1. OBJETIVO

Las políticas de seguridad en cómputo tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes de telemática) y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de cómputo de la Universidad Autónoma de Yucatán.

2. ALCANCE

Aplica a todas las dependencias de la UADY que hagan uso de los Servicios de Tecnologías de Información definidos en el catálogo de servicios de la CGTIC.

3. POLÍTICAS

1.- Las Dependencias de la UADY son las responsables de dar a conocer y hacer cumplir estas políticas de seguridad.

2.- Las Dependencias de la UADY pueden agregar, guías particulares complementarias, sin contradecir lo aquí descrito

4. POLÍTICAS INSTITUCIONALES DE SEGURIDAD EN CÓMPUTO

Contenido

Capítulo 1: Infraestructura

1. Las dependencias destinarán un área que fungirá como centro de telecomunicaciones donde ubicarán los sistemas de telecomunicaciones y los servidores.
2. El centro de telecomunicaciones de la dependencia debe seguir los estándares vigentes de protección y mantenimiento de los centros de telecomunicaciones.
3. El centro de telecomunicaciones deberá seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.
4. Las dependencias deberán considerar los estándares vigentes de cableado estructurado durante el diseño de nuevas áreas o en el crecimiento de las áreas existentes.
5. Las visitas a los centros de telecomunicaciones deben portar una identificación y llenar la bitácora de acceso.
6. Las visitas internas o externas podrán acceder a los centros de cómputo y de telecomunicaciones acompañadas, cuando menos, por un responsable de la institución asignado por el ATI, habiendo previamente solicitado el permiso de acceso al ATI.
7. Se deberán establecer horarios de acceso a instalaciones físicas, especificando los procedimientos y en qué casos se deberá hacer excepciones.
8. Se deberá definir qué personal está autorizado para mover, cambiar o extraer equipo de la dependencia a través de identificaciones y formatos de Entrada/Salida; y se debe informar de estas disposiciones a personal de seguridad.
9. La dependencia deberá seguir los procedimientos para inventario físico, firmas de resguardo para préstamos y usos dedicados de equipos de tecnología de información.
10. El resguardo de los equipos del centro de telecomunicaciones deberá quedar bajo a cargos del área de Tecnologías de Información de la DES, contando con un control de los equipos que permita conocer siempre la ubicación física de los mismos.
11. El centro de operaciones, así como las áreas que cuenten con equipos de misión crítica deberán contar con vigilancia y/o algún tipo de sistema que ayude a recabar evidencia de accesos físicos a las instalaciones.
12. Las puertas de acceso a las salas de cómputo deben ser preferentemente de vidrio transparente, para favorecer el control del uso de los recursos de cómputo.
13. Se debe contar con una póliza de servicio de mantenimiento y/o reemplazo de equipo, de acuerdo con el orden de prioridad del equipo de mayor impacto hasta el de menor, en la operación de la dependencia.

SITIO DE TELECOMUNICACIONES	Espacio exclusivo para los equipos de Telecomunicaciones y servidores
	Acceso restringido
	Recibir limpieza al menos una vez por semana
	Estar libre de contactos e instalaciones eléctricas en mal estado
	Contar por lo menos con un extinguidor de incendio adecuado y cercano al centro de telecomunicaciones (Extintores de dióxido de carbono (BC). Disminuyen el calor debido al enfriamiento que causa el dióxido de carbono al expandirse. Deben usarse únicamente para extinguir fuegos Clase B (combustibles líquidos y gaseosos) o C (equipos eléctricos energizados)).
	Climatización
ESQUEMA DE PROTECCIÓN ELÉCTRICA	Terminal aérea si se cuenta con torre
	Instalación y monitoreo de eventos
	Sistema de tierras físicas
	Supresores de corriente
	Protectores de las líneas de datos
	Sistemas de Alimentación Ininterrumpida UPS No-break
	Barras de tierra
CABLEADO ESTRUCTURADO	Certificado
	Documentación de conectividad
	Norma TIA/EIA 568B soporte tecnologías de Gigabit para Backbone.
	Rack de comunicaciones Rack de servidores
	Centros de distribución
	Referenciar a tierra los racks y equipos activos
	Registros, Backbones principales y secundario que contemplen los ductos, registros principales y secundario que contemplen los ductos.

Tabla 1 - Requisitos de Infraestructura para centro de telecomunicaciones

ESTÁNDARES INFRAESTRUCTURA

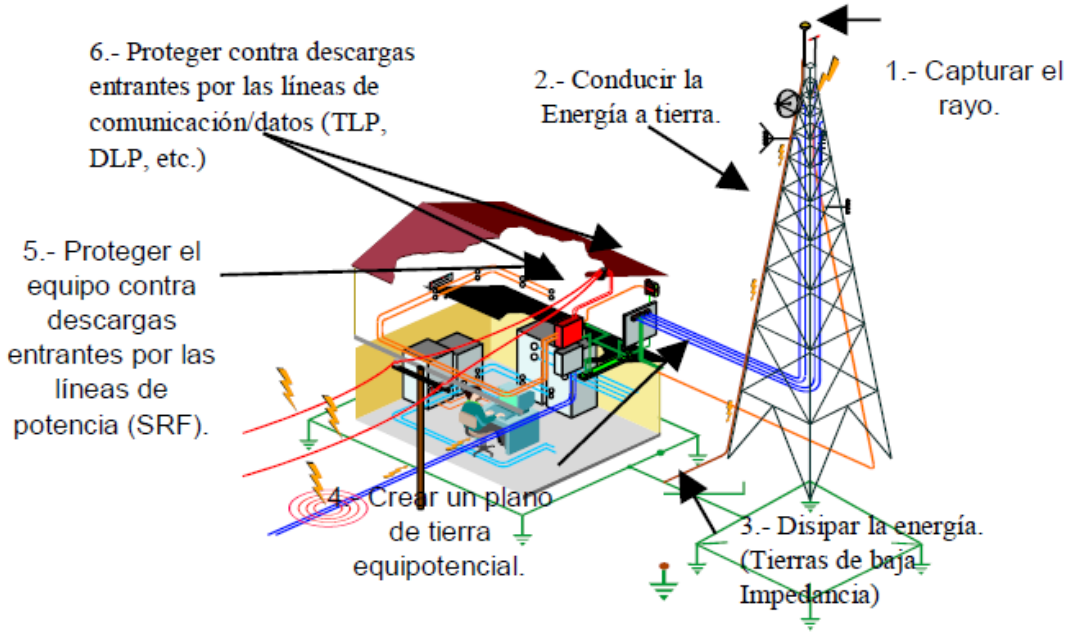


Figura 1 - Modelo de Protección eléctrica en instalaciones de sistemas de cómputo y comunicaciones

1. Capturar la descarga atmosférica en un punto designado.
   Se requiere contar con una terminal aérea, para una adecuada protección ante descargas eléctricas, el cual deberá aterrizarse a un sistema de tierra física tipo delta.

2. Conducir sin riesgo la descarga a tierra en forma segura.
   Conductor de cobre.

3. Disipar la energía a tierra.
   Los componentes del sistema de tierra deberán ser: Conector soldadura exotérmica Caldwell, Electrodo, Electrodo a tierra fabricados con una barra de acero recubierta por una gruesa película de cobre (0.254 mm) de acuerdo con las Normas ANSI/UL 467-1984 y ANSI C 33-8, 1972 y Tierra. La resistividad del terreno deberá ser considerada, incluyendo el contenido de humedad y la temperatura.

4. Crear un plano de tierra equipotencial.
   Interconectar todos los Sistemas de Electrodos de Tierra.
   Sistema general de Tierra.
   Sistemas de Tierra de Pararrayos.
   Sistemas de Tierra de Telecomunicaciones.
   Cable para Sistemas de Tierra.
   Conectar todos los objetos conductivos internos y externos de las instalaciones a Tierra.
   Proveer una diferencia de potencial lo más cercana a cero durante transitorios que eleven el potencial

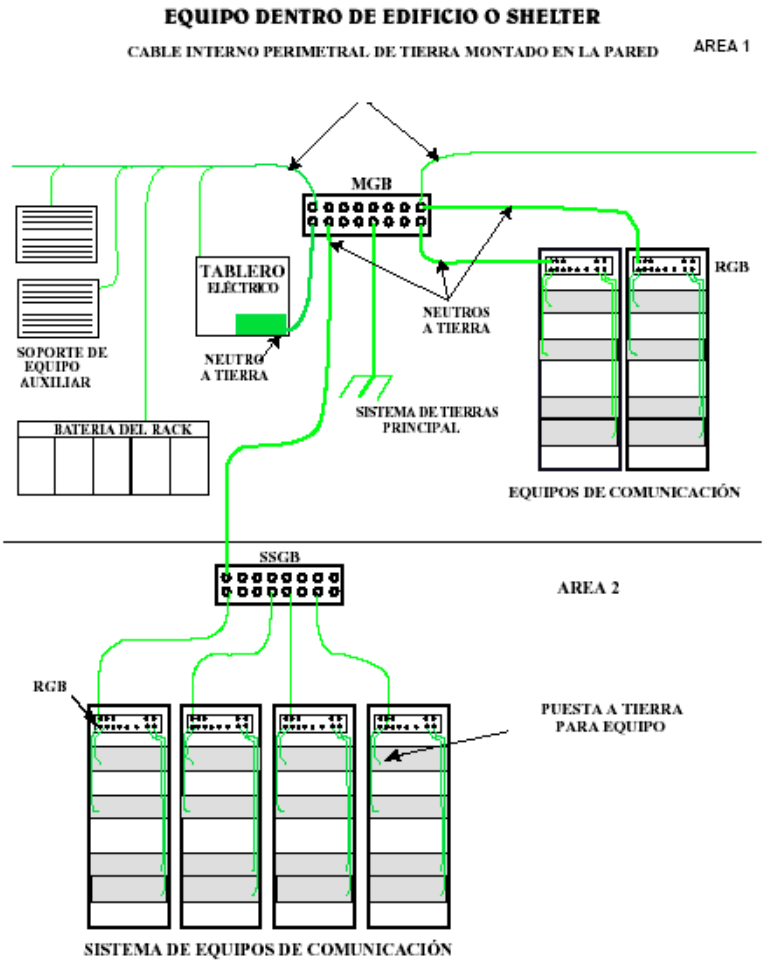


Figura 2 - Sistemas de tierra en centro de comunicaciones

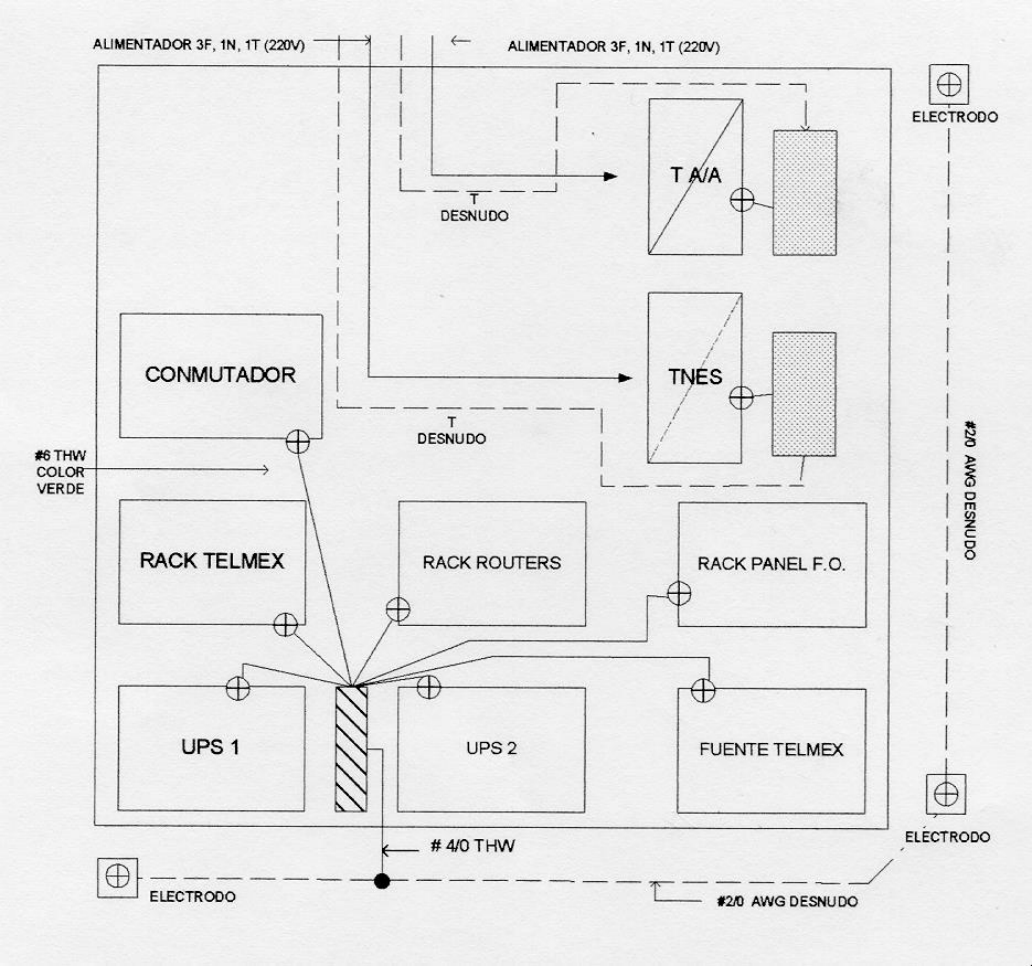
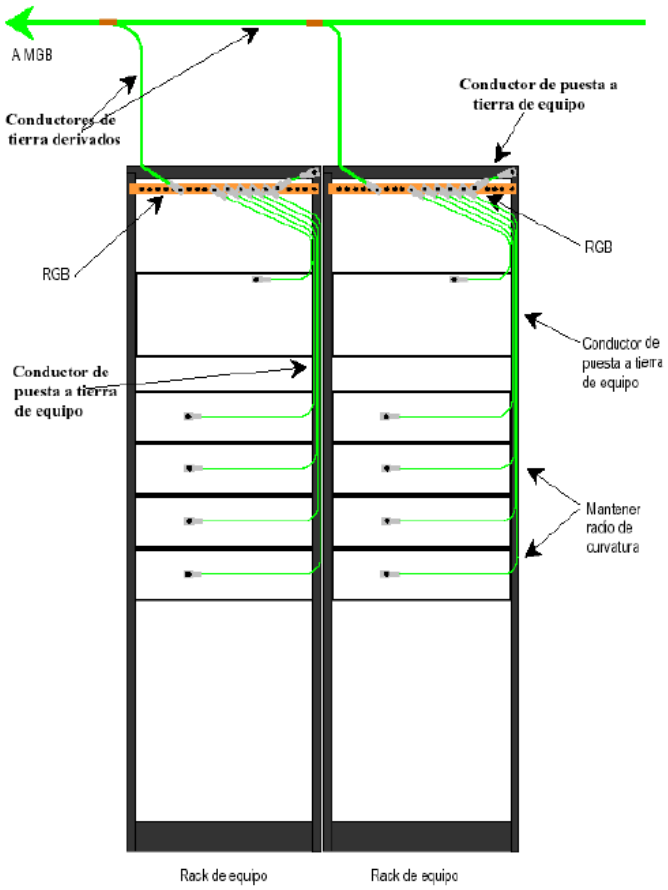


Figura 3 - Sistemas de tierra en centro de comunicaciones, planos



NOTA: El rack debe estar totalmente aislado del piso. Y el Sistema de Tierra solo vendrá por arriba.

Figura 4 - Sistemas de tierra para Racks

5. Proteger contra transitorios entrantes por los circuitos de potencia.
   Contar con supresores contra transitorios en las líneas de corriente.
6. Proteger contra transitorios entrantes por los circuitos de comunicación/datos.

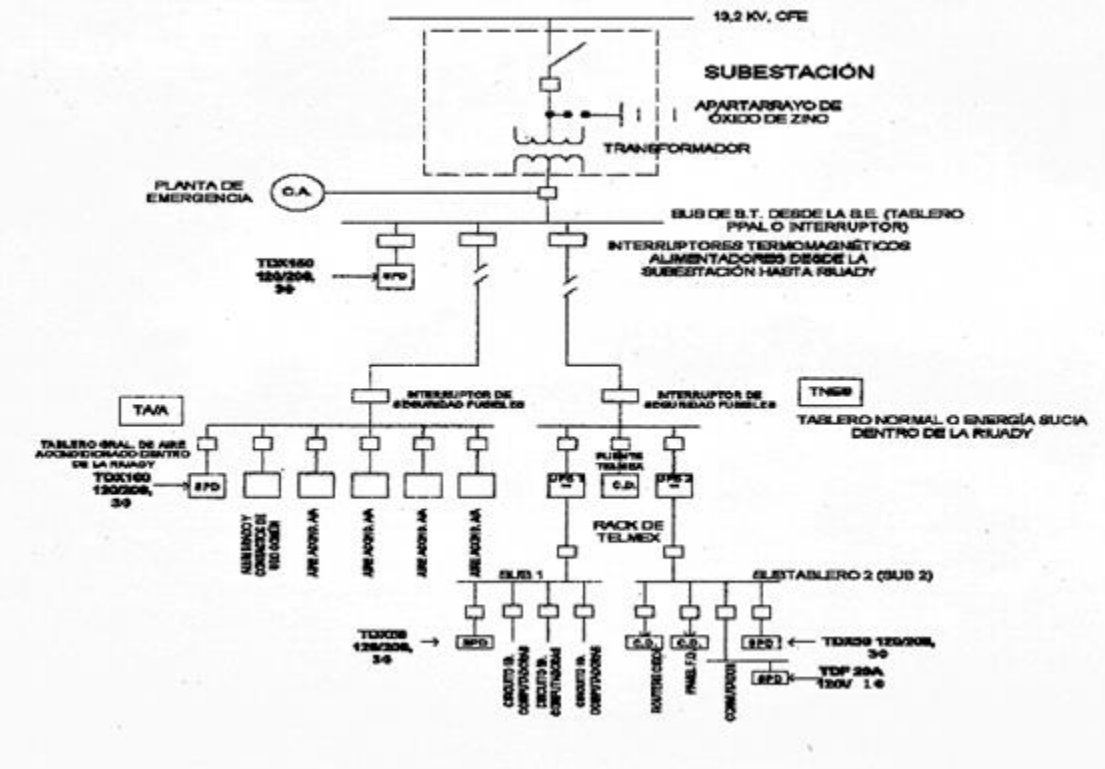


Figura 5 - Sistema eléctrico

REQUISITOS DE TELECOMUNICACIONES

Se recomienda seguir las normas de cableado estructurado, según la norma vigente, que garantizan una mejor administración de los servidores de red, equipos de telecomunicaciones y cableado de los mismos, de acuerdo con los siguientes lineamientos (Figura 6.- Estándar para un centro de comunicaciones en DES):

- Instalación de un rack de piso de 19" de ancho y 7 pies de alto.
- Instalación de un kit de protección para la infraestructura metálica: barra de conexión a tierra, aisladores y alfombra de aislamiento.
- Usar cableado par trenzado categoría 6.
- Todas las conexiones de red deberán conectarse a un panel de parcheo según sea el medio físico: par trenzado o fibra óptica.
- Al menos las conexiones de inalámbricos y/o *backbones* deberán contar con protector de líneas. Se recomienda la instalación de un panel de protección de líneas, el cual deberá estar aterrizado a tierra.
- Instalar protectores de línea para las conexiones de los enlaces alternos: E1, DSL y/o ISDN.

Estándar de Centro de Comunicaciones

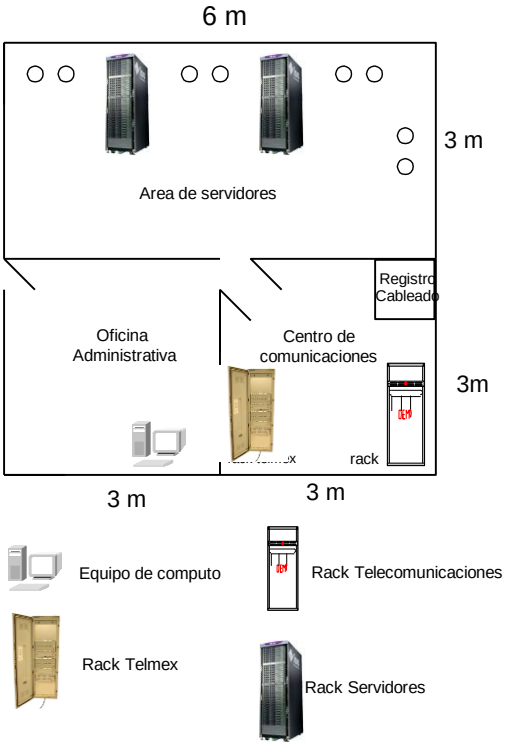


Figura 6.- Estándar para un centro de comunicaciones en DES

Capítulo 2: Telecomunicaciones

1. Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo. Entendiendo por sistema de comunicaciones: el equipo activo y los sistemas de cableado.
2. El uso de analizadores de red es permitido única y exclusivamente para monitorear la funcionalidad de la red de una dependencia, contribuyendo a la consolidación del sistema de seguridad en la UADY.
3. No se permite el uso de servicios de red que provoquen una carga excesiva sobre recursos escasos.
4. La RIUADY no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.
5. Cuando se detecte un uso no aceptable de los recursos de red, se desconectará temporal o permanentemente al usuario o red involucrados. La reconexión se hará en cuanto se considere que el uso no aceptable haya sido contenido.
6. Los equipos de telecomunicaciones deberán configurarse de acuerdo con el estándar vigente de configuración.

ENLACES	Destinar un equipo para el sistema de monitoreo. Instalación y configuración del sistema de monitoreo. Instalación y configuración segura de ruteo
	Enlaces inalámbricos: 1. Torre resistente al medio ambiente 2. Orientación de antenas 3. Polarización horizontal 4. Instalación de caja NEMA de acuerdo con el modelo de protección eléctrica. 5. Configuración de bridges inalámbricos. 6. Iluminación 7. Mantenimiento anual: pintura, retensado, iluminación, etc. 8. Garantía / reposición de bridges 9. Máximo 4 enlaces por torre.
RED SWITCHEADA	Instalación y configuración de *switches* capa 3
	Instalación y configuración de *switches* capa 4
	Aplicación de estándar de configuración para *switches* de la RIUADY
	Configuración de clase y calidad de servicio de acuerdo con los perfiles de uso

ACCESOS INALÁMBRICOS	Instalación y configuración de puntos de acceso
	Aplicación de las Políticas de Computadoras Inalámbricas y Portátiles en la RIUADY.
	Asignación de subred para la WLAN.
	Asignar un equipo de cómputo para implementar los servicios de autentificación de usuario y asignación dinámica de direcciones IP.
ACELERADORES WEB	Instalación y configuración de servicio de web
INTERNET	Instalación y configuración de perfiles para el uso de Internet

Tabla 2 - Requisitos para equipos de telecomunicaciones

ESTÁNDARES

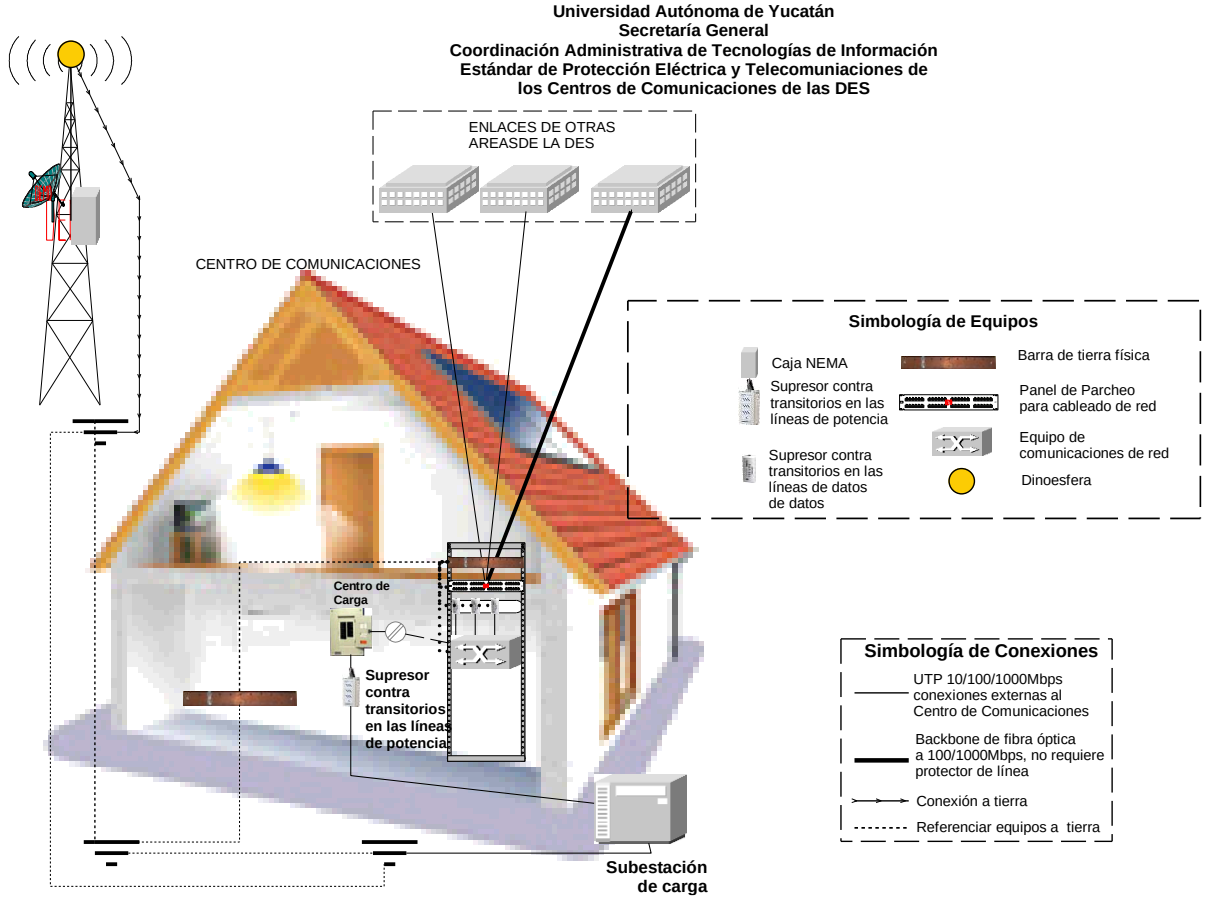


Figura 7 - Estándar de protección eléctrica y telecomunicaciones de los centros de telecomunicaciones de las DES

Estándar de conexión en Caja NEMA de los enlaces inalámbricos en la RIUADY

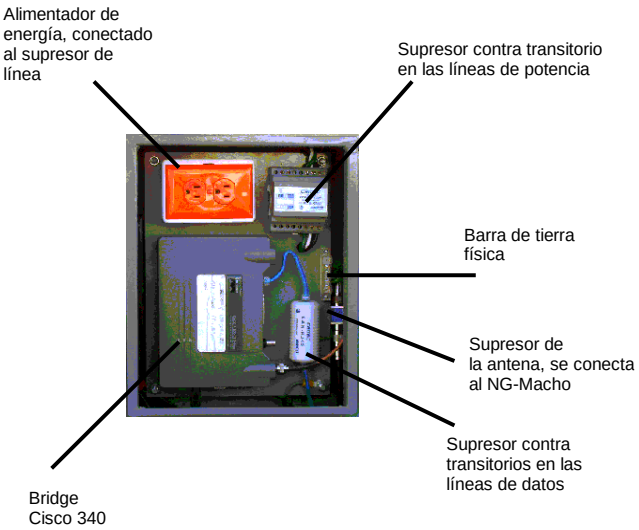


Figura 8 - Estándar de conexión en caja NEMA de los enlaces inalámbricos de la RIUADY

Capítulo 3: Políticas de uso aceptable de la RIUADY

1. La RIUADY proporciona servicios de información, comunicación e infraestructura de TIC para apoyar el desarrollo de las capacidades académicas de la institución, satisfacer las necesidades de acceso a la información, la coexistencia de modalidades educativas y práctica de la innovación, potenciando el desarrollo del trabajo colegiado y de gestión.

2. Todo servicio de información que se incorpore a la RIUADY deberá cumplir con las políticas de seguridad en cómputo.

3. Nadie puede ver, copiar, alterar o destruir la información de un usuario sin el consentimiento explícito del afectado.

4. No se permite interferir o entorpecer las actividades de los demás usuarios por cualquier medio o evento que no haya sido solicitado expresamente por los mismos.

5. Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de la UADY y se usarán exclusivamente para actividades relacionadas con la institución.

6. Todas las cuentas de acceso a los sistemas y recursos de cómputo de la RIUADY son personales e intransferibles, se permite su uso única y exclusivamente a los propietarios de estas.

7. El centro de operaciones de la RIUADY es el encargado de suministrar medidas de seguridad razonables contra la intrusión o daños a la información almacenada en los sistemas, como la instalación de cualquier herramienta, dispositivo o versión de software que refuerce la seguridad de los sistemas. Sin embargo, debido a la amplitud y constante innovación de los mecanismos de ataque no es posible garantizar una seguridad total.

8. El centro de operaciones de la RIUADY y el ATI de la DES deben poner a disposición de los usuarios e informar, sobre los esquemas y herramientas de TIC que refuercen la seguridad de los sistemas de información de la UADY.

9. El Centro de Operaciones de la RIUADY y el ATI de la DES son los únicos autorizados para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de determinar y solucionar anomalías, usos indebidos o cualquier falla que provoque problemas de comunicación.

REQUISITOS

1. Guías complementarias de DES
2. Perfiles de usuarios

ESTÁNDARES

Perfil	Descripción	Comentario	Servicios
1	Personal administrativo y estudiantes que requieren recursos de Internet y acceso a los servicios de la RIUADY.	Estos usuarios saldrán por el enlace inalámbrico o enlace digital (e1 o metropolitano).	Correo electrónico, ftp, mensajería, web
2	Personal académico y administrativo que por la naturaleza de su trabajo de docencia, extensión o investigación hace mayor uso de las búsquedas en Internet y mantiene contactos importantes vía correo electrónico.	Estos usuarios saldrán por el enlace digital (e1 o metropolitano), pudiendo privilegiarse su acceso a Internet vía servicios FTTH.	Correo electrónico, ftp, chat, web
3	Personal administrativo, académico y que labora en las áreas de informática, desarrollo, no requiere acceso prioritario a Internet, hace un constante acceso al Sistema Institucional de Información y al sistema de bibliotecas.	Estos usuarios saldrán por el enlace digital (e1 o metropolitano), ya que requieren estabilidad en el servicio	SiiUady Voz sobre IP Videoconferencia
4	Personal académico, administrativo y directivos de la dependencia que por la naturaleza de su trabajo requieren disponibilidad de todos los recursos en cualquier momento.	Éstos usuarios tendrán acceso enlace digital (e1 o metropolitano), pudiendo adicionalmente privilegiarse el acceso a Internet a través de enlaces FTTH..	Correo electrónico, ftp, chat, web SiiUady Voz sobre IP Videoconferencia
5	En caso de contar con algún perfil adicional de usuarios favor de anotar aquí las características		
6	En caso de contar con algún perfil adicional de usuarios favor de anotar aquí las características		

Tabla 3 - Perfiles básicos de usuarios

Capítulo 4: Servidores

1. La instalación y/o configuración de todo servidor conectado a la RIUADY deberá ser notificada al Centro de Operaciones de la RIUADY.
2. Los servidores conectados a la RIUADY deberán seguir los estándares de seguridad vigentes para su instalación, configuración e implementación.
3. Durante la configuración del servidor, los ATI deberán normar el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.
4. La información de los servidores deberá ser respaldada de acuerdo con estándares de seguridad vigentes.
5. Los servicios institucionales sólo podrán proveerse si se cumplen los requisitos de infraestructura, administración y seguridad de las Tecnologías de Información.
   El Centro de Operaciones de la RIUADY es el encargado de asignar las cuentas a los usuarios para el uso de correo electrónico en los servidores que administra.
6. Las dependencias podrán utilizar la infraestructura de la RIUADY para proveer servicios de información en su intranet, cumpliendo con las políticas de seguridad en cómputo.
7. El ATI será el responsable de la administración de contraseñas de los servicios de información de su DES alojados en su intranet o en la nube, y deberá guardar su confidencialidad, siguiendo las buenas prácticas para manejo de contraseñas.
8. Cuando un usuario o un ATI responsable de un Servidor deje de tener alguna relación oficial con la institución, el área de Recursos Humanos de la dependencia deberá notificar al Centro de Operaciones de la RIUADY, para aplicar las medidas necesarias para preservar la seguridad de los servicios de información de la UADY.
9. El ATI deberá cumplir con los requisitos de administración y seguridad de los servidores de su intranet.
10. El Centro de Operaciones de la RIUADY tendrá la autoridad para aislar un servidor en caso de que no cumpla con las políticas de uso aceptable y determine que pone en riesgo la seguridad de la información de la institución o la DES.
11. Cada dependencia será responsable de clasificar y determinar la criticidad de la información almacenada en sus Servidores.
12. Los Servidores que contienen información crítica deberán ser separados de la red interna y colocados en una DMZ.
13. La contraseña deberá contar con al menos 10 caracteres, teniendo al menos tres de los cuatro distintos tipos de caracteres: mayúsculas, minúsculas, números y no alfanuméricos.

Capítulo 5: Antivirus

1. Los equipos de cómputo deberán recibir su configuración y políticas a través de la solución antivirus institucional.
2. La solución antivirus institucional ejecutará diariamente de manera automática las actividades de detección y/o eliminación de software malicioso, en los equipos de cómputo.
3. La solución antivirus institucional se actualizará diariamente de manera automática,
4. El ATI será responsable de instalar de manera manual el agente y verificar su correcta operación posteriormente.
5. Será responsabilidad del ATI, reportar y enviar a la CGTIC, las muestras de los archivos infectados por software malicioso no detectado por la solución antivirus institucional.
6. En caso de contingencia con algún software malicioso que la solución antivirus no haya detectado, el Centro de Operaciones de la RIUADY llevará a cabo las siguientes actividades:
   - Emitirá inmediatamente en un máximo de 24 horas una alerta a los ATIs y a los usuarios, y publicará información más detallada en la página web del Centro de Operaciones de la RIUADY.
   - Se pondrá en contacto con el fabricante de la solución antivirus con el fin de determinar la estrategia más efectiva para eliminar el software malicioso.
   - Aplicará centralmente las configuraciones necesarias para la detección y/o eliminación del software malicioso.
   - Actualizará las firmas antivirus a través de la consola central de administración.
   - En caso de ser necesario, creará y distribuirá los procedimientos necesarios para la eliminación manual del software malicioso.
7. El ATI será el responsable de:
   - Implementar la Solución Antivirus Institucional en todos los equipos de cómputo a su cargo.
   - Solucionar contingencias presentadas, ante el surgimiento de software malicioso que la solución no haya detectado.
   - Notificar al centro de operaciones de la RIUADY en caso de contingencia con software malicioso.
8. Con el fin de evitar la propagación del software malicioso a otras redes de la RIUADY, el Centro de Operaciones de la RIUADY aislará la red de una dependencia notificando a las autoridades competentes, en las condiciones siguientes:
   - Cuando la contingencia con software malicioso no sea controlada.
   - Si la dependencia no aplica las políticas de software antivirus institucional
10. Todos los Equipo de Computo que se conecte a la red interna de una DES deberá contar con un sistema antivirus actualizado.
11. Todos los equipos de cómputo de la UADY deberán tener instalada la última versión aprobada de la solución antivirus institucional por el Centro de Operaciones de la RIUADY.
12. El Centro de Operaciones de la RIUADY podrá aplicar las acciones necesarias en el sistema antivirus institucional para garantizar la seguridad de la información de los equipos, sistemas y usuarios de cómputo.:

13. El ATI deberá llevar a cabo actividades de monitoreo por lo menos una vez a la semana, desde la consola de administración del sistema antivirus institucional y notificar cualquier anomalía que detecte al Centro de Operaciones de la RIUADY.

Capítulo: 6: Esquema de Seguridad en Servidores

Administración y seguridad de servidores

Se deberá proporcionar una disponibilidad del 98%, excluyendo los mantenimientos programados.

Cada dependencia deberá establecer un programa de mantenimiento preventivo a sus Equipos Servidores que contendrá como mínimo:

- Respaldo de las configuraciones.
- Actualizaciones de software.
- Resguardar y depurar las bitácoras del sistema.
- Revisión de su configuración.
- Limpieza física

El ATI deberá utilizar la herramienta de monitoreo institucional para la revisión del desempeño del Servidor.

Cada dependencia deberá establecer un programa de respaldos de información crítica.

Plataformas Windows

El Servidor deberá contar con las características y configuraciones mínimas recomendadas en las Wikis de la RIUADY

El Servidor deberá contar con sistema antivirus institucional y firewall activado.

Plataformas Unix/Linux

El Servidor deberá contar con las características y configuraciones mínimas recomendadas en las Wikis de la RIUADY

El Servidor deberá contar con sistema antivirus, firewall y detección de intrusos institucional.

Capítulo 7: Políticas de tecnologías web

1. La publicación de información en el portal web de la Universidad Autónoma de Yucatán (www.uady.mx) deberá considerar los siguientes aspectos fundamentales: imagen institucional, presencia universitaria, funcionalidad y contenido con base en el estándar vigente.

2. Únicamente se publicará información a solicitud de las DES, grupos estudiantiles, asociaciones, sociedades de alumnos o grupos diversos reconocidos por la Universidad Autónoma de Yucatán.

3. Se prohíbe la publicación de información estipulada por las leyes federales, estatales y municipales vigentes, así como la publicación de información privada o secreta, calumnias, injurias o difamaciones contra cualquier persona física o moral. Además de cualquier información de carácter comercial y ajenas a la institución o que persiga fines de lucro.

4. Por cada Sitio web de la DES, deberá existir los siguientes roles: administrador de Tecnologías Web, responsable de la información, y encargado de mantener el contenido. Quienes deberán mantener actualizado el sitio web con base en el estándar vigente; siendo el responsable de la información, la persona que avala y se responsabiliza del contenido.

5. El ATW es la persona que se encargará de crear, colocar y actualizar la información en el sitio web de la DES, debiendo cubrir los estándares vigentes para el desarrollo de sitios web. Dicho responsable deberá ser empleado de la Universidad Autónoma de Yucatán, sin embargo, se pueden contratar servicios de desarrollo de forma externa.

6. El ATW es responsable de generar respaldos y depuración periódica del sitio web a su cargo.

7. En cumplimiento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), si algún Sistema de Información Web solicita información considerada sensible al usuario a través de formularios, este deberá contar con un aviso de privacidad que indique cómo será usada la información recabada.

8. Las páginas académicas (profesores, alumnos) que por su naturaleza pudieran contener alguna información privada o personal deberán incluir en su página principal una leyenda que aclare que la información contenida en sus páginas, tanto texto como ligas, son responsabilidad de la persona y no expresan el punto de vista de la Universidad Autónoma de Yucatán o alguna de sus dependencias o hacer una "***página de responsabilidad"***. Lo anterior no es de ninguna manera un permiso para poder publicar información no académica.

9. Los servicios de la RIUADY para la publicación de información en el servidor de la Universidad son las siguientes: hospedaje de sitios web, cuentas de acceso para administración de sitios web, dominios virtuales, auditoría de código y alojamiento de bases de datos para sistemas web.

10. El centro de operaciones otorgará un plazo máximo de un mes a partir del aviso de hospedaje de sitio web de la DES para colocar información, en caso contrario será deshabilitado y para habilitarlo nuevamente, se tendrá que solicitar de nueva cuenta el servicio de hospedaje de sitio web.

11. Es obligación del ATW de la DES optimizar el almacenamiento que tiene asignado en el sitio web, por lo cual no deberá subir información irrelevante o redundante. Cada mes se deberán depurar los archivos, retirando aquellos que ya no sean de utilidad. No se permite por ningún motivo, tener información personal en el sitio web de la DES.

12. En caso de que la DES realice un uso no aceptable del servicio web se realizará una suspensión temporal del sitio web en el servidor y la cancelación de la cuenta hasta que el uso no aceptable haya pasado.

13. Los Sistemas de Información Web por incorporarse en el portal web de la Universidad Autónoma de Yucatán, deberán pasar por una auditoría de seguridad, antes de su publicación, a fin de comprobar que no existe riesgo para los demás sitios Web hospedados en el servidor. En caso de que el Sistema de Información Web, se ponga en funcionamiento sin haberse solucionado los incumplimientos encontrados en la auditoría de seguridad, será responsabilidad de la dependencia; por lo que, en caso de sufrir algún ataque, será dado de baja inmediatamente hasta que se corrijan los incumplimientos de seguridad.

14. No se deberán publicar sitios web con información incompleta o sistemas parcialmente desarrollados, ya que el contenido se encuentra público en Internet ya que se afecta tanto la imagen institucional, como la seguridad de los servidores.

15. El uso de cuentas institucionales para redes sociales deberá apegarse al documento de "Recomendaciones de Seguridad para el uso de Redes Sociales"

REQUERIMIENTOS DE DESARROLLO Y ADMINISTRACIÓN DE SITIOS WEB INSTITUCIONALES

- Los espacios web y bases de datos que ofrece la Coordinación General de Tecnologías de la Información y Comunicación se encuentran ubicados en equipos servidores de recursos limitados, útiles únicamente para sistemas pequeños y de pocos usuarios concurrentes. En caso de que se pretenda implementar un Sistema de Información Web con alta demanda de usuarios y procesamiento, se deberá solicitar una reunión de requerimientos a la Coordinación para plantear alternativas de alojamiento.
- Una página web no debe exceder de 2MB en el peso total de carga.
- Enlaces a los siguientes URLs (direcciones web), según a donde corresponda la sección:
    - Al portal web de la Universidad Autónoma de Yucatán (http://www.uady.mx)
    - Al departamento inmediato al que corresponde, en caso de que esta tenga una sección en el servidor.
    - Nombre y cuenta de correo de la persona responsable de la información del sitio web.
    - Nombre y cuenta de correo del ATW.
    - Despliegue de la fecha actual
    - Opcionalmente un contador de accesos proporcionado por el Centro de Operaciones de la RIUADY
- Utilizar un diseño y estilos estandarizados para crear consistencia visual en todos los documentos relacionados, utilizando la plantilla institucional.
- Que las páginas sean sencillas y pequeñas.
- Evitar el uso de imágenes grandes y escalarlas usando etiquetas HTML.
- Utilizar el mínimo de texto en listas o menús
- Utilizar la leyenda de derechos de autor (D.R.) cuando sea apropiado y/o necesario
- Indicar con una leyenda si alguna liga va a llevar a un documento o imagen grande, y señalar el tamaño en KB.
- Usar un esquema de programación que permita la compatibilidad con diferentes navegadores.
- Enfoque orientado a los usuarios que requiere la realización de pruebas preliminares con un grupo de usuarios, para observar la facilidad de navegación, lógica de uso y tiempos de acceso

- Al desarrollar sistemas web, se debe optimizar el número de consultas a la base de datos, a la vez que se eviten consultas anidadas, así como cerrar todas las conexiones hechas a la misma.
- Para bases de datos relacionales, se deberán agregar índices para optimizar consultas con uniones entre las tablas.
- Realizar las debidas validaciones a los formularios del sitio web
- A fin de evitar ataques de inyección a las bases de datos, se deberá implementar la función mysql_real_escape_string() en aquellos parámetros recibidos por GET y/o POST que se integren a la consulta de base de datos.
- Evitar el pase de parámetros de formularios por GET, dado que la información es vista en la URL, pudiéndose cachar en el navegador, al mismo tiempo que este método está limitado a 255 caracteres.
- El portal institucional permitirá como máximo la publicación de tres banners simultáneos, por lo que, en caso de existir más solicitudes de publicación de banners, el centro de operaciones de la RIUADY en conjunto con los responsables de la información determinarán los banners seleccionados.
- Al solicitar la creación de Dominios Virtuales temporales, usados para eventos y/o congresos, el solicitante deberá especificar su periodo de vigencia y, una vez concluido este, ingresar una nueva solicitud para la baja del dominio.
- Los nombres de dominios virtuales deberán llevar la siguiente nomenclatura:
    - www.{NOMBREDOMINIO}.{DES}.uady.mx.
    - NOMBREDOMINIO deberá ser un nombre corto que identifique la naturaleza del sitio.
    - DES es el nombre abreviado de la dependencia que solicita el dominio. En caso de tratarse de sitios de índole institucional, se podrá prescindir del nombre de la dependencia.

Información considerada no aceptable para sitios web institucionales

- Material ofensivo para la comunidad, esto incluye frases groseras, subversivas, racistas o similares.
- Información de actividades ilegales
- Material que muestre o promueva el abuso en cualquier forma
- Material que promueva el daño físico, emocional o psicológico de un individuo o grupo.
- Páginas con propósitos comerciales, por ejemplo:
    - Venta de cualquier producto o servicio
    - Patrocinadores o publicistas que originen o no, un ingreso económico, promoviendo actividades personales o que no tengan fines académicos
    - Imágenes, "banners" o logotipos comerciales de cualquier clase con o sin ligas que no tengan convenio con la Universidad
- Páginas o imágenes ocultas o aquellas que no pueden ser accedidas desde un lugar visible.
- Archivos de otros servidores, con o sin fines de lucro.
- Páginas para infringir los derechos de autor, incluyendo la piratería o ligas a lugares que lo contengan o lo promuevan, así como los archivos multimedia, información o publicación de números de serie o de registro de programas, o cualquier tipo de actividad o utilería para romper las protecciones.
- Promover las páginas y/o páginas que consistan en ligas a lugares no seguros.

Capítulo 8: Políticas de videoconferencia

1. La recepción de una solicitud del servicio de videoconferencia implica el conocimiento, aceptación y vigilancia de estas políticas por parte del solicitante.
2. Toda solicitud de servicio deberá hacerse por escrito mediante el sistema de atención a usuarios de la Coordinación General de Tecnologías de la Información y Comunicación(http://www.riuady.uady.mx/reportes), con un mínimo de 5 días hábiles previos al evento para conexiones a sitios pertenecientes a la UADY, y 15 días hábiles previos al evento para conexiones a sitios externos a la UADY.
3. La recepción de una solicitud de servicio no implica la garantía de prestación de este.
4. Toda solicitud de servicio estará sujeta a disponibilidad de enlaces, salas y equipos.
5. El centro de operaciones notificará al usuario la factibilidad del servicio en un plazo no mayor a 24 horas posteriores a la recepción de la solicitud correspondiente.
6. El usuario deberá especificar todos los elementos necesarios para su evento que se indican en la solicitud para que dé inicio el trámite. El Centro de Operaciones de la RIUADY no se hace responsable por fallas en el servicio a causa de omisiones y/o falsificaciones en las que incurra el solicitante.
7. Se vigilarán todos los horarios estrictamente, no habiendo prórroga durante o después del horario solicitado. El Organizador de la actividad debe considerar, antes de entregar su solicitud, el tiempo estrictamente necesario para las sesiones y pruebas
8. El usuario deberá concertar la videoconferencia con los sitios requeridos. El centro de operaciones de la RIUADY solicitará al usuario los datos de los contactos académicos y técnicos correspondientes.
9. El centro de operaciones de la RIUADY sujeta su programación al horario vigente en el centro de México, así como al calendario de labores de la Universidad Autónoma de Yucatán.
10. No se permitirá la conexión de sitios a cualquier videoconferencia cuando ésta lleve trascurridos más de cinco minutos.
11. Todo sitio en las DES de la UADY deberá poseer un identificador claramente visible, que permita a los sitios remotos reconocerlo durante una videoconferencia.
12. Toda sala que no cumpla las normas y procedimientos específicos de las videoconferencias: cancelación de micrófonos, tiempos de interacción, total de asistentes y registros definidos por los organizadores de los eventos, es susceptible de ser desconectada de la videoconferencia sin previo aviso.
13. Toda DES que posea una sala de videoconferencia es responsable de su instalación, administración y mantenimiento.
14. Los equipos de videoconferencia de las DES deberán cumplir con las normas técnicas internacionales de operación de equipos multimedia, en función del tipo de enlace que se utilice.

15. Todo equipo de videoconferencia en la RIUADY deberá ser compatible con el resto de los sistemas que componen dicha red.
16. La RIUADY no se hace responsable por la calidad de servicio y funcionamiento de equipos que no cumplan con las normas aquí definidas.

REQUISITOS VIDEOCONFERENCIA

- Iluminación especial con luz indirecta.
- Paredes, techos y suelos acústicos, en colores no brillantes (se recomiendan el beige, gris o azul).
- Micrófonos de largo alcance.
- Bocinas altoparlantes.
- Aire acondicionado tipo mini Split.
- Cancelación de eco y ruido.
- Área de control.
- Extensión telefónica.
- Muebles cómodos.
- Ubicación de la cámara y de videoconferencia y videoproyector de acuerdo con el diagrama enviado.
- Enlace para comunicación a la red vía IP.
- Conexión de red en sala de videoconferencia.
- Dos conexiones de red para conexiones vía IP. Se requiere cableado UTP categoría 5e+ o 6 que deberán conectarse directamente al panel de parcheo del Centro de Comunicaciones de la Dependencia y del panel al equipo de comunicaciones (switch). En caso de que la distancia sea mayor a los 90 metros se requerirá realizar la conexión al centro de distribución de red más cercano.
- Cableado estructurado directamente al panel de parcheo del Centro de Comunicaciones de la Dependencia.
- Cámara de videoconferencia con conexión IP y soporte de protocolos H.323 y G.711.
- Códec (codificador/decodificador) (incluido en la cámara).
- La dirección IP de la cámara debe estar en la red 148.209.0.0 con máscara de red 255.255.255.0, de acuerdo con el rango proporcionado por el Centro de Operaciones de la RIUADY.
- El equipo de conferencia se debe ubicar en un espacio especial y debe estar disponible cuando se necesite sin llegar a requerir su configuración completa en cada ocasión.
- Pantalla y/o monitores de al menos 27" (TV).
- Proyector.

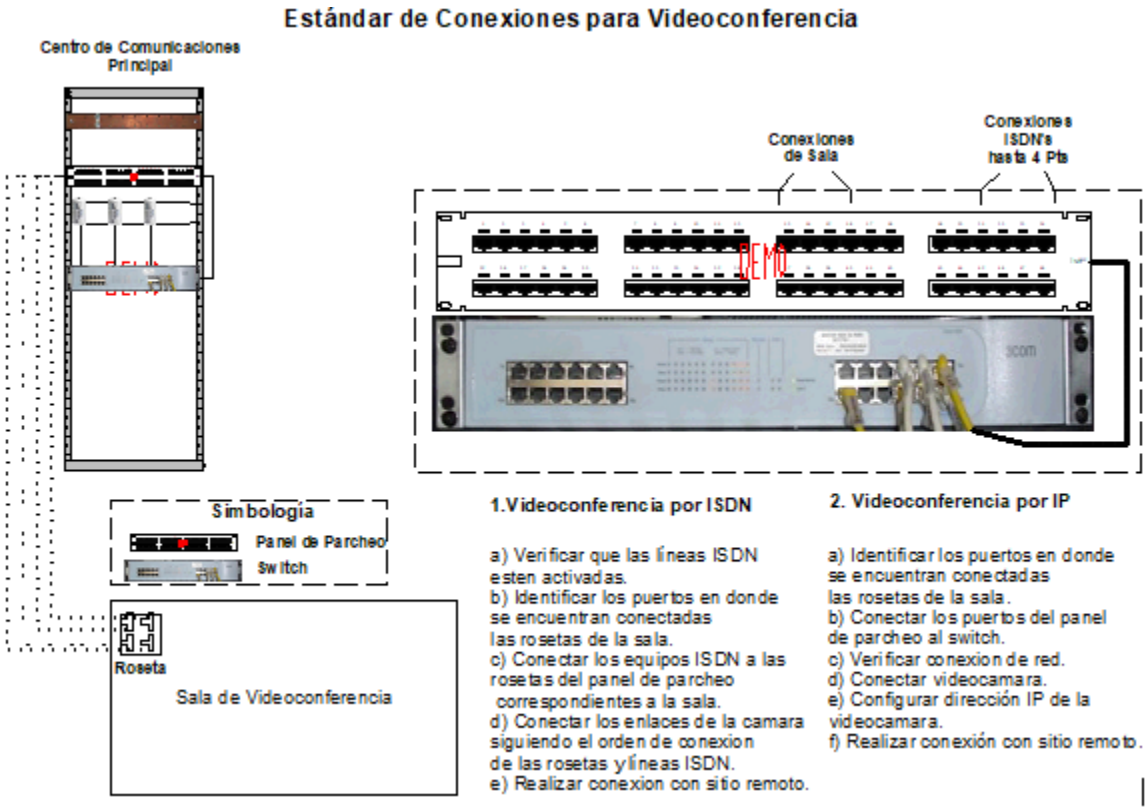


Figura 9 - Estándar de conexiones para videoconferencia

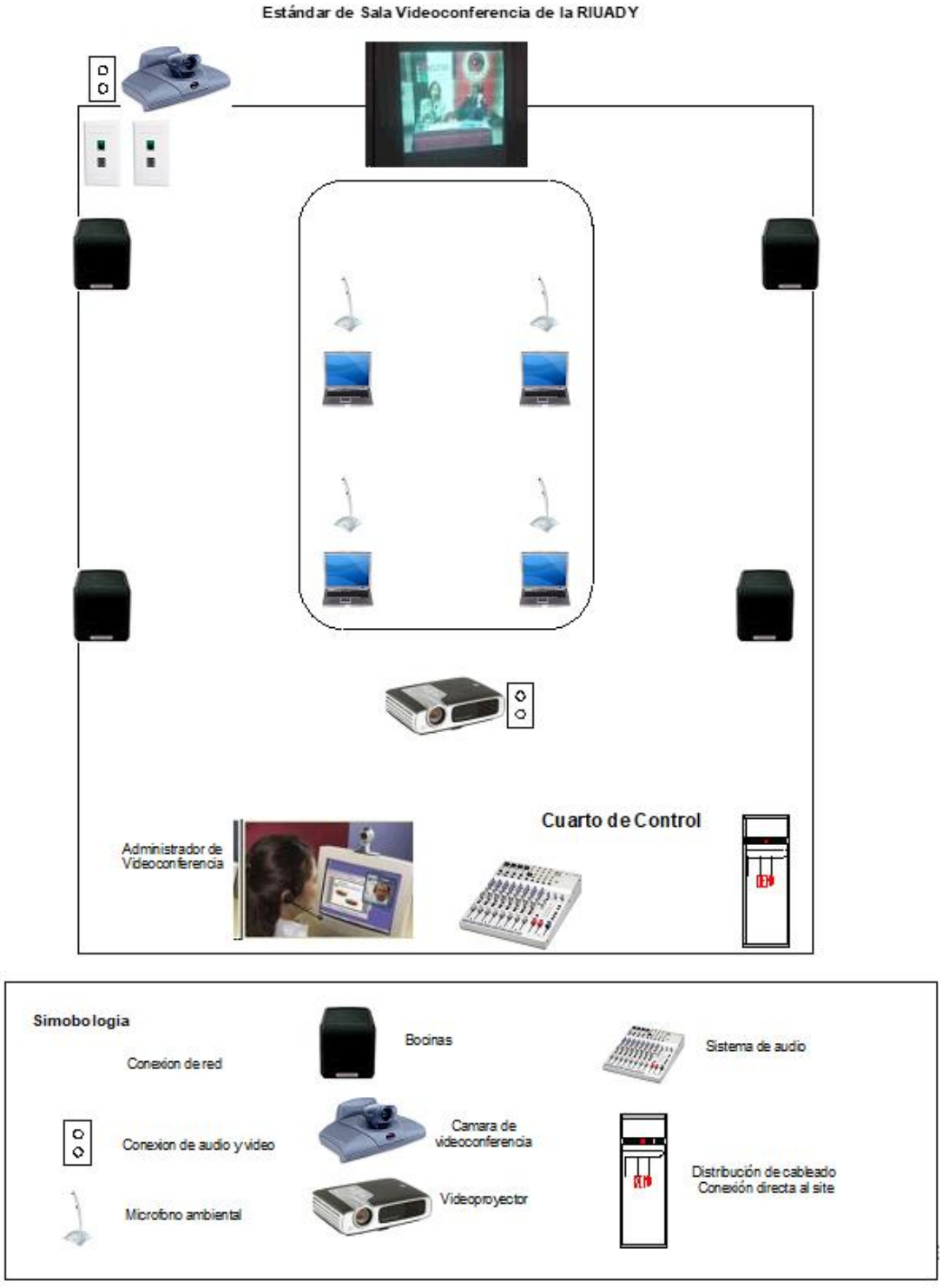


Figura 10 - Estándar de sala de videoconferencia de la RIUADY

Capítulo 9: Política de continuidad y contingencia de los servicios

Respaldos

1. La Información crítica de las Dependencias (correo electrónico, información administrativa y académica) será respaldada diariamente en forma automática y manual, según los procedimientos generados para tal efecto.
2. Los respaldos de la información crítica deberán ser almacenados en un lugar seguro y distante del sitio de trabajo.
3. La DES contará con un plan de contingencia para dar continuidad a los servicios de información definidos como críticos.
4.

Plan de Contingencia en caso de Tormenta Tropical o Huracán

Acciones Preventivas

1. Equipos de Comunicaciones y Servidores

    a. Sacar respaldos de información de la DES.
    b. Apagar y desconectar equipos de cómputo y comunicaciones, incluyendo no-breaks.
    c. Colocar los equipos, incluyendo los no-breaks sobre mesas.
    d. Alejar los equipos de las ventanas o de alguna posible entrada de humedad.

2. Infraestructura física y servicios

    a. Contar con impermeables, lámparas de emergencia, cintas.
    b. Encintar ventanas.
    c. Cubrir los equipos con bolsas de plástico

3. DES que cuentan con Planta de Emergencia:

    a. Realizar mantenimiento general de la planta eléctrica de emergencia.
    b. Mantener tanque lleno de diesel.
    c. Tener un tambo de diesel lleno.

4. Sistema de comunicación con personal.

    a. Contar una línea telefónica analógica con dispositivo analógico, en su caso conectar un teléfono analógico en la línea ISDN de su DES.
    b. Mantener los teléfonos celulares cargados.

Acciones después de la Tormenta Tropical/Huracán

5. Revisión de daños en las ventanas del centro de comunicaciones, centro de cómputo y/o áreas correspondientes. En su caso aislar los equipos afectados o en amenaza. Limpiar y secar pisos.
6. Verificar el funcionamiento de las líneas telefónicas.
7. Secar los equipos no breaks antes de encenderlos a fin de evitar que exploten por exceso de humedad; en lo posible con compresor de aire.
8. Secar los equipos de comunicaciones y posteriormente verificar que los equipos estén en funcionamiento.
9. En caso de contar con enlace inalámbrico, verificar posibles daños en la infraestructura de torre de comunicaciones.
10. Proporcionar las facilidades de acceso a los centros de comunicaciones al personal de la Coordinación General de Tecnologías de Información, para la realización de configuraciones de respaldo en caso de requerirse.

REQUISITOS

Redundancia servicios	1. Utilización de los clientes delgados. 2. VPNs. 3. Disponibilidad de equipos de comunicaciones obsoletos.
Protección eléctrica	Mantenimiento semestral de la planta: limpieza y verificación de los niveles y en caso su completar diesel, aceite, refrigerante y líquidos para acumuladores.
Redundancia comunicaciones	1. Equipos de respaldo: switches, ruteadores, bridges, módulos de equipos de comunicaciones. 2. Tecnología XRN.
Enlaces	1. Enlace inalámbrico 2. Enlaces E1's. 3. Equipo con módem y línea telefónica. 4. Enlace a Infinitum
Personal	Guardia permanente

Tabla 4 - Acciones preventivas de contingencia

Capítulo 10: Política de dependencias universitarias

1. Las Dependencias deben llevar un control total escrito y/o sistematizado de sus recursos de cómputo que permitan un adecuado control interno.

2. Las Dependencias son las responsables de calendarizar y organizar al personal encargado del mantenimiento preventivo y correctivo de los equipos de cómputo e instalaciones que sirvan para garantizar las operaciones de los Servicios de TI.

3. La Dependencias son las responsables del buen uso y funcionamiento de los analizadores de redes, quedando el Centro de Operaciones de la RIUADY como organismo asesor respecto de la funcionalidad de este.

4. Si una dependencia viola las políticas de uso aceptable de la RIUADY, el Centro de Operaciones de la RIUADY aislará la red de esa dependencia.

5. El uso de analizadores de redes por personal no autorizado de las dependencias que genere un problema de seguridad podrá ser sancionado.

6. Cuando un usuario deje de laborar o de tener una relación con la institución el área de Recursos Humanos de las Dependencias deberá reportar al ATI y/o al Centro de Operaciones de la RIUADY, así como cualquier instancia de la universidad en la que este usuario tenga algún servicio activo.

7. Cuando un usuario deje de laborar o de tener una relación con la institución se deberán dar de baja las cuentas que este usuario tenga asignadas (o cambiar las contraseñas) y recibir los equipos que le hayan sido asignados.

Capítulo 11: Administrador de tecnologías de información

1. El ATI debe desactivar las cuentas INET de los usuarios, en los siguientes
    a) Si pone en peligro el buen funcionamiento de los sistemas.
    b) Si se sospecha de algún intruso utilizando una cuenta ajena.
    c) Cuando el jefe inmediato del usuario lo solicite mediante un documento explícito.
2. El ATI deberá ingresar de forma remota a computadoras única y exclusivamente para la solución de problemas y bajo solicitud explícita del propietario de la computadora.
3. El ATI deberá utilizar los analizadores de acuerdo con los siguientes lineamientos:
    a) Previa capacitación recibida del Centro de Operaciones de la RIUADY.
    b) Realizar la instalación bajo estricta licencia, con excepción de los de dominio público.
4. El ATI deberá realizar respaldos por lo menos una vez al mes de la información de los recursos de cómputo que tenga a su cargo.
5. El ATI debe actualizar la información de los recursos de cómputo de la Dependencia a su cargo, cada vez que adquiera e instale equipo o software.
6. El ATI debe registrar cada máquina en el control interno de equipo de cómputo y red de la Dependencia a su cargo.
7. El ATI debe auditar periódicamente los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.
8. EL ATI debe realizar la instalación o adaptación de sus sistemas de cómputo de acuerdo a las necesidades de la propia dependencia, debiendo reportar los cambios requeridos al Centro de Operaciones de la RIUADY.
9. Es responsabilidad del ATI revisar diariamente las bitácoras de los sistemas a su cargo.
10. EL ATI reportará al Centro de Operaciones de la RIUADY, los incidentes de seguridad, a través del sistema de atención de usuarios, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.

Capítulo 12: Políticas para usuarios

1. Los recursos de cómputo y Servicios de TI empleados por el usuario deberán ser afines al trabajo desarrollado, no deberán ser proporcionados a personas ajenas y no deberán ser utilizados para fines personales.
2. Todo usuario debe respetar la privacidad, confidencialidad y derechos individuales de los demás usuarios.
3. El correo electrónico no se usará para envío masivo, materiales de uso no académico o innecesarios (entiéndase por correo masivo todo aquel que sea ajeno a la institución, tales como cadenas, publicidad y propaganda comercial, política o social, etcétera).
4. El usuario deberá respaldar su información, dependiendo de la importancia y frecuencia de modificación de esta.
5. Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de propiedad intelectual.
6. Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de TI de la UADY, de acuerdo con las políticas que en este documento se mencionan.
7. Los usuarios deberán solicitar apoyo al ATI de su dependencia ante cualquier duda en el manejo de los recursos de TI de la institución.
8. El usuario deberá renovar su contraseña al menos una vez al año y colaborar en lo que sea necesario, a solicitud del ATI.
9. El usuario deberá notificar al ATI en los siguientes casos:
    a. Si observa cualquier comportamiento anormal en el Servicio de TI.
    b. Cuando un usuario deje de tener alguna relación oficial con la institución, el área de recursos humanos o control escolar de la dependencia deberá notificar al ATI, para la actualización del perfil del usuario, preservando la seguridad de los servicios de información de la UADY.
10. Si un usuario viola las políticas de uso de los servicios de TI, el ATI podrá cancelar totalmente su cuenta de acceso, notificando a las autoridades correspondientes.
11. El usuario no deberá desinstalar la solución antivirus de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus.
12. Si el usuario hace uso de medios de almacenamiento personales, éstos serán analizados por la solución antivirus en la computadora del usuario o por el equipo designado para tal efecto.
13. El usuario deberá comunicarse con el ATI de su dependencia en caso de problemas de virus para buscar la solución.
14. El usuario será responsable del comportamiento de su equipo dentro de la RIUADY. El ATI se reserva el derecho de desconectarlo de la red cuando se detecte un comportamiento inadecuado.
15. Los usuarios de cómputo de la DES tendrán derecho a una cuenta personal para uso de los servicios de TI misma que se proporcionará por el departamento de cómputo a solicitud expresa del usuario y para lo cual deberá cumplir alguno de los siguientes requisitos: ser personal académico, personal administrativo o alumno.

16. El usuario deberá autenticarse con su cuenta institucional para tener acceso a los servicios de TI que la DES le proporcione.
    - El perfil de los alumnos deberá tener restricciones de seguridad establecidas por el departamento de cómputo.
    - El usuario será responsable del uso de su cuenta de usuario institucional
    - El usuario será el responsable de su información.
    - Las cuentas de usuario serán deshabilitadas después de cierto tiempo de inactividad y tendrán que ser reactivadas a solicitud del usuario.
    - El departamento de cómputo podrá cancelar de forma temporal o permanente las cuentas de usuario si detecta un uso no adecuado de las mismas.

Capítulo 13: Políticas para centros de cómputo

1. Los centros de cómputo podrán ofrecer servicios de cómputo, soporte técnico y servicios audiovisuales.

2. Cada dependencia deberá contar con un reglamento actualizado de uso de los centros de cómputo de acuerdo con el estándar de operación de estos.

3. Cada dependencia dará a conocer dicho reglamento mediante diversos mecanismos como pláticas introductorias y la publicación vía web y la entrega del documento.

4. La administración de los centros de cómputo deberá llevarse a través de métodos automatizados.

5. Los ATI de los centros de cómputo deberán verificar el grado de seguridad y si es legal del software adquirido e instalado en los equipos del centro de cómputo.

6. Para optimizar tiempo y recursos de los centros de cómputo, las dependencias deberán contar con los siguientes elementos mínimos: un cañón, conexión a la RIUADY y equipo de cómputo en cada sala. Los equipos deberán ser fijados para evitar alteración o robo de estos.

7. Se podrá dar asesoría de acuerdo con los criterios y prioridades de atención establecidos por el ATI.

8. Equipo de cómputo ajeno a la institución no se dará el soporte por parte del centro de cómputo. A menos que lo autorice alguna autoridad o solo se podrá dar soporte cuando requiera conexión a la red.

9. Las dependencias deberán contar con personal para actividades administrativas, para soporte técnico, para administrar los recursos de cómputo y desarrollo de aplicaciones. No existe personal para todas las actividades

10. El centro de cómputo de la dependencia deberá contar con la siguiente documentación: información técnica (red, edificios, eléctricas, manuales y procedimientos), normatividad, inventarios de hardware y software que puede basarse en los estándares y procedimientos desarrollados o recopilados por el Centro de Operaciones de la RIUADY.

Capítulo 14: Políticas de correo electrónico institucional

1. La cuenta de correo electrónico institucional es personal, intransferible y renovable por el usuario.

2. El servicio de correo electrónico es de carácter académico informativo, quedando estrictamente prohibido el uso con fines comerciales, lucrativos, promoción o venta.

3. Es responsabilidad del poseedor de una cuenta, el mantener la confidencialidad de la contraseña.

4. La confidencialidad del servicio de correo electrónico son productos del manejo que los usuarios den al servicio, por lo que es recomendable mantener las reservas correspondientes.

5. Es responsabilidad del usuario el respaldo y el contenido de la información de su buzón de correo electrónico.

6. Para obtener una cuenta de correo @correo.uady.mx, el ATI deberá acceder a http://www.riuady.uady.mx/reportes y seguir los pasos mencionados en el sitio para solicitar una cuenta de académico, administrativo o de alumno.

Capítulo 15: Políticas de directorio activo (INET)

De computadoras

1. Todas las computadoras de la DES conectadas a la RIUADY deberán pertenecer al Directorio Activo (INET) y cumplir con los Estándares y Políticas Antivirus de la UADY.

2. El ATI deberá integrar todas las computadoras de su dependencia al esquema de INET de acuerdo con el instructivo para agregar una computadora a INET.

3. Las computadoras que se encuentren inactivas por más de 120 días naturales serán desactivadas de manera automática por los procesos de mantenimiento del servicio de Directorio Activo.

4. Las computadoras que se encuentren inactivas por más de 180 días naturales serán eliminadas de manera automática por los procesos de mantenimiento del servicio de INET.

De cuentas de usuarios INET

1. La cuenta INET del personal de la UADY deberá estar homologada con su cuenta de correo electrónico institucional, esto es, el identificador del usuario (login) INET deberá ser igual al identificador del usuario (login) de correo electrónico.

2. La cuenta INET es personal, intransferible y renovable por el usuario.

3. Es responsabilidad del poseedor de una cuenta INET, el mantener la confidencialidad de la contraseña.

4. Las cuentas que se encuentren inactivas por más de 120 días naturales serán desactivadas de manera automática por los procesos de mantenimiento del servicio INET.

5. Las cuentas que se encuentren inactivas por más de 180 días naturales serán eliminadas de manera automática por los procesos de mantenimiento del servicio de INET. Notificar al ATI en el caso del personal con licencia.

6. Es responsabilidad del ATI desactivar o eliminar de manera inmediata, las cuentas de directorio activo del personal que ya no labore en la UADY, previa notificación por parte de recursos humanos de la DES.

7. En caso de que algún personal sea transferido a otra dependencia de la UADY, es responsabilidad del ATI remover los permisos otorgados a la cuenta INET de este personal sobre los servicios e información de la dependencia origen; esto aplica a todos los servicios que requieren una autenticación con INET, previa notificación por parte de recursos humanos de la DES.

8. Al crear la cuenta INET de personal de la dependencia, el ATI deberá validar la existencia de la cuenta en el servicio. En caso de que la cuenta INET ya existe en otra dependencia, el ATI deberá solicitar al Centro de Operaciones a través del Sistema de Atención a Usuarios la transferencia de esta cuenta a su dependencia. El Centro de Operaciones transferirá la cuenta tomando en cuenta lo siguiente:
    a. El Centro de Operaciones notificará por correo electrónico al ATI de la dependencia origen sobre la transferencia del usuario.
    b. Todo usuario que sea transferido de una dependencia a otra perderá la membresía existente a todos los grupos de INET de la dependencia origen.
    c. El Centro de Operaciones no eliminará el acceso sobre los servicios e información de la dependencia de origen, de acuerdo con la política 17.6.

Capítulo 16: Políticas de red inalámbricos

1. Toda instalación solución inalámbrica deberá cumplir con las políticas de Directorio Activo (INET) y Políticas de Uso Aceptable de la RIUADY.

2. El Centro de Operaciones de la RIUADY, se reservará el derecho de inhabilitar cualquier solución inalámbrica que no cumpla con las políticas de los Servicios de Red Inalámbrica detectada.

3. Cualquier solución inalámbrica será instalada y configurada por el Centro de Operaciones y el ATI de la DES.

4. Cuando la velocidad de transmisión de la información en la solución inalámbrica sea baja o limitada, originados por equipos no estandarizados, exceso de usuarios simultáneos y/o estar fuera de la cobertura de la solución inalámbrica; el centro de operaciones no podrá garantizar el funcionamiento de los servicios de la RIUADY e internet.

ESQUEMA DE SERVICIOS INALÁMBRICOS

Servicios inalámbricos

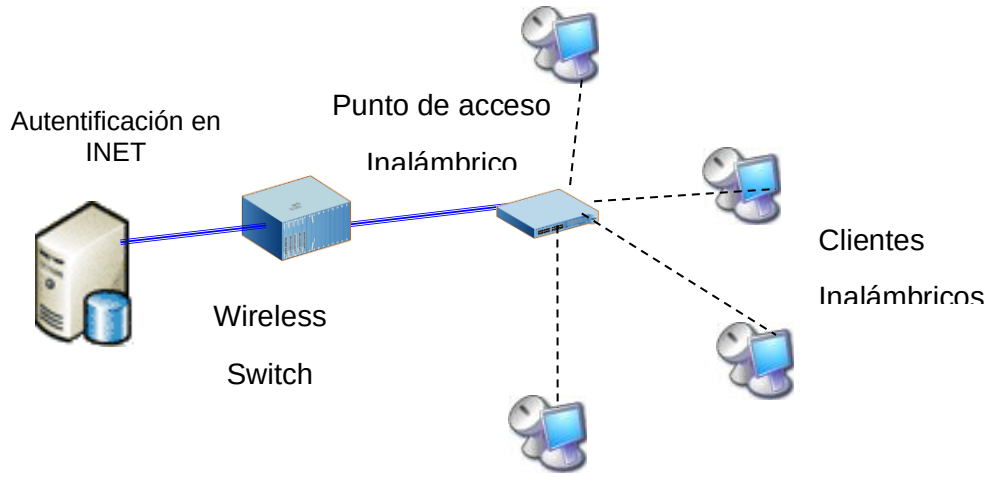


Figura 11 - Servicios Inalámbricos

Capítulo 17: Herramienta de trabajo colaborativo en la NUBE (Webex)

1. La recepción de una solicitud del servicio de WEBEX implica el conocimiento, aceptación y reforzamiento de estas políticas por parte del solicitante.

2. Toda solicitud de servicio deberá realizarse a través el Sistema de Atención a Usuarios de la Coordinación General de Tecnologías de la Información y Comunicación (http://www.riuady.uady.mx/reportes), con un mínimo de 5 días hábiles previos al evento.

3. El solicitante de la reunión será responsable de distribuir el Número de la sesión y la Contraseña de la sesión a los participantes de la reunión.

4. La sesión será monitoreada en todo momento y podrá ser finalizada sin previa notificación en caso de identificarse que se incurre en la presentación o uso de contenido NO ACADÉMICO.

A continuación, se proporciona un listado de referencia para contenido NO ACADÉMICO:

- Material ofensivo para la comunidad, esto incluye frases groseras, subversivas, racistas o similares.
- Información de actividades ilegales
- Material que muestre o promueva el abuso en cualquier forma.
- Material que promueva el daño físico, emocional o psicológico de un individuo o grupo.
- Información con propósitos comerciales, por ejemplo:
- Venta de cualquier producto o servicio.
- Patrocinadores o publicistas que originen o no, un ingreso económico, promoviendo actividades personales o que no tengan fines académicos.
- Imágenes, "banners" o logotipos comerciales de cualquier clase con o sin ligas que no tengan convenio con la Universidad
- Contenido para infringir los derechos de autor, incluyendo la piratería o ligas a lugares que lo contengan o lo promuevan, así como los archivos multimedia, información o publicación de números de serie o de registro de programas, o cualquier tipo de actividad o utilería para romper las protecciones.

5. La CGTIC no se hace responsable por la calidad de servicio y funcionamiento de computadoras no estandarizadas que no cumplan con los estándares requeridos en este documento.

6. La CGTIC no se hace responsable por la calidad de servicio y funcionamiento en redes inalámbricas que no cumplan con la cobertura y calidad requerida por el servicio.

Capítulo 18: Pantalla y escritorio limpio.

1. Equipos de cómputo.

a. Toda vez que un usuario se ausente de su lugar de trabajo, deberá cerrar la sesión de trabajo para proteger el acceso a las aplicaciones y servicios de la institución.
b. El escritorio de los equipos de cómputo (pantalla inicial) deberá tener solamente carpetas, archivos y/o aplicaciones de uso diario.
c. Una vez que el usuario ha terminado su jornada laboral, deberá apagar el equipo.

2. Equipos de reproducción de información.

a. Los equipos de reproducción de información (por ejemplo: impresoras, fotocopiadoras), deben estar ubicados en lugares con acceso controlado.
b. La información clasificada o sensible, cuando se imprima, debe ser retirada inmediatamente de las impresoras, evitando el acceso a esta información por personas no autorizadas.

3. Espacio de trabajo.

a. Los documentos con información personal de otros usuarios u dependencias solamente se colocan en los escritorios mientras el usuario está trabajando en ellos.
b. Cuando una persona externa se acerque a hablar con algún usuario que esté manejando información sensible o confidencial, se debe dar vuelta a la hoja o cerrar el expediente.
c. En caso de haber usuarios que estén ubicados cerca de zonas con acceso al público, al ausentarse de su lugar de trabajo deben guardar los documentos y medios que contengan información confidencial o de uso interno.
d. Al finalizar la jornada de trabajo, todo usuario deberá guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno.

Capítulo 19: Sanciones.

A usuarios:

1. Cualquier acción que vaya en contra de las políticas de seguridad en cómputo de la UADY será sancionada con la suspensión de los servicios de cómputo y red, por un período de tres meses en una primera ocasión y de manera indefinida en caso de reincidencia.

A Dependencias:

1. Cuando se presente una contingencia cuyo origen sea la falta de aplicación de las políticas de seguridad en cómputo, el Centro de Operaciones de la RIUADY aislará la red de una dependencia hasta que las acciones de mitigación correspondientes hayan sido llevadas a cabo.

2. Cuando se determine que un servidor sea el origen de una contingencia, El Centro de Operaciones de la RIUADY aislará

PERSONAL QUE PARTICIPÓ EN LA ELABORACIÓN DEL DOCUMENTO:

Fis. Juan Antonio Herrera Correa
MATI Carmen Denis Polanco
MATI Carmen Díaz Novelo
MATI Israel Novelo Zel
MAO David Loeza Dorantes
LCC Miguel Briceño Quijano
MATI Mario Gutiérrez Leal
MAO Emmanuel Serrano Piña
LCS Marcela Concha Vázquez
MCC Enrique Solís Pomar
MAO Wilberth Pérez Segura
L.C.C. Claudia Pacheco Puch
MAO Marco Cervera Piña
MAO Angel Arroyo Herrera
LATI Ana Cinthia Piñeiro Quiñones
L.C.C. Rodrigo Esparza Sánchez
MAO José René Martín Castillo
LATI Ángel Gabriel Pisté Homa
LI Maribel Pérez Rodríguez
LCC Iliana Georgina Alonso Morales
Lic. Jorge Raúl Carrillo Cabrera

Referencias Bibliográficas

Briceño Quijano, Miguel; Las TIC como Soporte a la Gestión del Conocimiento; Facultad de Ingeniería Química, Universidad Autónoma de Yucatán; México; 2003.

Díaz Novelo, Carmen; Planeación Tecnológica en la Red Integral de la Universidad Autónoma de Yucatán; Facultad de Ingeniería Química; Universidad Autónoma de Yucatán; México; 2002.

Novelo Zel, Israel; Modelo de Gestión Tecnológica de la RIUADY; Facultad de Ingeniería Química; Universidad Autónoma de Yucatán; México; 2004.

5. DOCUMENTOS DE REFERENCIA

Código	Nombre del documento	Lugar de almacenamiento
ANSI/TIA/EIA 568-B	Estándar para Cableado de Telecomunicaciones en Edificios Comerciales.	Documento Electrónico. Archivo del área.
J-STD 607-A.	Estándar de Telecomunicaciones para sistema de protección y tierras en Edificios Comerciales.	Documento Electrónico. Archivo del área.
ISO 17799.	Estándar de Seguridad en Cómputo.	Documento Electrónico. Archivo del área.

6. GLOSARIO

6.1 .- SIGLAS

ABD. Administrador de las bases de datos del Sistema Institucional de Información.

ATI. Administrador de Tecnologías de Información. Responsable de la administración de los equipos de cómputo, sistemas de información y redes de telemática de una dependencia de la UADY.

ATW. Administrador de Tecnologías Web. Responsable de la administración de las Tecnologías y servicios Web.

6.2 .- DEFINICIONES

Base de datos. Colección de archivos interrelacionados.

Centro de Operaciones. Es la dependencia que se encarga del funcionamiento y operación de la RIUADY.

Centro de telecomunicaciones. Espacio designado en la dependencia a los equipos de telecomunicaciones y servidores.

Cobertura. Área geográfica donde se proporciona la señal y el servicio de red inalámbrica.

Contraseña. Conjunto de caracteres que permite el acceso de un usuario a un recurso informático.

Dependencia. Facultad, Escuela, Dependencia de Educación Superior, Campus, Dirección, Subdirección, Departamento y Centro de Investigaciones de la UADY.

Dependencia Origen. Dependencia desde la cual se transferirá una cuenta INET.

INET. Nombre del servicio de Directorio Activo en la UADY.

Internet académico. Es un servicio de acceso a Internet a través del navegador Web para profesores, investigadores y proyectos académicos institucionales

Intranet. Servicios de información y comunicación de una DES.
Solución Antivirus Institucional. Conjunto de herramientas de software administradas institucionalmente que son utilizadas en la UADY para la detección y/o eliminación de software malicioso.

Software Malicioso. También conocido como código maligno o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse, robar o dañar información de un equipo de cómputo o sistema de información.

TIC. Tecnologías de Información y de comunicaciones.

Usuario. Cualquier persona que haga uso de los servicios proporcionados por las dependencias responsables de los equipos de cómputo, sistemas de información y redes de telemática.

7. CONTROL DE REVISIONES

Nivel de revisión	Sección y/o página	Descripción de la modificación y mejora	Fecha de modificación
01	1 - 49	Corrección nombres, estandarización tamaños y fuentes, redacción y ortografía. Adecuación de políticas. Adecuación de imágenes.	22 de agosto de 2007
02	2, 26 – 28, 50	Adecuación de las políticas web de acuerdo al crecimiento y desarrollo de servicios. (Artículo 8.10, 8.11, 8.12, 8.16, 8.17, 8.18, 8.19 y estándares de desarrollo de sitios web).	20 de agosto de 2009
03	Caps. 2,3,4,6, 7 y 10	Adecuación de las políticas de infraestructura: artículo 2.13, tabla 1, puntos 2 y 5 de estándar protección eléctrica; requisitos de telecomunicaciones; capítulo 3 adecuación ortografía y término, tabla 3. Cambios generales en las políticas de antivirus. Capítulo 7, modificación a las actualizaciones de: respaldo diario, plataforma Unix, de educación en línea, sistema institucional de información, requisitos duplicados. Actualización artículos 10.2, 10.9, eliminación 10.10, 10.19, 10.20, 10.21. Ajuste en la numeración de los capítulos.	1 de julio de 2010
04	Caps. 16, 17, 18, 19 y 20	Se agregaron nuevos capítulos: las políticas de correo electrónico institucional, directorio activo, internet académico y servicios inalámbricos. El capítulo de sanciones se convirtió en el capítulo 20. Se revisó la ortografía y redacción de todo el documento. Se modificaron las políticas relacionadas con el GSC cambiándolo por Centro de Operaciones y ATI de DES.	27 de mayo de 2011
05	Caps. 1, 6 y 20	Se actualizó el glosario y se agregó el término al Software Malicioso. Se actualizaron todas las políticas del software antivirus institucional. Se actualizaron las sanciones creando la división de sanciones entre usuarios y dependencias. Se actualizaron los capítulos los de las políticas capítulos quedando en 19.	20 de diciembre de 2013

06	Cap. 8	Se actualizaron las políticas de seguridad web y se eliminaron políticas obsoletas en esta misma sección.	30 de abril de 2014
07	Cap. 19	Actualización al nuevo formato F-DGPLANEI-CC/GA-01/REV:03 Actualización de la numeración de las secciones. Correcciones de Ortografía en General. Se añadió el capítulo número 19 sobre las políticas de la plataforma de trabajo colaborativo (WEBEX). Quedando un total de 20 capítulos.	13 de mayo de 2015
08	Sección 4	Se añadió una tabla de contenido. Se actualizaron los puntos 1, 5, 8 y 10 del capítulo 1. Se actualizó la Tabla 1.- Requisitos de Infraestructura para los centros de telecomunicaciones. Se actualizaron los REQUISITOS DE TELECOMUNICACIONES Se añadió la Figura 6a.- Estándar para un centro de comunicaciones en una DES. Se añadió la Figura 6b.- Estándar para un centro de comunicaciones en una DES. Se añadió la figura 7.- Estándar para un centro de distribución de red (site secundario) en una DES. Se actualizaron los puntos 2 y 4 del Capítulo 2. Telecomunicaciones Se actualizó la Tabla 2.- Requisitos para las telecomunicaciones Se actualizó la Tabla 3.- Perfiles básicos de usuarios Se añadió el CAPÍTULO 20. PANTALLA Y ESCRITORIO LIMPIO	20 de marzo de 2016
09	Cap. 1,2,3,4,5,6,10,11,12,14,15,16	Se actualizaron los puntos 5 y 8 del capítulo 1. Se actualizó la Tabla 1.- Requisitos de Infraestructura para los centros de telecomunicaciones. Se actualizaron los siguientes apartados SITIOS DE TELECOMUNICACIONES, ESQUEMA DE PROTECCIÓN ELÉCTRICA, CABLEADO ESTRUCTURADO, REQUISITOS DE TELECOMUNICACIONES.	22 de septiembre de 2019

		Se eliminaron las 6a,6b y 7a, dejando únicamente la figura 6. Se actualizaron los puntos 2 y 5 del Capítulo 2. Telecomunicaciones. Se actualizó la Tabla 2.- Requisitos para las telecomunicaciones Se agregó la figura 7.- Estándar de protección eléctrica y telecomunicaciones de los centros de telecomunicaciones de las DES Se agregó la figura 8.- Estándar de conexión en la caja NEMA de los enlaces inalámbricos de la RIUADY. Se actualizaron los comentarios de los perfiles 2 y 4, en la Tabla 3.- Perfiles básicos de usuarios del Capítulo 3. POLÍTICAS DE USO ACEPTABLE DE LA RIUADY Se actualizó el Capítulo 4. SERVIDORES, pasando de 15 a 13 puntos. Se actualizó el Capítulo 5. ANTIVIRUS de 10 a 13 puntos. Se actualizó el Capítulo 6. ESQUEMA DE SEGURIDAD EN SERVIDORES. Se actualizó la tabla 4. Requisitos de Seguridad. Se eliminó ESTÁNDARES Y PROCEDIMIENTOS. Se actualizó el Capítulo 10. POLÍTICAS DE DEPENDENCIAS UNIVERSITARIAS Se cambió el punto 1 del Capítulo 11. ADMINISTRADOR DE TECNOLOGÍAS DE INFORMACIÓN Se eliminaron los requisitos para ser ATI Se eliminó la Figura 13.- Organigrama de las Tecnologías de Información en una DES Se actualizó el Capítulo 12. POLÍTICAS PARA USUARIOS. Pasando de 15 a 21 puntos. Se actualizó el capítulo 14. POLÍTICAS DE CORREO INSTITUCIONAL	

		Se actualizó el capítulo 15. POLÍTICAS DE DIRECTORIO ACTIVO (INET) Se eliminó el punto 3 en DE COMPUTADORAS. Se eliminó el punto 4 en DE CUENTAS DE USUARIOS INET Se eliminó el capítulo 16. Políticas de uso de internet académico Cambio de siglas a la CGTIC	

Nota: Ésta sección será utilizada a partir de la primera modificación a este documento. La revisión 00, se mantendrá en blanco.

Revisó	**Aprobó**
MATI. Israel Novelo Zel *Coordinador de Infraestructura Tecnológica de la CGTIC*	*MT Sergio Antonio Cervera Loeza* *Coordinador General de Tecnologías de la Información y Comunicación*