POLÍTICA INFORMÁTICA

CENTRO REGIONAL DE INVESTIGACIONES MULTIDISCIPLINARIAS

UNAM

FECHA DE APROBACIÓN:

Mayo 2019

Política Informática (Cuarta versión)

MAYO 2019

Índice

Introducción

Con base en lo establecido en el artículo 5, fracción VIII, así como en el artículo 43, fracción VII, sección sexta artículos del 61 al 63, del Reglamento Interno del CRIM, se hace necesario contar con una política informática que oriente el crecimiento y renovación de la infraestructura.

Se entiende por política informática al conjunto de planes, programas y acciones en el ámbito de tecnologías para el tratamiento de la información, la protección y la seguridad de los datos y medios informáticos.

La política informática guía las formas y la actuación del personal del CRIM, así como de cualquier otra persona con acceso a los recursos y servicios informáticos. A través de ésta se declaran los principios sobre los cuales se cimenta la operación de los sistemas de información y comunicación del CRIM.

A partir de la presente política se desarrollarán los reglamentos en los cuales se detallen los procedimientos y formas específicas de cada aspecto aquí señalado.

Capítulo 1 - DE LOS TIPOS DE USUARIO

1.1 Usuario administrador

El usuario administrador es aquel integrante del Departamento de Sistemas de Información y Comunicación (DSIC) del CRIM, que tiene todos los privilegios y características que permiten operar completamente un sistema y/o servidor, de acuerdo con las responsabilidades que tiene asignadas.

1.1.1 Responsabilidades

a) Garantizar que los sistemas y servicios estén disponibles para todos los usuarios y que la información se procese y transfiera correctamente.
b) Realizar respaldos de la información y configuración residente en los sistemas y equipos a su cargo, verificando que se hayan realizado correctamente.
c) Restaurar la información derivada de los respaldos que realiza, en caso de ser necesario.
d) Realizar las actualizaciones y configuraciones que se requieran en los sistemas y equipos a su cargo, para asegurar el correcto funcionamiento y seguridad de éstos.
e) Orientar a los usuarios en el uso y manejo de los equipos, aplicaciones e infraestructura de cómputo.
f) Entregar todas las credenciales de acceso a servidores y sistemas al finalizar la relación laboral.
g) El nuevo usuario administrador a cargo deberá cambiar de forma inmediata todas las contraseñas cuando un administrador de su área deje de prestar sus servicios.

1.2 Usuario interno

Se considera usuario interno, a todo el personal académico y administrativo del CRIM que tenga un equipo de cómputo asignado.

1.2.1 Responsabilidades

a) Conservar en buen estado y funcionamiento los equipos e infraestructura de cómputo de conformidad con las políticas de uso y seguridad informática establecidos en el CRIM.
b) Solicitar a través de los mecanismos establecidos el uso de los servicios que ofrece el Departamento de Sistemas de Información y Comunicación (DSIC).

1.3 Usuario invitado

Se considera como usuario invitado, a toda persona que se encuentre trabajando de forma temporal en labores académicas o administrativas, bajo la coordinación y responsabilidad de un integrante de la comunidad del CRIM.

1.3.1 Responsabilidades

a) Conservar en buen estado y funcionamiento los equipos e infraestructura de cómputo de conformidad con las políticas de uso y seguridad informática establecidos en el CRIM.
b) Solicitar a través de los procedimientos establecidos el uso de los servicios que ofrece el Departamento de Sistemas de Información y Comunicación (DSIC).

Capítulo 2 - DE LOS EQUIPOS DE CÓMPUTO Y PERIFÉRICOS

2.1 Solicitud y adquisición

El área autorizada para presentar ante la Secretaría Administrativa las solicitudes de compra de equipo de cómputo y periféricos es el DSIC, independientemente de que se trate de recursos de presupuesto UNAM o de proyectos extraordinarios (PAPIIT, PAPIME, CONACyT, etc.), por lo cual los interesados en adquirir equipo deberán acudir a dicho departamento, el cual realizará el análisis de las necesidades informáticas, para definir las características del mismo y asegurar que sea compatible con la infraestructura del CRIM y cumpla con la normatividad universitaria.

El DSIC presentará las solicitudes de equipo ante la Comisión de Política Informática (CPI) para su revisión y visto bueno. La Secretaría Administrativa realizará las adquisiciones de conformidad con la disponibilidad presupuestal y en apego a los trámites y procedimientos vigentes.

2.2 Asignación y resguardo

Se asignará equipo de cómputo y periféricos a todo el personal académico y administrativo del CRIM que así lo requiera para el desarrollo de sus actividades.

Todos los equipos de cómputo deberán estar disponibles en el CRIM, para efectos de revisión y mantener actualizado el censo de cómputo.

Los equipos de cómputo, cualesquiera que éstos fueran, no pueden transferirse, moverse o trasladarse a otros lugares sin el previo consentimiento del DSIC y la Secretaría Administrativa.

En el caso del equipo de cómputo adquirido con recursos extraordinarios, al término del proyecto, el responsable debe entregarlo para su reasignación y en caso de requerirlo, se dará preferencia al resguardante.

Todo personal que termine su relación laboral con el CRIM, debe entregar al DSIC los recursos informáticos (equipos de cómputo o periféricos), que se le hayan asignado durante su estancia en el Centro.

2.2.1 Equipos de escritorio

Se asignará un equipo de escritorio a todo el personal académico y administrativo del CRIM que así lo requiera para el desarrollo de sus actividades. Se podrá asignar equipo adicional al personal de apoyo, siempre y cuando haya disponibilidad de equipo, previa autorización de la CPI, quedando también ese equipo bajo resguardo del integrante de la comunidad responsable.

2.2.2 Equipos portátiles

Se podrán asignar equipos portátiles a quienes requieran realizar trabajo de campo o en consideración al tipo de labores que desempeñan.

2.2.3 Equipos periféricos

Se privilegiará que los equipos periféricos tales como impresoras, escáneres, multifuncionales, etc., sean de uso común para un área específica, bajo la responsabilidad del titular de dicha área con el fin de mejorar el servicio y el control de los consumibles.

Se podrán asignar equipos periféricos tales como impresoras, escáneres, multifuncionales, etc., previa justificación y aprobación de la CPI, a los usuarios que así lo requieran.

2.3 Baja de equipo

2.3.1 Por robo o extravío

En caso de robo o extravío de equipo de cómputo del CRIM, el usuario resguardante deberá notificar al DSIC, para que se tomen las medidas preventivas de protección a la infraestructura.

Asimismo, deberá levantar un acta administrativa de hechos ante del Departamento de Bienes, Suministros y Servicios Generales del CRIM, y generar una denuncia ante el Ministerio Público.

2.3.2 Obsolescencia o falla

El DSIC es el encargado de revisar todo el equipo de cómputo y catalogarlo como obsoleto cuando su rendimiento y procesamiento sea insuficiente y no sea posible actualizar su hardware para mejorar estas condiciones.

El DSIC hará la solicitud de baja ante del Departamento de Bienes, Suministros y Servicios Generales del CRIM.

2.4 Préstamo de equipo

Se podrá prestar equipo de cómputo, periféricos y proyectores exclusivamente al personal del CRIM. Todas las solicitudes deberán realizarse ante el DSIC vía correo electrónico a la dirección sistemas@crim.unam.mx, con una antelación de tres días hábiles a la fecha en que sea requerido el equipo. El préstamo estará sujeto a disponibilidad.

El usuario tiene la obligación de revisar el equipo al momento de recibirlo y entregarlo, así como de notificar al encargado del área de cualquier anomalía encontrada. En caso de no hacerlo, el usuario deberá hacerse responsable de solventar la reposición o reparación del equipo o accesorio dañado o faltante.

2.5 Mantenimiento preventivo y correctivo

El DSIC es el encargado de coordinar el mantenimiento preventivo de los equipos de cómputo y periféricos del CRIM, el cual deberá realizarse dos veces por año.

En caso de que se presente alguna falla o malfuncionamiento, el usuario deberá notificar al DSIC para la revisión del equipo y en su caso, su reparación.

Capítulo 3 - DEL USO DE DISPOSITIVOS MÓVILES Y EQUIPOS PERSONALES

Los usuarios invitados que estén interesados en obtener acceso a la red del CRIM para sus dispositivos móviles y equipos personales, deben presentar su solicitud ante el DSIC, para que le sean concedidos los permisos de acceso necesarios y se tenga un registro del dispositivo.

Los usuarios visitantes podrán hacer uso de la red creada para este fin, la cual cuenta con accesibilidad básica.

Capítulo 4 - DE LAS APLICACIONES DE SOFTWARE Y LICENCIAMIENTO

4.1 Solicitud y adquisición

El área autorizada para presentar ante la Secretaría Administrativa las solicitudes de compra de software y licenciamiento es el DSIC, independientemente de que se trate de recursos de presupuesto UNAM o de proyectos extraordinarios (PAPIIT, PAPIME, CONACyT, etc.), por lo cual los interesados en adquirir software deberán acudir a dicho departamento, el cual realizará el análisis de necesidades para definir las características del mismo y asegurar que sea compatible con la infraestructura del CRIM y cumpla con la normatividad universitaria.

El DSIC presentará las solicitudes de adquisición de software ante la CPI para su revisión y visto bueno. La Secretaría Administrativa realizará las adquisiciones de conformidad con la disponibilidad presupuestal y en apego a los trámites y procedimientos vigentes.

4.2 Asignación

Los usuarios deberán solicitar al DSIC la instalación del software requerido para el desarrollo de sus actividades académico-administrativas. El software solicitado sólo podrá ser instalado en equipo de cómputo con número de inventario de la UNAM. La instalación de software en los equipos deberá ser realizada o en su caso validada por el DSIC. En equipos de la UNAM no se podrá instalar software que no sea original o sin licenciamiento.

El DSIC realizará revisiones periódicas del equipo de cómputo, así como del software instalado en los mismos, a fin de conservar su buen funcionamiento y vigilar que se cumpla con la normatividad de la UNAM.

El trámite para la renovación y actualización del software y su licenciamiento es responsabilidad del DSIC, el cual deberá realizarse ante la Secretaría Administrativa.

Capítulo 5 - DE LOS SERVICIOS

5.1 Soporte Técnico

Las solicitudes de soporte técnico serán atendidas por el DSIC y los tiempos de respuesta serán de acuerdo con las tablas de impacto y urgencia definidos para cada servicio.

El horario establecido para la atención de soporte técnico es de 9:00 a 18:00 horas en días hábiles.

Las solicitudes de soporte técnico deberán ser realizadas a través de la herramienta SysAid, instalada en los equipos de usuarios o vía telefónica a la extensión 38351 del DSIC.

5.2 Correo electrónico

5.2.1 Tipos de cuentas, solicitud y vigencia

Cuentas de usuario: Se asignará una cuenta de correo electrónico institucional del dominio del CRIM al personal académico o administrativo para la realización de sus labores, para lo cual se deberá entregar ante el DSIC el formato correspondiente debidamente llenado y estará sujeto a visto bueno de la Secretaría de adscripción del solicitante. La vigencia de estas cuentas corresponderá con la de su permanencia en el CRIM.

Cuentas departamentales: Serán generadas cuentas específicas para cubrir las necesidades de comunicación oficial del CRIM, sus secretarías, departamentos, coordinaciones, programas, etc. Estas cuentas deberán ser solicitadas directamente ante el DSIC por el titular del área, mediante el formato de solicitud correspondiente y deberá contener el visto bueno de la Secretaría de adscripción del solicitante.

Cuentas temporales: Cuentas con propósitos específicos de comunicación derivados de contratos temporales o provisionales, así como de eventos y proyectos de diversa índole. Estas cuentas deberán ser solicitadas directamente ante el DSIC por el responsable de la actividad, mediante el formato de solicitud correspondiente y deberá contener el visto bueno de la secretaría de adscripción del solicitante. Estas cuentas tendrán una fecha de caducidad y se

desactivarán automáticamente a su término, a menos que se solicite lo contrario. Se abrirán con una vigencia no mayor de doce meses y podrán renovarse por periodos máximos similares.

5.2.2 Responsabilidades de los usuarios

Los usuarios son responsables de todas las actividades realizadas con sus cuentas de correo institucionales.

La cuenta de correo que proporciona la institución es personal e intransferible y no debe ser usada para:

- Propósitos comerciales y/o ajenos a la institución.
- Participar en la propagación de "cadenas", esquemas piramidales y correos SPAM de cualquier índole. Se consideran correos SPAM aquéllos no relacionados con las funciones específicas de los procesos de trabajo.
- Distribuir de forma masiva mensajes con contenido ajeno a las actividades académicas.
- Enviar o reenviar mensajes con contenido difamatorio, ofensivo, racista u obsceno.
- Usar pseudónimos y enviar mensajes anónimos, así como aquellos que consignen títulos, cargos o funciones no oficiales.
- Utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del emisor de correo.

Por su parte, el usuario debe dar aviso al CRIM de cualquier fallo de seguridad de su cuenta de correo, incluyendo su uso no autorizado, pérdida de la contraseña, etc.

5.2.3 Envíos y transferencias

Se recomienda vaciar periódicamente la papelera del correo electrónico.

Se recomienda el uso del campo CCO (Con Copia Oculta), para mantener la privacidad de los correos electrónicos de los destinatarios.

Los correos institucionales de interés general deberán ser enviados a través del Área de Difusión y Comunicación mediante listas de distribución, previa autorización de las autoridades correspondientes.

El sistema de correo electrónico elimina automáticamente los archivos con extensiones .exe, .pif, .scr, .vbs, .cmd, .com, .bat, .hta, por considerarlos como una posible amenaza (virus).

Se recomienda la compresión de los archivos al compartirlos a través de la red, para disminuir las exigencias técnicas en su transmisión.

5.2.4 Sanciones

El uso en el servicio de correo electrónico deberá ser para cumplir con fines institucionales y académicos y, en caso contrario, el uso inadecuado pudiera ocasionar la inhabilitación temporal o permanente de las cuentas, dependiendo de su alcance.

Si existe evidencia de que el usuario no está haciendo un buen uso del servicio, no está respetando los lineamientos establecidos en esta política o está incurriendo en actividades ilícitas mediante el servicio de correo, el CRIM se reserva el derecho de tomar acciones disciplinarias, de acuerdo a la normativa universitaria y a la legislación vigente.

5.2.5 Generales

Esta política será revisada y actualizada por la Comisión de Política Informática (CPI) del CRIM conforme se requiera. Los usuarios serán informados oportunamente de las modificaciones a la misma mediante circular emitida por la Dirección del CRIM.

Los casos no previstos serán resueltos por la CPI.

5.3 Desarrollo de software

El desarrollo e implantación de sistemas, herramientas y software tiene como propósito apoyar, facilitar y agilizar las actividades administrativas y académicas del personal del CRIM. Cuando se trate de desarrollo de software en colaboración con alguna otra organización interna o externa, se deben seguir los lineamientos establecidos por la UNAM.

Es necesaria la elaboración de la documentación que permita dar seguimiento a las aplicaciones de software durante todo su ciclo de vida, siguiendo la metodología que la dependencia considere adecuada para dicho fin.

La elección de la tecnología de desarrollo y bases de datos debe ser realizada en referencia a la compatibilidad con los demás sistemas con los que la aplicación pueda interactuar. El desarrollo e implantación de sistemas sólo podrá realizarse a través del DSIC o bajo el visto bueno del mismo.

Previo a la liberación de los sistemas de información debe realizarse un análisis de seguridad en un ambiente de pruebas, corrigiendo la totalidad de los fallos que sean detectados.

5.4 Red local (LAN)

El DSIC es el único autorizado para instalar, configurar y dar mantenimiento a la infraestructura de red (ruteadores, puntos de acceso, cableado, etc.) del CRIM.

Los administradores de la red deben contar con herramientas de monitoreo de redes, tales como verificadores de integridad, detectores de intrusos, firewall, etc., con el propósito de contar con información útil para el análisis y optimización continua de la infraestructura.

El CRIM utiliza esquema de VLANs (redes privadas virtuales) configuradas de acuerdo a las necesidades de los usuarios, el cual será administrado únicamente por el DSIC.

Las direcciones IP fijas sólo serán asignadas a servidores y servicios. Los usuarios utilizan direcciones IP dinámicas. Las direcciones IP que pueden otorgarse para equipos periféricos son homologadas y sólo se otorgan bajo disponibilidad y previa justificación de uso.

El DSIC es el responsable de la configuración y asignación de direcciones IP asignadas a los equipos de cómputo y periféricos.

El DSIC es el único responsable de servidores de DHCP. Los administradores de red deben contar con un inventario lógico de la red a su cargo, con la relación de las direcciones IP que incluya el nombre del responsable o servicio.

5.5 Red Inalámbrica del CRIM

La instalación y configuración de los Puntos de Acceso (Access Point – AP) y de cualquier dispositivo inalámbrico de red, será realizado por los administradores del DSIC.

El CRIM cuenta con dos redes inalámbricas. La primera de uso interno, para los usuarios que requieran acceso a Internet y servicios de la red (servidores e impresoras). La segunda para usuarios visitantes que sólo requieran acceso a Internet.

La configuración de acceso a la red inalámbrica interna, la realizan los técnicos académicos del DSIC, previa autorización del responsable del área de adscripción del usuario solicitante.

Será considerado un uso inapropiado, sobrepasar el ancho de banda de la red inalámbrica mediante la realización de actividades que no sean con fines académicos e institucionales. Este tipo de acciones serán notificadas a la CPI para su evaluación y, en su caso, para la determinación de las sanciones aplicables.

5.6 Red Inalámbrica Universitaria (RIU)

El CRIM cuenta con conexión a la RIU de la UNAM, un servicio que se proporciona en los campus universitarios. El registro a la RIU es un trámite personal que se realiza ante la Dirección General de Tecnologías de Información (DGTIC) de la UNAM.

5.7 Escaneo, impresión y ploteo

Los usuarios del CRIM pueden hacer uso del escáner en el DSIC realizando su registro de uso en la bitácora correspondiente.

Los usuarios del CRIM pueden solicitar la configuración de las impresoras del DSIC para realizar sus impresiones.

Los usuarios invitados pueden solicitar la configuración de las impresoras del DSIC, previa autorización del responsable del área de adscripción del usuario solicitante.

Los usuarios del CRIM pueden solicitar apoyo al DSIC para realizar impresiones en plotter.

5.8 Videoconferencia

El CRIM ofrece el servicio de videoconferencia, un sistema interactivo, punto a punto o multipunto, que permite a varios usuarios mantener una conversación virtual por medio de la transmisión en tiempo real de video, sonido y texto a través de Internet.

El servicio se brinda en las propias instalaciones del Centro mediante sus sistemas de videoconferencia o aplicaciones especializadas.

5.8.1 Disposiciones generales

Los solicitantes del servicio de videoconferencia son responsables de hacer un buen uso de los recursos de esta herramienta.

La solicitud, reservación y uso de los recursos de videoconferencia del CRIM (salas, equipos y enlaces) están sujetos a las políticas de servicio de videoconferencias.

Toda situación no prevista en estas políticas deberá ser consultada con el DSIC.

5.8.2 Reservación

Las solicitudes de servicio de videoconferencia se realizan a través de la Secretaría Académica del CRIM y son registradas en el Sistema de Administración de Eventos.

El solicitante debe indicar todos sus requerimientos al momento de solicitar el servicio para evitar fallas durante el evento.

Las solicitudes de servicio de videoconferencias están sujetas a disponibilidad de sala y equipo (códec), y deben realizarse con una anticipación de al menos 5 días hábiles previos al evento.

Si se requieren pruebas adicionales de conectividad y niveles de audio, las solicitudes deben hacerse con una anticipación de al menos 8 días hábiles.

El solicitante deberá proporcionar información completa sobre la(s) institución(es) participantes a fin de establecer contacto previo.

El DSIC no se hace responsable por fallas en el servicio por omisiones en el llenado de la solicitud o por causas ajenas al DSIC.

5.8.3. Prestación del servicio

El servicio de videoconferencias se otorgará en días hábiles de 9:00 a 18:00 horas.

Toda información expuesta durante la sesión es responsabilidad única y exclusiva de los participantes.

Los servicios de grabación deben ser solicitados con al menos 2 días hábiles de anticipación y estarán sujetos a disponibilidad.

5.9 Transmisión remota

Los servicios adicionales como transmisión por streaming- webcast (transmisión de audio y video por Internet), presentaciones, proyección de videos, películas, etc., están sujetos a disponibilidad

por lo cual deben ser solicitados al menos 15 días hábiles previos a la realización del evento, lo cual no garantiza la aprobación por parte de la DGTIC.

5.10 Proyectos especiales

Toda solicitud de apoyo a proyectos especiales debe solicitarse a la Secretaría Académica y revisarse por la CPI.

5.11 Apoyo a reuniones en sala

El apoyo técnico a reuniones o eventos relacionado con TIC se otorgará cuando haya sido solicitado previamente a través de la Secretaría Académica del CRIM y registrado en el Sistema de Administración de Eventos del CRIM.

El calendario de reservaciones de actividades, eventos y videoconferencias programadas se publica en la página: www.crim.unam.mx/eventos

Capítulo 6 - DE LA INFORMACIÓN

El usuario es responsable de la información que recibe, genera y guarda, así como del respaldo de la misma, en caso de requerir apoyo para realizar esta última actividad podrá solicitarlo al DSIC.

Capítulo 7 - DEL SITIO WEB

El sitio web del CRIM es el espacio virtual mediante el cual se da a conocer información oficial, así como actividades relacionadas con el quehacer institucional y académico. Su infraestructura se sustenta por las mejores prácticas de seguridad y administración de TI bajo los "Lineamientos de Sitios Web Institucionales" de la UNAM en servidores, aplicaciones, licencias, configuraciones, contenidos y procedimientos. Se encuentra alojado bajo el dominio www.crim.unam.mx.

7.1. Administración

La administración de los servidores, aplicaciones, licencias y configuraciones del sitio web institucional está a cargo del DSIC.

La actualización de los contenidos que se publican en cada sección del sitio web institucional es responsabilidad del área que genera la información. Los contenidos generales del sitio son responsabilidad de la Secretaría Técnica (ST).

La solicitud de usuarios y contraseñas para edición de contenidos en el sitio web institucional deberán ser solicitados a la ST y se solicitará el visto bueno de la CPI.

Las solicitudes de publicación de información sobre proyectos específicos, deberán hacerse llegar a la CPI a fin de determinar su pertinencia y procedencia y serán turnadas al DSIC a fin de determinar

su viabilidad y, en su caso, definir si se integra en el sitio web del CRIM o bien se publica en la plataforma de sitios web personales institucionales de la UNAM (www.paginaspersonales.unam.mx), para lo cual se considerarán los objetivos, requerimientos, financiamiento, contenidos, alcance y vigencia, entre otros aspectos.

7.2. Lineamientos sitios web institucionales

Los sitios web institucionales del CRIM se encuentran bajo el dominio: ***.crim.unam.mx***. Deben estar sustentados en las mejores prácticas de seguridad y administración de TI bajo los "Lineamientos de Sitios Web Institucionales" de la UNAM en servidores, aplicaciones, licencias, configuraciones, contenidos y procedimientos (www.visibilidadweb.unam.mx).

La única instancia autorizada para desarrollar sitios web institucionales es el DSIC y es su responsabilidad elaborar y mantener actualizado el inventario, así como administrar y controlar su operación. La actualización de contenidos estará a cargo de cada uno de los responsables del sitio web.

Capítulo 8 - DE LAS PLATAFORMAS EDUCATIVAS O RECURSOS ACADÉMICOS

Las plataformas educativas son para uso exclusivo del personal académico del CRIM y en apoyo a la impartición de docencia en la UNAM. El área responsable de su administración y mantenimiento es la Coordinación de Docencia del CRIM. Las cuentas de acceso deben estar aprobadas por el titular docente, quien debe confirmar que sean de los inscritos al curso.

Los titulares docentes de la plataforma educativa son responsables de hacer un buen uso de los recursos de esta herramienta.

Capítulo 9 - DE LA ADMINISTRACIÓN DE LOS CENTROS DE DATOS

Los Centros de Datos, son los espacios donde se concentran el equipamiento informático y electrónico necesarios para el procesamiento de la información de una organización.

9.1 Instalaciones

9.1.1 Instalación eléctrica

Los equipos de cómputo, PC y monitores, así como los activos de telecomunicaciones, deben estar conectados al sistema de alimentación ininterrumpida (UPS) del CRIM (contactos color naranja).

Se debe contar con un sistema de tierras físicas, conectado al sistema de tierras general del CRIM.

Los cuartos de telecomunicaciones deben tener contactos regulados dobles conectados a circuitos exclusivos para alimentar los equipos que sean alojados en gabinetes; así mismo, se deberá disponer de contactos para pruebas y herramientas cerca de éstos.

9.1.2 Climatización

Se debe garantizar que los cuartos de telecomunicaciones se mantengan a una temperatura entre 18 y 24 grados centígrados, con humedad relativa entre 30% y 55% para el correcto funcionamiento de los equipos activos, para lo cual se debe contar con dispositivos de aire acondicionado en óptimas condiciones de funcionamiento.

9.1.3 Cableado

Todos los elementos del cableado estructurado deben ser de la misma categoría, marca y solución y la instalación debe cumplir con lo establecido en la norma TIA vigente. Los cables de red deben ser ensamblados de fábrica.

En los casos donde la salida de datos quede en exteriores (por ejemplo, puntos de acceso o cámaras para exteriores), los accesorios de conexión deberán ser de tipo industrial o contar con características de resistencia a la intemperie.

Deben existir por lo menos dos puntos de cableado estructurado por cada área de trabajo.

9.1.3.1 Etiquetado

Deben instalarse etiquetas de identificación a cada uno de los cables UTP en ambos extremos del remate, las etiquetas deben quedar en el forro del cable a 10 cm del elemento de remate, así como en el panel de parcheo y en el *face plate* de la salida de usuario.

9.1.4 Acceso

Se deben implantar controles para autorizar o no el acceso a los centros de datos.

No se podrá ingresar con alimentos o bebidas.

9.2. Servidores y equipo de telecomunicaciones

Todos los servidores y equipo de telecomunicaciones deben ubicarse en lugares de acceso físico restringido y deben tener puertas con cerraduras de seguridad para acceder a ellos.

Los servidores y equipo de telecomunicaciones deben tener una instalación eléctrica adecuada, así como tierra física y sistemas de alimentación ininterrumpida o de emergencia, UPS.

El área donde se encuentren los servidores y equipo de telecomunicaciones debe cumplir con los estándares de cableado estructurado. Se debe conservar limpio, organizado y despejado de objetos extraños o ajenos al uso al cual están destinados.

Los administradores o responsables de los servidores y equipo de telecomunicaciones son los encargados de su monitoreo, actualización, evaluación e instalación de parches de seguridad.

Es responsabilidad de los administradores la actualización de los certificados digitales en los servidores web en caso de contar con alguno.

La utilización de servidores del CRIM es con fines únicamente institucionales y académicos, por lo que cualquier solicitud de uso debe contar con el visto bueno del CPI.

Capítulo 10 - DE LA SEGURIDAD

10.1 Física

Mantener los equipos de cómputo alejados de cualquier agente que pueda causar algún daño o interfiera con su rendimiento como son: fuego, humo, polvo, temperaturas extremas, rayos solares, vibraciones, roedores, insectos, ruido eléctrico, balastros, equipo industrial, agua, entre otros.

10.2 Informática

Se refiere a la protección de la infraestructura computacional y circulante a través de la red. El CRIM cuenta con un *firewall* físico*,* que se encarga de monitorear el tráfico de red, entrante y saliente, y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

Capítulo 11 - DE LA TELEFONÍA IP

El CRIM buscará garantizar que en cada espacio físico que así lo amerite esté disponible una línea telefónica con extensión UNAM.

11.1 Solicitud y adquisición

El área autorizada para presentar solicitudes de asignación de teléfonos IP es el DSIC, previo análisis del requerimiento. Posteriormente presenta la solicitud ante la CPI para su revisión y visto bueno. La Secretaría Administrativa del CRIM realizará las adquisiciones de conformidad con la disponibilidad presupuestal y en apego a los trámites y procedimientos vigentes.

11.2 Asignación y resguardo

Todos los aparatos y líneas telefónicas deben permanecer en el CRIM y no pueden transferirse, moverse o trasladarse a otros lugares sin el previo consentimiento del DSIC y la Secretaría Administrativa del CRIM.

Todo personal que termine una relación laboral debe entregar al DSIC los aparatos telefónicos que se le hayan asignado durante su estancia en el Centro.

11.3 Baja de equipo

En caso de robo o extravío de teléfonos IP del CRIM, el usuario resguardante deberá notificar al DSIC. Asimismo, deberá levantar un acta administrativa de hechos ante del Departamento de

Bienes, Suministros y Servicios Generales del CRIM, y generar una denuncia ante el Ministerio Público.

El DSIC podrá solicitar a la Secretaría Administrativa del CRIM, la baja del aparato telefónico por fallas en el equipo.

11.4 Mantenimiento preventivo y correctivo

El DSIC es el encargado de coordinar el mantenimiento preventivo de los aparatos telefónicos IP, una vez por año.

En caso de que se presente alguna falla o malfuncionamiento del aparato o la línea telefónica IP, el usuario deberá notificar al DSIC para revisión y en su caso, reparación o baja.

Capítulo 12 - DE LA AUDITORÍA

Junto con la DGTIC / UNAM, el DSIC programa la realización de auditorías informáticas periódicas a los diferentes servicios en TIC sin afectar a los usuarios del servicio, de acuerdo con los horarios y días que el administrador considere pertinentes para minimizar el impacto de las acciones.

Toda auditoría informática debe quedar documentada a lo largo del proceso, incluyendo los resultados para su atención y seguimiento. La información resultante de estas auditorías deberá ser considerada como confidencial y sensible.

Capítulo 13 - DEL INCUMPLIMIENTO Y LAS FALTAS

El DSIC tiene la responsabilidad de notificar a la CPI cualquier incidente grave, ataque o intento de explotar alguna vulnerabilidad en equipos de cómputo e infraestructura del CRIM, para que proceda conforme corresponda.

El DSIC mantendrá informada periódicamente a la CPI sobre la situación que guarda el cumplimiento de estas políticas a fin de que se realicen las adecuaciones o mejoras necesarias.

Capítulo 14 – TRANSITORIOS

Todos aquellos asuntos que no hayan sido considerados en este documento serán resueltos por la CPI.

La política informática entrará en vigor al día siguiente de la publicación de la circular emitida por la Dirección del CRIM.

GLOSARIO

CPI: Comisión de Política Informática del CRIM de la UNAM.

Dirección IP: es un número que identifica, de manera única, lógica y jerárquica, a un elemento o dispositivo en la red que utilice el protocolo IP (*Internet Protocol*).

Dirección IP fija: el número que identifica al equipo de forma permanente, es decir que no cambia.

Dirección IP dinámica: el número que identifica al equipo de forma variable por medio de un servidor especial (DHCP) que realiza esta tarea.

Dirección IP homologada: Dirección cuyo segmento corresponde a las redes públicas y que son accesibles desde Internet.

Dirección IP no homologada o privada: Dirección cuyo segmento corresponde a las redes locales y que no son accesibles desde Internet.

DGTIC: Dirección General de Cómputo y de Tecnologías de Información y Comunicación de la UNAM.

DSIC: Departamento de Sistemas de Información y Comunicación del CRIM de la UNAM.

DHCP: Por sus siglas en inglés de *Dynamic Host Configuration Protocol*, se refiere al servicio o protocolo de asignación dinámica de direcciones IP.

Dispositivo móvil: Son computadoras portátiles, *smartphones*, Asistentes Personales Digitales (PDA), Discos Compactos (CD), Discos Digitales Versátiles (DVD), unidades flash, discos duros portátiles, dispositivos *Bluetooth* y cualquier otro equipo que permita la movilidad de la información, ya sea para su procesamiento o su almacenamiento, de propiedad privada o del CRIM.

***Face plate*:** Son las tapas plásticas que se encuentran normalmente en las paredes y es en donde se conectan los cables de red.

Firewall: Aplicación de software o dispositivo de hardware que limita el acceso hacia una red, equipo de cómputo o sistema de software, en base a un conjunto de reglas establecidas.

Incidente: Cualquier falta o incumplimiento a las políticas establecidas en este documento.

***Malware*:** Código generado con fines maliciosos que se introduce en los equipos y sistemas de cómputo afectando el funcionamiento y rendimiento, entre los que ubicamos: virus, caballos de troya, gusanos, *spyware*, etc.

Panel de parcheo: Es el elemento que recibe todo el cableado estructurado de la red. Todas las líneas de entrada y salida de los equipos de cómputo (computadoras, servidores, impresoras, entre otros) tendrán su conexión a uno de estos paneles.

PC: *Personal Computer* por sus siglas en inglés. Equipo de cómputo de escritorio diseñado para ser utilizado individualmente.

Punto de Acceso (*Access Point*) o PA: Dispositivo que permite la conexión a la red de manera inalámbrica.

***SysAid* –** Herramienta de software utilizada para el registro y control de solicitudes e incidentes relacionados con tecnologías de información.

Switch: O conmutador, es un dispositivo de interconexión de redes informáticas.

TI: Tecnologías de Información, se refiere al uso de equipos de telecomunicaciones y computadoras para la transmisión, el procesamiento y el almacenamiento de datos.

TIA: Por sus siglas en inglés *Telecommunications Industry Association*, es un estándar de cableado estructurado.

TIC: Tecnologías de la Información y la Comunicación (TIC) son todos aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos, tales como: computadoras, teléfonos móviles, televisores, reproductores portátiles de audio y video o consolas de juego.

UPS: Por sus siglas en inglés *Uninterruptible Power Supply*, es un dispositivo de suministro eléctrico que cuenta con una batería que proporciona energía a otros dispositivos en caso de interrupción o falla del suministro principal.