de 1</b>
	<b>Actualización al 6 de mayo de 2007</b>	

## **Administración de Proyectos**

### **Detalle del procedimiento**


<b>No.</b>	<b>Detalle de las actividades</b>	<b>Responsable</b>
1	Solicitud escrita y detallada en el "Formulario de Requerimiento a Sistemas"	Usuario
2	Aprobación del requerimiento mediante el "Formulario de Requerimiento a Sistemas"	Jefe del Area Usuaría
3	Evaluación de la solicitud, análisis del impacto del desarrollo del proyecto sobre los sistemas existentes y sobre el trabajo de los demás usuarios de la Facultad y comunicación al área usuaria sobre la posibilidad o no de llevar a cabo el requerimiento.	Encargado de Sist. del CRTP
4	Dependiendo de la complejidad y el impacto del requerimiento debe requerirse la autorización del desarrollo del proyecto por parte del Comité de Sistemas.	Comité de Sistemas.
5	Reunión con el usuario solicitante para establecer exactamente los detalles de la solicitud (en caso de ser necesario).	Encargado de Sist. del CRTP
6	Establecer los tiempos de ejecución de la solicitud y comunicación del mismo al usuario y al área solicitante.	Encargado de Sist. del CRTP
7	Desarrollo del requerimiento.	Encargado de Sist. del CRTP
8	Realización de pruebas internas luego de completado el trabajo de desarrollo.	Encargado de Sist. del CRTP
9	Realización de pruebas con el usuario solicitante.	Encargado de Sist. del CRTP
10	Realización del pase a producción del desarrollo realizado.	Encargado de Sist. del CRTP
11	Cierre de proyecto mediante firma de aceptación del usuario solicitante en el "Formulario de Requerimiento a Sistemas"	Usuario

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PR/ 8.05.01
--	---	---	---	----------------------------



## INVENTARIO DE HARDWARE

[illegible]

	<b>FORMULARIO PARA EL INVENTARIO DE RECURSOS DE INFORMACION</b>	<b>Pagina</b>

INVENTARIO DE RECURSOS DE INFORMACIÓN				
	<b>Nombre del Propietario</b>			
	<b>Cargo</b>			
	<b>Fecha de actualización</b>			
<b>Nº</b>	<b>Título del recurso de Información</b>	<b>Criticidad</b>	<b>Origen</b>	<b>Rótulo</b>
Elaborado por Usuario Propietario		Aprobado por Jefe de Área		

Criticidad:	Confidencial, Privada, Pública
Origen:	Elaboración Manual, Sistema Modelo Informacional, Otro Sistema
Rótulo:	Empleado para sobres cajas o paquetes contenedores de documentos y para medios magnéticos como Cintas, CDs, DVDs, etc.





## INVENTARIO DE SOFTWARE CLIENTE

(AL    /    /    )

[illegible]



---

**Pagina**

## INVENTARIO DE SOFTWARE SERVIDOR

(AL / / )

[illegible]



---

**Pagina**

## LIBRO DE VISITAS A LA SALA DE SERVIDORES

[illegible]

	<b>FORMULARIO DE REGISTRO DE CONFIGURACION DE PROTECTOR DE PANTALLAS</b>	<b>Pagina</b>

### REGISTRO DE CONFIGURACIÓN DE PROTECTOR DE PANTALLAS

Cód. Equipo	Responsable del recurso	Área	Fecha de Configuración	Firma del Responsable del recurso

Entre: \_\_\_\_\_ y \_\_\_\_\_ (fechas)

\_\_\_\_\_  
Encargado de Sistemas  
del CRTP

	<b>FORMULARIO DE REGISTRO SEMANAL</b>	Pagina _____

### FORMULARIO DE REGISTRO SEMANAL

(DEL MES DE \_\_\_\_\_ DE \_\_\_\_\_ )


Componente	Lunes ____	Lunes ____	Lunes ____	Lunes ____	Lunes ____
Servidor Principal					
Servidor NAT					
Modem					
Switches					

**Observaciones\*:**

Componente	Lunes ____	Lunes ____	Lunes ____	Lunes ____	Lunes ____
Servidor Principal					
Servidor NAT					
Modem					
Switches					

\*Registrar cualquier eventualidad surgida durante la revisión semanal o entre una revisión y otra.

\_\_\_\_\_  
Encargado de  
Sistemas del CRTP

	<b>FORMULARIO DE REQUERIMIENTO A SISTEMAS DEL CRTP</b>	<b>Pagina</b>

Fecha: \_\_\_\_ / \_\_\_\_ / \_\_\_\_

Nombre del usuario que realiza el requerimiento: \_\_\_\_\_

Cargo del usuario que realiza el requerimiento: \_\_\_\_\_

Nombre del Jefe de Area o Autoridad que autoriza: \_\_\_\_\_

**Tipo de Requerimiento:**

Nuevo módulo: ☐      Cambio en el Sistema: ☐      Nuevo reporte / estadístico MI: ☐

Alta de usuario: ☐      Alta de rol: ☐      Baja de usuario: ☐

Modificación de Notas: ☐      Cambio en Inscripción: ☐      Otro: ☐

Explique detalladamente el requerimiento:

---



---



---

_____	_____	_____
Firma de Usuario	Firma de Jefe de Area o Autoridad	Autorización de Director de Carrera

**Sistemas**

Detalle del trabajo técnico requerido:

---



---




---

Fecha de realización: \_\_\_\_\_ Responsable: \_\_\_\_\_


---

Fecha de cierre: \_\_\_\_\_ Firma de usuario: \_\_\_\_\_

	<b>FORMULARIO</b> <b>REGISTRO DE GENERACION DE BACKUP</b>		Pagina

Fecha	Hora	Nombre del Backup	Tipo de Backup (BD, SIS)*	Ubicación en el Servidor	Firma del Encargado de Sistemas del CRTP


\*Tipo de Backup: Base de Datos (BD) o Sistema Modelo Informacional (SIS)

	<b>FORMULARIO</b> <b>REGISTRO DE MEDIOS MAGNETICOS DE BACKUP</b>		Pagina

Número de CD	Fecha	Tipo de Backup (BD, SIS)*	Firma del Encargado de Sistemas del CRTP	Firma del Director del CRTP (Revisión)

\*Tipo de Backup: Base de Datos (BD) o Sistema Modelo Informacional (SIS)



	<h1 style="text-align: center;">MANUAL DE FUNCIONES DEL COMITÉ DE SISTEMAS</h1>	Pagina 1 de 3
Actualización al 2 de mayo de 2007		

## Introducción

Debe constituirse un Comité de Sistemas y debe delegarse la responsabilidad de presidirlo al Director de Carrera.

## Propósito del Manual de Funciones

El propósito del presente manual, es el de servir como documento normativo y de consulta para todas las áreas vinculadas, cuyas autoridades son miembros del Comité de Sistemas.

## Objetivo General

Administrar de una manera eficiente el área de Sistemas del CRTP de la Facultad.

## Funciones

Aprobar, reprobado la factibilidad de los proyectos presentados, mencionando tiempos, recursos y alternativas, por el Encargado de Sistemas del CRTP.

Aprobar, reprobado los requerimientos más importantes por los usuarios de la Facultad y presentadas, mencionando tiempos, recursos y alternativas, por el Encargado de Sistemas del CRTP

Aprobar, reprobado cambios estructurales dentro del Sistema Modelo Informacional, sean estos de configuración o desarrollo, presentadas, mencionando tiempos, recursos y alternativas, por el Encargado de Sistemas del CRTP.

Aprobar, reprobado los cambios de versión de programas y pases a producción de los mismos, presentadas, mencionando tiempos, recursos y alternativas, por el Encargado de Sistemas del CRTP.


## Integrantes del comité y responsabilidades

El Comité de Sistemas es el responsable de aprobar, cambiar o rechazar las actividades del Area de Sistemas del CRTP.

El Comité de Sistemas debería estar compuesto por:

- Director de Carrera - Presidente

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  MF/001
--	---	---	---	-----------------------

	<h1 style="text-align: center;">MANUAL DE FUNCIONES DEL COMITÉ DE SISTEMAS</h1>	<p>Página 2 de 3</p>
<p style="text-align: center;">Actualización al 2 de mayo de 2007</p>		

- Director del CRTP – Vicepresidente
- Encargado de Sistemas del CRTP – Secretario de Actas
- (Persona a ser designada) - Vocal

La responsabilidad de presidir el Comité es del Director de Carrera, la cual puede ser asumida por el Director del CRTP en caso de ausencia del Director de Carrera.

El Director de Carrera, el Director del CRTP, tienen derecho a voz y voto en las decisiones del Comité.

El Encargado de Sistemas del CRTP es el responsable de presentar el informe de la situación del área de Sistemas al Comité. Asiste a las reuniones en calidad de secretario de actas y con derecho a voz. Tienen también la responsabilidad de generar el Acta de Comité de Sistemas de cada una de las reuniones del Comité.

### **Periodicidad de las reuniones del Comité de Sistemas**

Inicialmente se prevé que el Comité de Sistemas tenga reuniones bimensuales para tratar los temas más importantes relacionados con las actividades del Área de Sistemas del CRTP. Sin embargo, en base a los proyectos y requerimientos que deban ser analizados, esta periodicidad puede sufrir modificaciones.

### **Aprobación de actividades y acciones**

Una vez presentados los antecedentes por el Encargado de Sistemas del CRTP, se comenzará a investigar las solicitudes y se priorizarán de acuerdo al grado de importancia.


Se debatirá la solicitud presentada por los usuarios y seguidamente se definirá un plan de acción a tomar de acuerdo a las prioridades que el Comité vea por conveniente.

Al final de cada reunión, el Secretario de Actas generará el Acta de Comité en el cual deben incluirse los temas tratados y la firma de todos los asistentes. (En el Anexo se presenta un formato que puede ser utilizado para generar las Actas de Comité).

### **Función de seguridad del Comité de Sistemas**

La seguridad de la información es una responsabilidad de la Facultad compartida por todos los usuarios y autoridades universitarias. Por consiguiente, debe existir un Comité de Sistemas que garantice que existe una clara dirección y un apoyo manifiesto de la Dirección a las iniciativas de seguridad. Este comité debe promover la seguridad dentro de la Facultad mediante un adecuado compromiso y una apropiada asignación de recursos. El Comité, en materia de seguridad, debe comprender las siguientes funciones:

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  MF/001
--	---	---	---	-----------------------

	<h1 style="text-align: center;">MANUAL DE FUNCIONES DEL COMITÉ DE SISTEMAS</h1>	<p>Página 3 de 3</p>
<p style="text-align: center;">Actualización al 2 de mayo de 2007</p>		

- a. Revisar y aprobar las políticas y responsabilidades generales en materia de seguridad de la información.
- b. Monitorear cambios significativos en la exposición de los recursos de información frente a las mayores amenazas.
- c. Revisar y monitorear los incidentes relativos a la seguridad.
- d. Aprobar las principales iniciativas para incrementar la seguridad de la información.

## ANEXO.

### Acta No. #/2007 COMITÉ DE SISTEMAS

#### Lugar, fecha y hora

La Paz, # de %%% de 2007, horas ##:##

#### Participantes de la reunión

%%%%%%%%

#### Orden del día

%%%%%%%%

%%%%%%%%


#### Conclusiones

%%%%%%%%

#### POR EL COMITÉ DE SISTEMAS

(Firmas de los asistentes a la reunión)


Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  MF/001
--	--	---	---	-----------------------

	<div style="text-align: center;"> <h1>PLAN DE CONTINGENCIAS</h1> </div>	<div style="text-align: center;">         Pagina 1 de 22       </div>
	<div style="text-align: center;">         Actualización al 7 de abril de 2007       </div>	

## INDICE DEL CONTENIDO

<b>1. OBJETIVO .....</b>	<b>2</b>
<b>2. ALCANCE .....</b>	<b>2</b>
<b>3. DEFINICIÓN DE RESPONSABILIDADES.....</b>	<b>2</b>
<b>4. TÉRMINOS Y DEFINICIONES.....</b>	<b>3</b>
<b>5. IDENTIFICACIÓN DE SERVICIOS DEL ÁREA DE SISTEMAS DEL CRTP.....</b>	<b>4</b>
<b>6. IDENTIFICACIÓN DE RIESGOS Y SERVICIOS CRÍTICOS.....</b>	<b>4</b>
<b>7. MATRIZ DE RIESGOS .....</b>	<b>6</b>
<b>8. PROCEDIMIENTOS DE EMERGENCIA Y RECUPERACIÓN .....</b>	<b>7</b>
<b>8.1. PREVENCIÓN DE EMERGENCIAS.....</b>	<b>7</b>
<b>8.1.1. CAPACITACIÓN.....</b>	<b>9</b>
<b>8.1.2. IDENTIFICACIÓN DE EMERGENCIAS.....</b>	<b>11</b>
<b>8.1.3. RESPUESTAS A LAS EMERGENCIAS.....</b>	<b>12</b>
EVACUACIÓN DE LAS INSTALACIONES .....	15
<b>8.1.4. EVALUACIÓN DE DAÑOS.....</b>	<b>18</b>
<b>8.2. RECUPERACIÓN .....</b>	<b>19</b>
<b>8.2.1. PLAN DETALLADO .....</b>	<b>19</b>
RECUPERACIÓN DEL SERVIDOR DE PRODUCCIÓN .....	19
OPERACIONES DE RESCATE .....	21
<b>8.3. PRUEBAS AL PLAN DE CONTINGENCIAS .....</b>	<b>22</b>

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	---	---	---	-------------------------

	<h1 style="text-align: center;">PLAN DE CONTINGENCIAS</h1> <p style="text-align: center;">Actualización al 7 de abril de 2007</p>	<p style="text-align: center;">Pagina 2 de 22</p>
---	---	---

## 1. Objetivo

Proporcionar las acciones que deben ser adoptadas para la identificación de una eventualidad, así como para la recuperación de las operaciones de la Sala de Servidores y la restauración de los sistemas operativos, sistemas de aplicación, bases de datos, configuración de servidores, equipo de comunicaciones y estaciones de trabajo, así como la recuperación de la información crítica que contienen dichos equipos, en respuesta a la ocurrencia de incidentes de riesgo en la Facultad de Arquitectura, Artes, Diseño y Urbanismo de la Universidad Mayor de San Andrés.

## 2. Alcance

El plan de contingencias de la Sala de Servidores de la Facultad, será aplicado para la prevención y restablecimiento de los servicios y sistemas informáticos, ante la ocurrencia de incidentes de riesgo que amenacen el normal desarrollo de las actividades informatizadas de la Facultad.

El presente Plan cubre las contingencias que puedan presentarse en la Sala de Servidores o en el Área de Sistemas de la Facultad, y no cubre las dependencias o los ambientes de la Facultad que no se encuentren bajo la responsabilidad y supervisión del Encargado de Sistemas del CRTP.

Este procedimiento debe ser ejecutado por los grupos de emergencia y de apoyo definidos en el mismo, a fin de garantizar el restablecimiento oportuno de las operaciones, con la colaboración total del resto del personal de la Facultad.

## 3. Definición de responsabilidades

Los grupos de emergencia y apoyo, están conformados de la siguiente manera:


**Grupo de emergencia para la ejecución del Plan de Contingencia de la Sala de Servidores:**

Encargado de Sistemas del CRTP y Personal del Área de Sistemas del CRTP (en caso de contar con dicho personal).

**Grupo de apoyo para la ejecución del Plan de Contingencia de la Sala de Servidores:**

Director de Carrera  
Director del CRTP

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	--	---	---	-------------------------

	<h1>PLAN DE CONTINGENCIAS</h1>	Pagina <b>3 de 22</b>
Actualización al 7 de abril de 2007		

Las responsabilidades del personal comprendido en los grupos de emergencia y apoyo de sistemas, se describen a continuación y se incluye la responsabilidad de colaboración del resto del personal de la Facultad:

### **Del Grupo de Emergencia de Sistemas**

Es responsable de identificar oportunamente las situaciones de emergencia potenciales y de la ejecución de los procedimientos de emergencia, para poder asegurar la integridad del hardware, software y de los servicios que presta el Area de Sistemas y la Sala de Servidores, y garantizar la continuidad de las operaciones de la Facultad.

Es responsable de coordinar las acciones de capacitación, implementación, pruebas y ejecución del plan, debiendo asegurarse de que todo el personal entienda y cumpla los procedimientos de emergencia.

### **Del Grupo de Apoyo de Sistemas**

El grupo de apoyo de sistemas es responsable de prestar el apoyo estratégico de contingencia, ante la ocurrencia de incidentes.

Es responsable de dotar al grupo de emergencia, de todas herramientas, equipo necesario y soporte técnico a fin de restablecer oportunamente las operaciones de sistemas.

### **Del personal de la Facultad**


El personal administrativo y operativo de la Facultad, debe prestar el máximo apoyo durante la recuperación de las operaciones de sistemas.

Todo el personal de la Facultad, operativo y administrativo, debe mantener constante vigilancia a probables indicios de incidentes de riesgo, e informar inmediatamente al Encargado de Sistemas del CRTP.

## **4. Términos y Definiciones**

**Sitio Principal:** Es la Sala de Servidores, que se encuentra en las oficinas de la Facultad, donde está instalada la infraestructura tecnológica de la misma.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	---	---	---	-------------------------

	<h1 style="text-align: center;">PLAN DE CONTINGENCIAS</h1>	<p style="text-align: center;">Pagina <b>4 de 22</b></p>
	<b>Actualización al 7 de abril de 2007</b>	

**Riesgo:** Consecuencia producida por la ocurrencia de un incidente que involucra cierto nivel de impacto en las operaciones de la Facultad.

## 5. Identificación de Servicios del Área de Sistemas del CRTP

En el Área de Sistemas de la Facultad, existe una infraestructura de Hardware y Software instalada, que presta diferentes servicios de tecnología al interior de la Facultad. Dichos servicios son de gran importancia en las operaciones diarias de las diferentes áreas y en muchos casos, la continuidad de las mismas depende de la continuidad de los servicios de sistemas.

Los servicios generales que presta el Área de Sistemas son los siguientes:

- Servicios de Comunicaciones y de Red Local
- Servicio de Telecomunicaciones, Internet
- Servicios de Soporte técnico Help Desk
- Servicios de mantenimiento preventivo y correctivo
- Servicio del Sistema Modelo Informacional
- Servicio de Respaldo y Continuidad de las operaciones (Backup)
- Servicio de Seguridad de Sistemas


## 6. Identificación de riesgos y servicios críticos

Como se ha definido anteriormente, un riesgo es la consecuencia de un incidente. En este sentido, se deben identificar las causas o amenazas que ocasionan tales incidentes, que puedan interrumpir las operaciones de la Sala de Servidores y en consecuencia, las de la Facultad.

Las posibles amenazas que ocasionarían interrupciones en las operaciones de la Sala de Servidores, relacionadas con el entorno y humanas, se detallan a continuación:

- Amenazas por fallas en el Hardware
  - Errores en discos duros de los servidores
  - Las fuentes de poder de los servidores dejan de funcionar
  - Los procesadores de los servidores son inoperables
  - Las tarjetas de red no funcionan
  - Fallas en tarjetas madre o principales
  - Fallas en los Switches
  - Fallas en el Modem
  - Robo de componentes del Centro de Cómputo

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	--	---	---	-------------------------

	<h1 style="text-align: center;">PLAN DE CONTINGENCIAS</h1>	<p style="text-align: center;">Pagina <b>5 de 22</b></p>
	<b>Actualización al 7 de abril de 2007</b>	

- Amenazas por fallas en el Software
  - Ataques de virus
  - Intrusiones y software malicioso
  - Denegación de Servicio
- Interrupción de servicio de terceros
  - Interrupción del servicio de energía eléctrica
  - Interrupción del Servicio de Internet
  - Interrupción del Servicio de telefonía

Los riesgos a los que se exponen las operaciones, en caso de consumarse las amenazas mencionadas anteriormente son:


- 1) Riesgos por fallas en el Hardware
  - a) Pérdida de información del Sistema Modelo Informacional
  - b) Pérdida del Sistema Modelo Informacional
  - c) Pérdida de la Configuración de los Servidores
  - d) Pérdida de información de procedimientos alternativos o de respaldo
  - e) Interrupciones en los servicios del Área de Sistemas
- 2) Riesgos por fallas en el software
  - g) Desconfiguración e interrupción de los servicios del Área de Sistemas
  - h) Pérdida de información por ataques de virus y software malicioso
  - i) Vulnerabilidad ante ataques de hackers e intrusos
  - j) Daños a los Sistemas Operativos
  - k) Daños al Sistema de Base de Datos
- 3) Riesgos por interrupción de servicios
  - l) Inoperabilidad de los sistemas de aplicación
  - m) Inoperabilidad de los sistemas de red
  - n) Inoperabilidad de los sistemas de telecomunicación
  - o) Daños al Hardware por corto circuito
  - p) Daños a la estructura e información de la base de datos

Del detalle de riesgos citado, se pueden identificar que los servicios cuya interrupción causarían el mayor impacto en las operaciones de la Facultad son los siguientes:

- Servicio de Red Eléctrica
- Servicios de Comunicaciones y de Red Local
- Servicio de Telecomunicaciones, Internet
- Servicio del Sistema Modelo Informacional

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	--	---	---	-------------------------



	<b>PLAN DE CONTINGENCIAS</b>	Pagina <b>6 de 22</b>
	Actualización al 7 de abril de 2007	

## 7. Matriz de Riesgos

La siguiente matriz define cada uno de los riesgos identificados, las acciones correctivas y los responsables de realizar dichas acciones.

MATRIZ DE RIESGOS				
RIESGO		ACCIONES CORRECTIVAS		RESPONSABLES
Riesgos por fallas en el Hardware				
Pérdida de información del Sistema Modelo Informacional		Recuperación de las copias de respaldo.		Encargado de Sistemas del CRTP
Pérdida del Sistema Modelo Informacional		Reinstalación del Aplicativo. Restauración de la Base de Datos Recuperación de última copia de respaldo.		Encargado de Sistemas del CRTP
Pérdida de la Configuración de los Servidores		Restauración del último respaldo de configuración.		Encargado de Sistemas del CRTP
Pérdida de información de procedimientos alternativos o de respaldo		Recuperación de los archivos de respaldo.		Encargado de Sistemas del CRTP
Interrupciones en los servicios del Área de Sistemas		Restauración de los servidores, sistemas operativos y servicios.		Encargado de Sistemas del CRTP. Equipo de apoyo
Riesgos por fallas en el software				
Desconfiguración e interrupción de los servicios del Área de Sistemas		Reconfiguración de servicios		Encargado de Sistemas del CRTP
Pérdida de información por ataques de virus y software malicioso		Reinstalación de sistemas Limpieza de virus Actualización de antivirus Restauración de servicios		Encargado de Sistemas del CRTP
Vulnerabilidad ante ataques de hackers e intrusos		Actualizar los sistemas de prevención de intrusiones de los Sistemas Operativos		Encargado de Sistemas del CRTP
Daños a los Sistemas Operativos		Reinstalación o Restauración de Sistemas operativos. Restauración de Configuraciones		Encargado de Sistemas del CRTP
Daños a los Sistemas de Bases de Datos		Bajar los servicios		Encargado de
Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001



# PLAN DE CONTINGENCIAS

Página

7 de 22

Actualización al 7 de abril de 2007

## MATRIZ DE RIESGOS

RIESGO	ACCIONES CORRECTIVAS	RESPONSABLES
	Eliminar base dañada Restaurar base de datos Recuperar backup	Sistemas del CRTP
<b>Riesgos por interrupción de servicios</b>		
Inoperabilidad de los sistemas de aplicación	Se debe realizar una revisión periódica a la UPS.	Encargado de Sistemas del CRTP
Inoperabilidad de los sistemas de red	Se deben realizar revisiones periódicas a las instalaciones de red.	Encargado de Sistemas del CRTP
Inoperabilidad de los sistemas de telecomunicación	Depende del proveedor de servicios. Reportar fallas y daños.	Encargado de Sistemas del CRTP
Daños al Hardware por corto circuito.	Si hay daños en el Servidor central, habilitar el Servidor de Pruebas si es que es posible.	Encargado de Sistemas del CRTP
Daños a la estructura e información de las bases de datos.	Restauración de bases de datos y recuperación de backups.	Encargado de Sistemas del CRTP

## 8. Procedimientos de Emergencia y Recuperación


### 8.1. Prevención de Emergencias

Para garantizar que la Sala de Servidores esté un margen de tiempo razonable en línea, se deben prevenir los posibles incidentes de riesgo que puedan ocasionar fallas en los sistemas.

La principal acción a adoptar es la prevención de emergencias y para ello el Encargado de Sistemas del CRTP extrae copias de respaldo o Backups diarios, semanales y/o mensuales (*Ver Procedimiento de Copias de Respaldo o Backup*) que contienen las bases de datos y las aplicaciones.

Las mencionadas copias de respaldo, se encuentran ubicadas en un lugar seguro en el Area de Sistemas y están a disposición para ser empleadas en cualquier contingencia.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	---	---	---	-------------------------

	<h1>PLAN DE CONTINGENCIAS</h1>	Pagina <b>8 de 22</b>
	Actualización al 7 de abril de 2007	

## Ubicación del equipo y accesorios para utilizar ante una emergencia

- El Encargado de Sistemas del CRTP cuenta con medios magnéticos donde se encuentran las copias de respaldo de la base de datos del servidor principal de la Facultad, estas se encuentran en :
  - Una copia en CD se encuentra en un casillero en el Area de Sistemas
  - Un duplicado de las copias de respaldo que se encuentra en la computadora del Encargado de Sistemas del CRTP.

El Encargado de Sistemas del CRTP debe prestar atención a las indicaciones de emergencias potenciales, tanto dentro como fuera de la Sala de Servidores. Debe prever eventos de posibles riesgos potenciales y decidir las acciones requeridas para resolver cada situación, aplicando los procedimientos correspondientes.

El Encargado de Sistemas del CRTP contactará con anticipación al departamento de bomberos, la policía y otras autoridades locales para coordinarse con respecto al servicio que proporcionarían a la Sala de Servidores en caso de una eventualidad de riesgo.

Los siguientes requisitos, permitirán mantener un recurso de contingencia ante probables eventos de riesgo, que en caso de ocurrir, puedan mitigarse con agilidad.


## Rutas para la evacuación de la Sala de Servidores

Para garantizar que el personal del Área de Sistemas y otros que se encuentren en las proximidades de la Sala de Servidores, pueda ser evacuado sin dificultades en caso de contingencia, se requiere contar con rutas de evacuación.

En el caso del personal de Sistemas de la Facultad, existe sólo una ruta por la cual se puede realizar la evacuación desde la Sala de Servidores y es por las gradas que dan acceso al CRTP y luego a la Sala de Servidores.

La evacuación de la Sala de Servidores y del Area de Sistemas estará a cargo del Encargado de Sistemas del CRTP, el cual se encargará de avisar y supervisar el proceso de evacuación, sólo de las áreas mencionadas.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	--	---	---	-------------------------

	<h1 style="text-align: center;">PLAN DE CONTINGENCIAS</h1> <p style="text-align: center;">Actualización al 7 de abril de 2007</p>	<p style="text-align: center;">Pagina <b>9 de 22</b></p>
---	---	--

## Ubicación del equipo de emergencia

Una buena práctica de seguridad preventiva, es identificar con precisión la ubicación de todos y cada uno de los elementos del equipo de emergencia, a fin de reaccionar con oportunidad ante la ocurrencia de incendios, inundaciones u otros eventos que conlleven algún grado de riesgo, que podría afectar al personal y a las instalaciones de la Sala de Servidores.

## Equipo de respuesta a emergencias

El equipo de respuesta a emergencias, se refiere al grupo de empleados que debe asumir y adoptar la responsabilidad de reacción y ejecución de los procedimientos de emergencia, en caso de contingencias.

El Encargado de Sistemas del CRTP debe seleccionar y conformar un grupo de emergencia o de contingencia, de acuerdo a niveles jerárquicos, responsabilidades y habilidades, que puede estar formado por personal del Área de Sistemas y de otras áreas de la Facultad.

Como se muestra en el Anexo 1, los miembros del equipo seleccionado deben ser registrados en una lista en la que se cuente con la mínima información requerida para contacto y comunicación.

## Guía telefónica de emergencia

El Encargado de Sistemas del CRTP debe disponer de una lista actualizada de los números telefónicos clave de bomberos, policía, servicios de rescate, ambulancias, servicios de emergencia, y de otras autoridades.

El Anexo 2 muestra la mencionada guía, misma que debe ubicarse en un lugar visible y seguro en la Sala de Servidores. Es recomendable que el personal de la Facultad lleve consigo una copia de esta guía, para garantizar una reacción rápida.

### 8.1.1. Capacitación

La capacitación, es una actividad muy importante para la prevención de emergencias, ya que de este modo se garantiza que todo el personal responsable de las reacciones y la ejecución de las acciones preventivas, esté al tanto de sus atribuciones y de las tareas que debe cumplir en caso de contingencias.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	--	---	---	-------------------------

	<b>PLAN DE CONTINGENCIAS</b>		Pagina <b>10 de 22</b>
	Actualización al 7 de abril de 2007		

Los procedimientos de recuperación se distribuirán entre los responsables de las Áreas de Sistemas y las Áreas Usuarias y deberán estar a disposición de los empleados en caso de que la situación de contingencia requiera de su participación.

El proceso de capacitación comprende los siguientes pasos:


N°	Procedimiento	Responsable
1	Convocar al personal responsable y a los usuarios involucrados de los sistemas críticos.	Comité de Sistemas
2	Registro de asistentes al proceso de capacitación e inicio de la capacitación.	Encargado de Sistemas del CRTP
3	Una vez realizada la Capacitación, elaborar un informe de novedades para la definición de las acciones correctivas a seguir en caso de existir alguna, al Plan de Contingencias.	Encargado de Sistemas del CRTP

El Formulario que se muestra en el Anexo 3, será empleado para registrar los eventos de capacitación.

El Encargado de Sistemas del CRTP gestionara ante las instancias correspondientes el entrenamiento en cuanto a procedimientos de evacuación y de eventualidades específicas, dirigido al equipo de respuesta a emergencias. El entrenamiento consistirá en pláticas, revisiones, recorridos y ejercicios, según se requiera. El equipo de respuestas a emergencias debe estar familiarizado con:

- Organización de equipos, roles y responsabilidades.
- Rutas de evacuación y procedimientos de evacuación.
- Uso del equipo para emergencias.
- Identificación de emergencias y procedimientos de respuesta.
- Contactos telefónicos de emergencia.
- Apoyo en actividades de rescate de los bomberos, de la policía y servicios médicos, en caso que estén entrenados para ello.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	--	---	---	-------------------------

	<h1 style="text-align: center;">PLAN DE CONTINGENCIAS</h1>	<p style="text-align: center;">Pagina <b>11 de 22</b></p>
	<b>Actualización al 7 de abril de 2007</b>	

## **Cese de las operaciones normales**

En algunas circunstancias, el Encargado de Sistemas del CRTP deberá suspender las operaciones de la Sala de Servidores y darán por terminado el turno de trabajo al momento en que la situación sea de potencial riesgo, este fuera de su control y limite la continuidad de las actividades. Para ello, requerirá la autorización del Director de Carrera.

Las situaciones extremas de cese de operaciones normales pueden presentarse en casos de tormentas eléctricas severas, terremotos, inundaciones, atentados, contingencias que afecten el perímetro y estén cerca de la Sala de Servidores, o disturbios y manifestaciones civiles.


En estos casos, además del cese de operaciones, se debe evaluar la necesidad de evacuación de las instalaciones (*Ver Rutas para la evacuación de la Sala de Servidores*).

### **8.1.2. Identificación de emergencias**

Todos los empleados del Area de Sistemas comparten la responsabilidad de identificar y reportar las emergencias reales o potenciales en el trabajo. Las indicaciones más comunes de una eventualidad pueden incluir:

- Alertas por problemas de datos o de ejecución del Sistema Modelo Informacional.
- Alarmas de intrusiones o accesos no autorizados.
- Alertas sobre daños físicos a la Sala de Sistemas.
- Fugas de agua o humedad en los pisos, paredes o techos, e inundación.
- Apagones, cortos en los tableros eléctricos, cambio de voltaje, daño a las fuentes de poder.
- Ruidos fuertes, explosiones, o sonidos crujientes de incendio.
- Presencia de grupos de personas ajenas al trabajo.
- Sismos y movimientos del edificio.
- Ruidos del edificio o de fallas estructurales.
- Clima severo o vientos fuertes.
- Alertas de personas en problemas.
- Humo o fuego.
- Olores fuertes tales como gas o químicos.
- Incidentes de riesgo en el perímetro.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	--	---	---	-------------------------

	<h1 style="text-align: center;">PLAN DE CONTINGENCIAS</h1>	<p style="text-align: right;">Pagina <b>12 de 22</b></p>
	<b>Actualización al 7 de abril de 2007</b>	

El empleado que detecte problemas, primero notificara a su jefe inmediato o autoridad universitaria. El jefe de área que haya sido notificado o se entere del problema debe determinar si se trata de un problema menor (ejemplo: fuego en un cesto de basura que fácilmente puede apagar el empleado mismo con o sin ayuda), o mayor (ejemplo: un gran fuego en la Sala de Servidores que el empleado no puede apagar) y en todo caso alertar al Encargado de Sistemas del CRTP.

**Si el problema es menor**, los empleados trataran de controlarlo rápidamente, sin arriesgar su propia seguridad. El primer jefe o autoridad en llegar al área del problema asumirá el control y dará los empleados las instrucciones necesarias para resolver el problema o para evacuar el área. En el momento en que el Encargado de Sistemas del CRTP llegue al área problemática, el jefe le presentara un reporte verbal y se realizarán las acciones correspondientes.


**Si el problema es mayor**, los empleados no tratarán de resolverlo, sino que evacuarán el área y esperarán las instrucciones del Encargado de Sistemas, Director del CRTP o del Director de Carrera. El Encargado de Sistemas del CRTP asumirá el control de la situación y dirigirá la solución de la misma.

### 8.1.3. Respuestas a las emergencias

#### Alarmas

Cuando el personal se de cuenta de algo anormal en cualquier información que maneja debe dar parte al Encargado de Sistemas del CRTP para que este a su vez tome las medidas que el caso aconseje.

	<b>Plan de Acción</b>		<b>Procedimientos a seguir</b>	
Desarrollado por:  Fernando Echavarria	1. Notificación del personal de anomalías.		Revisión del o los equipos.	
	2. Prueba del equipo.		Se probará el alcance del problema y se aislará la falla.	
	3. Paro del equipo		Informando al personal de la Facultad que dio la alarma que se restaurará su equipo, los equipos o la totalidad del lote informático (todo lo relacionado a sistemas: servidores, PCs, etc)	
	4. Coordinación de la		Se comenzará con la recuperación del	
	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001

	<h1 style="text-align: center;">PLAN DE CONTINGENCIAS</h1>	Pagina <b>13 de 22</b>
	Actualización al 7 de abril de 2007	

respuesta.	lugar que presenta la falla.
5. Puesta en línea	Se probará que la falla ha sido superada.

### Restauración parcial

Durante una restauración parcial, el personal afectado dejará de realizar sus tareas sin perjuicio a los demás empleados que siguen trabajando normalmente excepto que los mismos se encuentren en la cadena laboral.

El personal afectado deberá preparar su documentación y copias de respaldo para poder restaurar archivos o información que no se haya introducido entre la hora de copia de respaldo y la hora del incidente.

### Fugas de agua o humedad en los pisos, paredes o techos

Los empleados que detecten agua en el piso, en un área que muestre señas de riesgo de electrificación, no deberán pisar el agua. Si hay cajas eléctricas inundadas, el jefe del área o autoridad universitaria del área afectada debe localizar y bajar el interruptor de energía eléctrica que controla la caja. En caso de que se detecte humedad en losas o muros, los empleados no deberán tratar de investigar el problema. Los jefes y el Encargado de Sistemas del CRTP deberán bajar (desconectar) todos los interruptores de energía eléctrica y notificar al departamento de servicios correspondiente para que investigue y en su caso corrija el problema.

### Cortos en los tableros eléctricos (chispas)


Los empleados no deben investigar o tratar de corregir cortos circuitos o chispas asociadas con los tableros eléctricos, contactos o equipos. El Encargado de Sistemas del CRTP debe bajar (desconectar) los interruptores de suministro de energía eléctrica del área y notificar a ELECTROPAZ para que investigue y en su caso corrija el problema.

### Sismos y movimientos del edificio

En caso de sismos o movimientos del edificio, los empleados deben mantener la calma, si escuchan una alarma preventiva procederán de inmediato a desalojar las instalaciones y ubicarse en una área abierta que previamente se haya definido. Si no se tiene tiempo de evacuar las instalaciones deberán resguardarse bajo los marcos de las puertas, escritorios, o mesas. Una vez que el movimiento telúrico

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	--	---	---	-------------------------



	<h1 style="text-align: center;">PLAN DE CONTINGENCIAS</h1>	<p style="text-align: center;">Pagina <b>14 de 22</b></p>
	<b>Actualización al 7 de abril de 2007</b>	

haya terminado, los empleados, sin esperar a que se les ordene, iniciarán la evacuación ordenada de las instalaciones.

### **Amenazas telefónicas y amenazas de bombas**

Durante las operaciones normales del Area de Sistemas y de la Sala de Servidores, cualquier persona que conteste un teléfono, esta sujeta a recibir amenazas telefónicas dirigidas contra las instalaciones o contra el personal del Area de Sistemas ver Anexo 4. Siempre y en todos los teléfonos deberá haber por lo menos una copia de la forma para amenaza de bomba, ver Anexo 5.

El personal que reciba una amenaza por teléfono deberá emplear la forma que muestra el Anexo 4 o 5 para documentar todas las amenazas telefónicas. La persona que reciba la llamada hará lo siguiente:

- a) Tratar todas las amenazas como hechos reales.
- b) No elaborará supuestos a cerca de los motivos presentados por el amenazante.
- c) Notificará únicamente al jefe inmediato, autoridad universitaria o al Encargado de Sistemas del CRTP.
- d) No comentará la amenaza con otros empleados, hasta que la situación esté bajo control o hasta que las autoridades a cargo indiquen lo contrario.


El Encargado de Sistemas del CRTP rápidamente evaluará la amenaza, después de analizar la situación puede coordinar la evacuación del personal, antes de que la policía se presente a realizar la búsqueda y se encargue de los objetos que resulten sospechosos, inmediatamente hará el reporte de la amenaza de bomba a la policía y al equipo de respuesta de emergencia para que realice la búsqueda en la Sala de Servidores.

El equipo efectuara la búsqueda en todas las áreas, dentro y fuera de las instalaciones, en los patios, corredores, baños y áreas de almacenamiento. En caso de que se identifique un objeto sospechoso, se deberá notificar inmediatamente al Encargado de Sistemas del CRTP o a la persona a cargo. Bajo ninguna circunstancia deberá ningún empleado tocar o mover el objeto.

### **Incendio**

En caso de incendio, el personal debe alertar inmediatamente al grupo de emergencia o comunicarse con la unidad de bomberos. Como medida de prevención, en caso de poder controlar el fuego, emplee los extintores que se encuentran disponibles.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	--	---	---	-------------------------


	<h1 style="text-align: center;">PLAN DE CONTINGENCIAS</h1> <p style="text-align: center;">Actualización al 7 de abril de 2007</p>	<p style="text-align: right;">Pagina <b>15 de 22</b></p>
---	---	--

## Evacuación de las instalaciones

Cuando se identifica y se investiga una situación de emergencia, el Encargado de Sistemas del CRTP ordenará una evacuación ya sea parcial o total de la Sala de Servidores y del Area de Sistemas en general, incluyendo el CRTP. Si se ordena una evacuación parcial, el Encargado de Sistemas del CRTP monitoreará la situación personalmente y ordenará la evacuación total, una vez que este justificada. El proceso de evacuación se realizará conforme a los siguientes pasos:

1. Notificar al personal	Informando a todo el personal del Area de Sistemas y del CRTP que hay una evacuación en progreso.
2. Mover al personal	Evacuar a los empleados del Area de Sistemas y del CRTP y reunirlos en un área de recuperación seleccionada, alejada de las instalaciones.
3. Paro del equipo	Para minimizar los riesgos de descargas eléctricas y daños al equipo.
4. Asegurar las instalaciones	Para proteger la Sala de Servidores durante la situación de emergencia contra robo, vandalismo, etc.
5. Notificar a las autoridades	Informando a la policía, los bomberos, los rescatistas y a otras dependencias de apoyo en caso de la eventualidad de que las instalaciones han sufrido una emergencia.
6. Coordinar la respuesta	Para establecer un punto de control dentro del área de recuperación para comunicar la información del suceso y coordinarse con la policía, los bomberos y otras autoridades.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	--	---	---	-------------------------

	<div style="text-align: center;"> <h1>PLAN DE CONTINGENCIAS</h1> </div>	<div style="text-align: center;"> <p>Página</p> <p><b>16 de 22</b></p> </div>
	<p>Actualización al 7 de abril de 2007</p>	

## Evacuación parcial

Durante una evacuación parcial, la autoridad universitaria o el jefe del área afectada será el encargado de conducir a sus empleados y visitantes fuera del edificio y reunirá a los empleados y visitantes en el área de recuperación establecida. Los empleados que estén siendo evacuados, no deberán bloquear los corredores, ni interferir con los demás empleados que siguen laborando. Estos deberán permanecer alertas a las instrucciones del Encargado de Sistemas del CRTP, autoridad universitaria o de su jefe de área.

En caso de que el Decano o Vicedecano lo instruya, los jefes de las áreas no afectadas iniciarán el paro ordenado de sus operaciones, la evacuación de su personal y el regreso de su documentación, tomando en cuenta los siguientes aspectos:

- Evacuar a cualquier empleado con alguna minusvalía física y pedirles a todos los proveedores, al personal de servicio y a los visitantes que dejen de trabajar y salgan de las instalaciones.
- Guardar documentación y disquetes como sea posible, efectuar el respaldo y apagar tanto equipo de computación como sea posible. ¡No se deben apagar las luces!

Al abandonar las instalaciones, el Encargado de Sistemas del CRTP se llevará consigo los últimos respaldos.


El Decano será quien decida si es que los empleados tienen que regresar a trabajar o no en caso de que se desarrolle una eventualidad de riesgo. Los empleados no abandonarán el área de recuperación hasta que no sean verbalmente liberados por el Decano.

El área de recuperación será en un lugar seleccionado por el Encargado de Sistemas del CRTP como puede ser uno de los patios del edificio o algún lugar donde no corran peligro los empleados.

## Evacuación total

Si el Decano, Vicedecano o Director de Carrera ordenara una evacuación total, se llevara a cabo una evacuación de emergencia de acuerdo con los siguientes pasos:

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	--	---	---	-------------------------

	<h1 style="text-align: center;">PLAN DE CONTINGENCIAS</h1>	<p style="text-align: center;">Pagina <b>17 de 22</b></p>
	<b>Actualización al 7 de abril de 2007</b>	

## **a) Notificar al personal**

El Director de Carrera anunciará una “evacuación total” y se asegurará de que todos los jefes entiendan e inicien el proceso de evacuación. El Encargado de Sistemas del CRTP se asegurará de que todos los empleados, proveedores y visitantes de sistemas sean notificados.

## **b) Movilización del personal**

Los empleados deben permanecer calmados, escuchar y obedecer las instrucciones del Encargado de Sistemas del CRTP y/o sus jefes. Bajo las instrucciones de sus jefes, los empleados se moverán inmediatamente, no desperdiciarán el tiempo recogiendo sus efectos personales y permanecerán en silencio (con el propósito de que todos puedan escuchar las instrucciones).


Los jefes se asegurarán de que todos los empleados, proveedores o visitantes detengan sus trabajos, apaguen sus terminales y sigan la trayectoria de evacuación asignada para salir de las instalaciones. Los jefes se asegurarán de que el personal evacue el edificio rápidamente. Los jefes permanecerán serenos y mantendrán la calma comunicando sus instrucciones con claridad (repitiendo hasta que todo el personal las entienda).

Los jefes seguirán a su personal fuera del edificio y lo dirigirán al área de recuperación localizada lejos de las instalaciones. Los jefes reunirán y contarán a su personal (para asegurarse de que todo el personal bajo su cargo haya salido del edificio y se encuentre en el área de recuperación). De la misma manera, deberán tratar de hacer un conteo de las personas determinadas como ausentes.

Los jefes de área se posicionarán a si mismos a lo largo de la ruta de evacuación asegurándose de que el personal salga sin demora, avance rápidamente, hacia abajo (o hacia arriba) por las escaleras, a través de las puertas y a lo largo de los corredores. En ciertos casos, los jefes serán los que ordenen el avance o la espera del personal para que circulen.

Una vez que el personal haya salido de las instalaciones, el equipo de respuesta y los jefes inspeccionarán las áreas de trabajo para asegurarse de que todo el personal haya salido. Si el edificio consta de mas de un piso, los jefes deben empezar su inspección desde el piso más alto e ir descendiendo en su búsqueda.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	--	---	---	-------------------------

	<div style="text-align: center;"> <h1>PLAN DE CONTINGENCIAS</h1> </div>	<div style="text-align: center;"> <p>Página</p> <p><b>18 de 22</b></p> </div>
	<div style="text-align: center;"> <p><b>Actualización al 7 de abril de 2007</b></p> </div>	

El Director de Carrera actuará como punto focal para proporcionar información acerca de la eventualidad a la policía, a los bomberos, al personal de rescate y a otras autoridades que lleguen al área de recuperación. Cuando el equipo de respuesta llegue al área de recuperación, llevarán a cabo: el control del personal y gente ajena a la fundación; proporcionarán primeros auxilios a las personas heridas; trabajarán con la policía, los bomberos, los rescatistas y otro personal de apoyo y ayudarán en el control de las personas de los medios de comunicación masivos.

El Decano, Vicedecano o Director de Carrera controlará a los periodistas y reporteros y les comunicará toda la información relacionada con la emergencia. El Encargado de Sistemas del CRTP mantendrá informado al personal del Area de Sistemas y liberará al personal, según se requiera, para apoyar en la solución de la emergencia.

#### **8.1.4. Evaluación de daños**

Una vez que los equipos principales de la Sala de Servidores estén restaurados, el Encargado de Sistemas del CRTP tendrá que realizar la tarea de evaluar los daños y restaurar las plataformas de las instalaciones, para luego comunicárselas al Comité de Sistemas.


Si se aprueba la evaluación de daños y de seguridad, el Encargado de Sistemas del CRTP dirigirá al personal para una evaluación de los datos. Primero se evaluará en cuanto a la información almacenada y después se determinará la cantidad del daño a las instalaciones, al equipo, los documentos y los recursos de la Sala de Servidores para elaborar un plan de acción correctiva.

El Encargado de Sistemas llevará a cabo una evaluación del daño de la Sala de Servidores y generará un informe de emergencias que será elevado al Comité de Sistemas.

Una vez realizadas las acciones correctivas, y verificada la conformidad con los usuarios, se liberará el sistema en producción.

Una vez que el personal del Area de Sistemas y de las áreas usuarias afectadas este a salvo y reunido en el área de recuperación y que la policía y las autoridades de respuesta a emergencias (policía, bomberos, rescatistas, etc.) hayan terminado sus labores para la contención de la emergencia, se tendrá que realizar la tarea de evaluar los daños y de restablecer la recuperación de las instalaciones.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	--	---	---	-------------------------

	<h1>PLAN DE CONTINGENCIAS</h1>	Pagina <b>19 de 22</b>
Actualización al 7 de abril de 2007		

En la mayoría de los casos, el Encargado de Sistemas tendrá que trabajar junto con la policía, los bomberos y otras autoridades de emergencia para poder determinar si la Sala de Servidores es segura en cuanto al regreso del personal para efectuar una evaluación de daños. Se debe obtener la autorización de la policía, los bomberos y otras autoridades para casos de desastre, antes de permitir la entrada del personal a las instalaciones.

Si se aprueba la evaluación de daños y de seguridad, el Encargado de Sistemas del CRTP dirigirá al personal del equipo de respuesta a la emergencia en una evaluación de la Sala de Servidores. Primero se evaluará en cuanto a seguridad en su conjunto y después se determinará la cantidad del daño a las instalaciones, al equipo, los documentos y los recursos de la Sala de Servidores.

El equipo de recuperación deberá vigilar que nadie del personal incurra en un riesgo por realizar la evaluación de daños. El equipo de recuperación llevará a cabo una evaluación del daño de la Sala de Servidores y llenará un reporte de emergencias por escrito y lo entregará al Decano, Vicedecano o Director de Carrera.

Basándose en la evaluación del equipo de recuperación de emergencias y con la aprobación del Decano, Vicedecano o Director de Carrera, el Encargado de Sistemas del CRTP determinará si es que se inicia el proceso para la recuperación de la Sala de Servidores o bien deja ir a los empleados hasta que se lleve a cabo una evaluación mas completa y se implemente un enfoque para la recuperación.

## 8.2. Recuperación

### 8.2.1. Plan Detallado

El presente Plan es una guía de procedimientos para recuperar los servidores de la Facultad.


Los procedimientos a seguir son:

#### Recuperación del Servidor de Producción

##### Recuperación mediante la transferencia de datos del servidor de producción al servidor de desarrollo

Por esta opción se entiende que se intercambia el servidor de Desarrollo a Producción y viceversa, como ambos servidores tienen instalado el Sistema Modelo Informacional, no deberían presentarse problemas. Sin embargo, será

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	--	---	---	-------------------------

	<h1 style="text-align: center;">PLAN DE CONTINGENCIAS</h1>	<p style="text-align: center;">Pagina <b>20 de 22</b></p>
	<b>Actualización al 7 de abril de 2007</b>	

necesario recuperar la última copia de respaldo de la base de datos en el servidor de desarrollo.

Una vez realizado esto, los usuarios podrán ingresar al Sistema utilizando la misma ruta de acceso.

### **Recuperación mediante reinstalación del servidor**

Se toma como opción la referenciada cuando se debe recuperar íntegramente el servidor, y este debe ser instalado desde “cero”, utilizando software original, y seguidamente las configuraciones originales y particulares del servidor de Producción.

### **Pasos para Instalar el servidor de la Facultad**

- 1) Se debe instalar Linux Red Hat.
- 2) Se debe instalar el DBMS Postgress v. 7.4.
- 3) Se debe instalar el programa J2SDK v.1.4.2.
- 4) Se debe recuperar la base de datos utilizando para ello la última copia de respaldo obtenida.

Concluida la re-instalación del servidor, este se encuentra habilitado para su funcionamiento correcto dentro de la Facultad.

Si la eventualidad es menor y los daños limitados, el Encargado de Sistemas del CRTP puede dar instrucciones para que se inicie una recuperación parcial o completa de la Sala de Servidores.


Los jefes de área y autoridades administrativas recibirán instrucciones para autorizar limpiar sus áreas, evaluar el daño específico de sus equipos y documentación y analizar la viabilidad para reiniciar las operaciones (tratando de reiniciar los sistemas de computación).

Una vez que haya pasado el periodo de emergencia menor, el Encargado de Sistemas del CRTP primero se asegurará de que las instalaciones no tengan daño alguno para regresar a sus condiciones normales de operación.

El Encargado de Sistemas del CRTP ejercerá un cuidado extremo en la inspección de las instalaciones antes de permitir el acceso a los empleados.

El Encargado de Sistemas del CRTP personalmente verificará la seguridad del mismo antes de permitir la entrada del personal. Una vez que esta haya sido

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	--	---	---	-------------------------

	<div> <div>PLAN DE CONTINGENCIAS</div> <div>Actualización al 7 de abril de 2007</div> </div>	<div> <div>Página</div> <div>21 de 22</div> </div>
---	--	--

verificada, dará instrucciones verbales al equipo de respuesta para que vuelvan los empleados a la Sala de Servidores a reasumir sus funciones.

El equipo de recuperación también deberá llevar a cabo una investigación post-emergencia y presentara un reporte por escrito de los hallazgos, las conclusiones y las recomendaciones al Decano, Vicedecano o Director de Carrera, para su revisión.

El Formulario que se muestra en el Anexo 6, será empleado para registrar los sucesos de los incidentes.

Los empleados deben reintegrarse a su área de trabajo en forma ordenada. Los jefes se asegurarán de que todos sus empleados regresen al área de trabajo con el mínimo de demora.

El Encargado de Sistemas del CRTP debe regresar los respaldos magnéticos en su poder, retirados al ocurrir la eventualidad.

Si es que el daño ocasionado por la contingencia pone en peligro la seguridad de los empleados, el Decano, Vicedecano o Director de Carrera puede licenciar a los empleados de sus labores una vez que haya pasado el periodo de emergencia. Los empleados no podrán abandonar el área de trabajo hasta que no hayan sido verbalmente liberados por el Decano, Vicedecano o Director de Carrera.

Si se trata de una emergencia mayor, el Decano, Vicedecano o Director de Carrera determinará la necesidad real de personal, en adición al equipo de respuesta a la emergencia y licenciará al resto del personal una vez que se hayan deslindado responsabilidades. El Decano, Vicedecano o Director de Carrera debe determinar la severidad del evento y su impacto en las operaciones y debe informar a todos los empleados.


El Encargado de Sistemas del CRTP deberá aplicar la estrategia de recuperación para la Sala de Servidores. Una vez que hayan recibido la aprobación por parte del Decano, Vicedecano o Director de Carrera, informando al personal acerca de dicha estrategia de recuperación.

### Operaciones de rescate

Se requerirá del Encargado de Sistemas del CRTP y los jefes de área para llevar a cabo operaciones de rescate menores para restaurar totalmente la operación de la Sala de Servidores.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	--	---	---	-------------------------



	<h1 style="text-align: center;">PLAN DE CONTINGENCIAS</h1>	<p style="text-align: center;">Pagina <b>22 de 22</b></p>
	<b>Actualización al 7 de abril de 2007</b>	

El Encargado de Sistemas del CRTP pondrá en marcha el plan con los empleados designados que le ayudarán en estas operaciones de rescate, siempre y cuando el trabajo requerido quede dentro de las capacidades físicas de los empleados y no involucre riesgo para ellos.

Durante la operación de rescate, el Encargado de Sistemas del CRTP, los jefes de área, y los empleados reportarán cualquier problema potencial de seguridad.

### 8.3. Pruebas al Plan de Contingencias

Con el objetivo de establecer posibles ajustes al Plan es necesario realizar pruebas programadas y planificadas para este fin.

La periodicidad establecida inicialmente es de al menos una prueba anual del Plan de Contingencias.

Para este fin el Encargado de Sistemas del CRTP debe planificar dichas pruebas y liderar las mismas, convocando para ello a las personas que considere necesario y estableciendo las responsabilidades de cada uno de los participantes de las pruebas.


Estas pruebas pueden ser totales o parciales. Sin embargo en el transcurso de un año se debe llegar a probar todos los aspectos mencionados en el presente Plan.

Con el objetivo de no perjudicar el desarrollo normal de las actividades de los usuarios de la Facultad que utilizan los sistemas principales, será conveniente planificar estas pruebas en horas no laborables o durante los fines de semana.

Para documentar los aspectos evaluados en las pruebas al Plan de Contingencias, el Anexo 7 presenta un formulario a ser llenado en cada prueba realizada.

Concluida la prueba, el Encargado de Sistemas del CRTP debe generar un informe a ser elevado al Director del CRTP y al Director de Carrera, el cual debe incluir el detalle de las pruebas realizadas, los resultados, las conclusiones y acciones a seguir en caso de que el Plan requiera algunos ajustes o mejoras.

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL / 001
--	---	---	---	-------------------------

	<b>PLAN DE CONTINGENCIAS (ANEXOS)</b>	<b>Pagina</b> <b>1 de 7</b>
	<b>Actualización al 8 de abril de 2007</b>	

## ANEXO 1 Listado de los Grupos de Emergencia y Apoyo


### GRUPO DE EMERGENCIA PARA LA EJECUCION DEL PLAN DE CONTINGENCIAS

Paterno	Materno	Nombres	Dirección	Teléfono

### GRUPO DE APOYO PARA LA EJECUCION DEL PLAN DE CONTINGENCIAS

Paterno	Materno	Nombres	Dirección	Teléfono

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL.A / 001
--	--	---	---	---------------------------

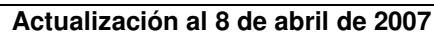
	<b>PLAN DE CONTINGENCIAS (ANEXOS)</b>	<b>Página</b>  <b>2 de 7</b>
	<b>Actualización al 8 de abril de 2007</b>	

## ANEXO 2 Lista de Teléfonos de Emergencia


### TELÉFONOS DE EMERGENCIA

INSTITUCIÓN DE EMERGENCIA	TELÉFONO
Radio Patrulla	110
Ambulancias	118
Bomberos	119
PAC	120
Reten de Emergencias de la HAM de La Paz	134
Grupo de Rescate	138
ELECTROPAZ	2333300
CRUZ ROJA BOLIVIANA	2227818
HOSPITAL DE CLINICAS	2229180
TRANSITO LA PAZ	2371224
POLICIA CAMINERA	2211214
EPSAS	2211222
SAR ILLIMANI FAB	2844040
HOSPITAL DEL NIÑO	2245154
AEROPUERTO	2810140
TRANSITO EL ALTO	2845059

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL.A / 001
--	--	---	---	---------------------------




Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL.A / 001
--	--	---	---	---------------------------

	<b>PLAN DE CONTINGENCIAS (ANEXOS)</b>	<b>Pagina</b> <b>4 de 7</b>
	<b>Actualización al 8 de abril de 2007</b>	

#### **ANEXO 4 Forma de registro de llamada de amenaza de Bomba**

REPORTER DE AMENAZA DE BOMBA					
<b>a) Escriba literalmente las palabras de la persona que llama.</b> Si fuese posible indague datos sobre la ubicación del dispositivo, forma, lugar en la que la instalaron, a qué grupo representa, etc.					
<b>b) Inmediatamente cuelgue el auricular, registre los siguientes datos.</b> Registre los datos que recuerde y los datos del teléfono al cual ingresó la llamada.					
Número de Teléfono:					
Fecha y Hora de recepción:					
Tiempo de llamada:					
Por la voz identifique:	<b>Varón</b>	Sí	No	<b>Mujer</b>	Sí No
<b>c) Otros comentarios u observaciones.</b>					
<b>d) Registre sus datos personales.</b>					
Nombre del Empleado:					
Cargo en la Fundación:					
Número telefónico personal:					


Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL.A / 001
--	--	---	---	---------------------------

	<b>PLAN DE CONTINGENCIAS (ANEXOS)</b>	<b>Pagina 5 de 7</b>
	<b>Actualización al 8 de abril de 2007</b>	

## ANEXO 5 Forma de registro de llamada de amenaza telefónica

REPORTER DE AMENAZA TELEFÓNICA					
<b>a) Escriba literalmente las palabras de la persona que llama.</b> Si fuese posible indague más datos sobre la persona que llama y el origen de la llamada, ciudad, país, etc.					
<b>b) Inmediatamente cuelgue el auricular, registre los siguientes datos.</b> Registre los datos que recuerde y los datos del teléfono al cual ingresó la llamada.					
Número de Teléfono:					
Fecha y Hora de recepción:					
Tiempo de llamada:					
Por la voz identifique:	<b>Varón</b>	Sí	No	<b>Mujer</b>	Sí No
<b>c) Otros comentarios u observaciones.</b>					
<b>d) Registre sus datos personales.</b>					
Nombre del Empleado:					
Cargo en la Fundación:					
Número telefónico personal:					

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL.A / 001
--	--	---	---	---------------------------


	<b>PLAN DE CONTINGENCIAS (ANEXOS)</b>	<b>Página</b>  <b>6 de 7</b>
	<b>Actualización al 8 de abril de 2007</b>	

## ANEXO 6    Formulario de Registro de Incidentes

REGISTRO DE INCIDENTES			
<b>Nombre del Involucrado:</b>	<b>Fecha del incidente:</b>	<b>Hr. Inicio:</b>	<b>Hr. Fin:</b>
<b>Área en la que se produjo:</b>			
<b>Tipo de Incidente</b>	<b>Descripción del incidente</b>		
a)    Incidente Natural.			
b)    Incidente del entorno.			
c)    Incidente Humano.			
<b>Consecuencias identificadas, acciones, reacciones adoptadas y observaciones:</b>  <div style="border: 1px solid black; height: 150px; margin-top: 5px;"></div>			
<i>En caso necesario adjunte las hojas que requiera.</i>			

Personal involucrado	Administrador de Sistemas
----------------------	---------------------------

Desarrollado por:	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL.A / 001
Fernando Echavarria				

	<h2 style="text-align: center;">PLAN DE CONTINGENCIAS (ANEXOS)</h2>	<b>Página</b> <b>7 de 7</b>
	<b>Actualización al 8 de abril de 2007</b>	

### ANEXO 7    Formulario de Registro de Pruebas del Plan de Contingencias

REGISTRO DE PRUEBAS DEL PLAN DE CONTINGENCIAS			
Nombre del Involucrado:	Fecha de la prueba :	Hr. Inicio:	Hr. Fin:
<b>Area :</b>			
<b>Contingencia probada</b>		<b>Función realizada</b>	
a)	Identificación de emergencias		
b)	Respuesta a emergencias		
c)	Evacuación total		
d)	Evacuación parcial		
e)	Identificación de equipo de emergencia.		
f)	Revisión de guías telefónicas		
g)	Llamadas telefónicas		
h)	Rescate		
i)	Primeros Auxilios		
<b>Observaciones:</b>  <i>En caso necesario adjunte las hojas que requiera.</i>			

Personal involucrado

Encargado de Sistemas del CRTP

Desarrollado por:  Fernando Echavarria	Revisión: Encargado de Sistemas del CRTP: Edson Quispe	Revisión: Dirección del CRTP: Max Arnsdorff	Aprobación: Dirección de Carrera: Roberto Moreira	Código:  PL.A / 001
--	--	---	---	---------------------------