CUDI-CDR
RFCMX 2
Categoría: Especificaciones
Grupo de Seguridad

Febrero-2003
M. Farias-Elinos (ULSA)
Ma. C. Mendoza (CICESE)
A. Fernandez (UNAM)
M.A. Balderas (UAT)
M. De la Cruz (IPN)
C. A. Altamirano (UNAM)
J. Castillo (CELANESE)

Políticas generales para el uso adecuado de la RedCUDI

Resumen

En este documento se describen los lineamientos para el uso adecuado de los recursos y servicios a los que se tiene derecho en RedCUDI. Todos los miembros conectados a esta red deberán conocer y respetar estas políticas con el fin de tener un funcionamiento saludable de la red. Estos lineamientos se dividen en los derechos, las responsabilidades y las sanciones para todas aquellas entidades miembros de CUDI y que tienen que ver con el desarrollo y uso de la Internet-2 en México (RedCUDI).

Palabras clave: Uso adecuado de RedCUDI, Internet-2 México, Políticas de uso de la red

Derecho de copia
Copyright © CUDI-CDR-Grupo de Seguridad (2003). Todos los derechos reservados. La distribución de este memo no está limitada.

Tabla de Contenido

1. Introducción 1
2. Derechos 2
3. Obligaciones (Responsabilidades) 2
4. Sanciones 4
5. Datos autores 5

1.Introducción

El propósito de RedCUDI es ser una red de alta capacidad con la cual se apoya la educación y a la investigación que se desempeña en las Universidades y Centros de Investigación del país. Por tal motivo se definen los siguientes derechos, obligaciones, responsabilidades y sanciones que componen una política[1,2] para regular el uso de la red con el fin de mantener un funcionamiento saludable de la RedCUDI que está conformada por los enlaces de la dorsal, los GigaPOP's, enlaces que van del punto de presencia hacia el asociado y los enlaces que van del asociado hacia el afiliado.

Durante el documento se utilizarán los términos de asociado y afiliado para denotar al asociado académico y al afiliado académico respectivamente; así mismo al hablar de grupos de trabajo se incluye a cada uno de los grupos de trabajo que existen en cada uno de los comités que conforman a CUDI. El asociado institucional se referirá como tal[3].

RedCUDI ofrece recursos y servicios que deben estar disponibles la mayor parte del tiempo, para ello es necesario que se cumplan los lineamientos que aquí se presentan, por lo cual el NOC-I2 y el grupo de seguridad se reservan el derecho de tomar acciones preventivas y/o correctivas para mantener el buen desempeño de la dorsal de RedCUDI.

2.Derechos

Art 1. Tendrán acceso a todos los recursos y servicios de la RedCUDI a que tengan derecho todos aquellos asociados y afiliados del ámbito académico y de investigación miembros de CUDI.

Art 2. Serán nodos de acceso a la dorsal de la RedCUDI todos los asociados académicos, además de aquellos asociados institucionales dedicados al ámbito de las telecomunicaciones.

Art 3. Tanto los asociados como afiliados podrán desarrollar aplicaciones para hacer uso de la Internet-2, siempre y cuando se apeguen a las regulaciones y recomendaciones que generen los grupos de trabajo.

Art 4. Los asociados y afiliados podrán anunciar las redes que requieran apegándose a las políticas de ruteo dictadas por el NOC de Internet 2 y/o el grupo de enrutamiento.

3.Obligaciones (Responsabilidades)

Art 5. Los administradores de la red local de los asociados y afiliados son responsables de las actividades que sucedan en su red.

Art 6. El tráfico generado por los asociados y afiliados será de carácter estrictamente académico y de investigación, queda fuera de la clasificación de investigación, aquellas actividades que involucren pruebas y/o búsqueda de vulnerabilidades, así como las actividades relativas, sin el visto bueno del Grupo de Seguridad de CUDI.

Art 7. Los asociados académicos podrán dar acceso a cualquier afiliado que solicite dicho servicio, en base a los lineamientos técnicos establecidos por el Comité de Desarrollo de la Red (CDR).

Art 8. Los asociados institucionales que den acceso a algún afiliado no podrán hacer uso de la RedCUDI, solamente servirán de puente entre los afiliados y la dorsal de RedCUDI

Art 9. Los asociados deberán contar con una figura denominada “oficial de seguridad”, el cual será nombrado oficialmente ante CUDI, quien será responsable de todo lo referente a la seguridad y miembro activo del grupo de seguridad, además de ser el punto de primer contacto y apoyo para los socios afiliados conectados, en lo referente a seguridad de la red.

Art 10. En el caso de los afiliados es recomendable la figura del "oficial de seguridad", el cual será nombrado oficialmente ante CUDI, quien también será miembro activo del grupo de seguridad, o en su defecto una persona responsable y punto de primer contacto para cualquier cuestión que se presente.

Art 11. Todos los grupos de trabajo de los diversos comités de CUDI deberán de publicar información con carácter de RFCMX, aquellas recomendaciones y especificaciones que sean necesarias para el aprovechamiento óptimo de la RedCUDI, cada vez que sea necesario y/o exista algún cambio importante en la red.

Art 12. Todo miembro de CUDI deberá apegarse a las recomendaciones que generen los grupos de trabajo, tanto en la parte técnica como en la parte de aplicaciones que se publiquen en los RFCMX's.

Art 13. Todo miembro deberá seguir las metodologías y los estándares internacionales recomendados por los grupos de trabajo de CUDI para el desarrollo de la Internet-2 en México, tanto en la parte de telecomunicaciones como de aplicaciones.

Art 14. Todo contenido de cualquier servicio que esté en la red de los asociados y afiliados que sean accesibles por Internet-2, deberán contener solamente información relacionada con sus actividades educativas y de investigación, actualizadas y con información fidedigna.

Art 15. Todo asociado y afiliado deberá tener un esquema de políticas propias para el control de sus usuarios y recursos, sobre todo aquellos que tenga acceso y/o sean accesibles por Internet-2; de tal manera que garanticen la protección de la información y recursos de su red interna contra modificaciones, acceso y/o destrucción no autorizada.

Art 16. Las políticas internas que tengan los asociados y afiliados no deberán de contraponerse, oponerse o eliminar las políticas de RedCUDI

Art 17. La administración de la infraestructura que conforma la dorsal de RedCUDI es responsabilidad de CUDI a través del NOC de Internet-2.

Art 18. Tanto el afiliado, como el asociado que le brinde conexión a la RedCUDI deberán de respetar mutuamente su privacidad.

Art 19. Todos los asociados y afiliados deberán respetar la integridad de los sistemas que componen la dorsal de la RedCUDI. Está prohibido infiltrarse a los equipos, como ruteadores y sistemas de cómputo que se instalen en la dorsal, de manera indebida y que puedan ocasionar conflictos (solicitudes de SNMP, etc.).

Art 20. RedCUDI no debe ser utilizada para la violación de sistemas de cómputo y equipos de telecomunicaciones ubicados en redes de los mismos asociados y afiliados, ni aquellos equipos que pertenezcan a otras redes internas y externas al país.

Art 21. RedCUDI no debe de utilizarse para distribuir información dañina, como virus, caballos de Troya o cualquier otro código malicioso; o información que

atente contra las leyes federales y estatales del país o cualquier tratado o acuerdo establecido con otros países, siempre y cuando dichos tratados sean de carácter académico e investigación.

Art 22. Los asociados y afiliados están obligados a difundir las políticas de seguridad de RedCUDI entre los usuarios y administradores de su red.

Art 23. Toda sospecha de ataque que sea detectada por algún asociado y/o afiliado de origen externo a sus redes deberá de reportarla al mail abuse@cudi.edu.mx.

Art 24. Los asociados y afiliados deberán de promover la capacitación del personal técnico y en especial del "oficial de seguridad", con el fin de disminuir los problemas de seguridad en RedCUDI, y como medio de tener respuesta inmediata a los problemas que se presenten.

Art 25. Los asociados y afiliados deberán tener restringido el acceso, tanto físico como lógico y de forma adecuada, de al menos a los equipos frontera de su red con RedCUDI.

4.Sanciones

Art 26. En caso de presentarse algún incidente en la red de algún afiliado que afecte al funcionamiento y/o comprometa la RedCUDI, el asociado podrá realizar la desconexión temporal del servicio hacia el afiliado en forma inmediata hasta que el problema quede resuelto y con el visto bueno del grupo de seguridad.

Art 27. En caso de presentarse algún incidente en la red de algún asociado que afecte al funcionamiento de la RedCUDI, el NOC podrá realizar la desconexión temporal del servicio hacia el asociado en forma inmediata hasta que el problema quede resuelto y con el visto bueno del grupo de seguridad.

Art 28. En caso de que algún asociado incumpla con sus actividades de seguridad, el grupo de seguridad con apoyo del NOC podrá restringir el servicio de RedCUDI hasta que se de una solución al incumplimiento.

Art 29. En caso de que algún afiliado incumpla con sus actividades de seguridad el oficial de seguridad del asociado correspondiente con el apoyo y recomendaciones de otros integrantes del grupo de seguridad podrá restringir el servicio de RedCUDI hasta que se de una solución al incumplimiento.

Art 30. Cuando se detecte algún uso inapropiado de la RedCUDI o acciones que atenten contra las regulaciones que se emitan en los RFCMX, el grupo de seguridad y el NOC de RedCUDI se reservan tomar las medidas pertinentes al respecto como por ejemplo: la desconexión lógica del asociado o afiliado.

Art 31. Todo problema de seguridad que se genere y no se contemple en este o en algún documento futuro quedará en manos del grupo de seguridad quien podrá apoyarse en algún grupo de trabajo y/o comité de CUDI para buscar alguna solución posible.

5.Datos autores

Mario Farias-Elinos
Universidad La Salle (ULSA)
Escuela de Ingeniería / Dirección de Posgrado e Investigación
Benjamín Franklin 47
Col. Hipódromo Condesa
México, DF, 06140
Tel: (55) 5278-9530
Fax: (55) 5515-7631
e-mail: elinos@ci.ulsa.mx

María Concepción Mendoza
Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE)
Km. 107, Carretera Tijuana-Ensenada
Ensenada, BCN, 22860
e-mail: m.c@losdominguezmendoza.org

Azael Fernández Alcántara
Universidad Nacional Autónoma de México (UNAM)
Dirección General de Servicios de Cómputo Académico (DGSCA)
Laboratorio de Tecnologías Emergentes de Redes (NETLab)
Circuito Exterior S/N, C.U.
México, DF, 04510
Tel: (55) 5622-8857
Fax: (55) 5622-8588
e-mail: azael@redes.unam.mx

Marco A. Balderas
Universidad Autónoma de Tamaulipas (UAT)
Centro Universitario Adolfo López Mateos
Cd. Victoria, Tamaulipas, 87040
Tel: () 348-1700
Fax: () 348-1701
e-mail: workn@mail.ru

Manuel De la Cruz Cruz
Instituto Politécnico Nacional (IPN)
Dirección de Telemática
Edif. Inteligente, Unidad Prof. Adolfo López Mateos, Zacatenco
Mexico, DF.
Tel: (55) 5729-6000 x 51424, 51430
Fax: (55) 8329-4083
e-mail: mdelacruz@ipn.mx

Carlos A. Vicente Altamirano
Universidad Nacional Autónoma de México (UNAM)
Dirección General de Servicios de Cómputo Académico (DGSCA)
Centro de Operación de la Red
Circuito Exterior S/N, C.U.
México, DF, 04510
Tel: (55) 5622-8526
e-mail: carlos@antares.noc.unam.mx

Juan Gariel Castillo Martínez
CELANESE
México, DF
e-mail: jcastillo@celanese.com.mx

Referencias

[1] Fraser, B., Ed., "Sites Security Handbook", FYI 8, RFC 2196, Septiembre 1997
[2] "Information technology – Code of practice for information security management", ISO/IEC 17799:2000, 2000

[3] Acta de la Asamblea Constitutiva de Corporación Universitaria para el Desarrollo de Internet, Asociación Civil. http://www.cudi.edu.mx/members/acta_final.pdf, Marzo 1999