

LINEAMIENTOS PARA LA CREACIÓN DE EQUIPOS DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT)

La XIX Reunión del Comité Consultivo Permanente I: Telecomunicaciones/ Tecnologías de la Información y la Comunicación (CCP.I),

CONSIDERANDO:

- a) Que en la Resolución AG/RES. 2681 (XLI-O/11) “Ampliación del Acceso a las Telecomunicaciones y las Tecnologías de la Información y la Comunicación por medio del Fortalecimiento de la Comisión Interamericana de Telecomunicaciones”, párrafo operativo 1, en su primer resuelve se señala que se debe reiterar a la CITEI a que continúe colaborando estrechamente con los Estados Miembros para el intercambio de prácticas óptimas de políticas, tecnologías y estrategias nacionales de las telecomunicaciones y las tecnologías de la información y la comunicación (telecomunicaciones/TIC), y que se promueva aún más la utilización de todos los medios apropiados para atender a las áreas rurales, aisladas e insuficientemente atendidas;
- b) Que es mandato del Grupo de Trabajo sobre Despliegue de Tecnologías y Servicios del Comité Consultivo Permanente I: Telecomunicaciones/TIC producir y recomendar metodologías y mejores prácticas para la ciberseguridad;
- c) Que la confianza y seguridad en la utilización de las telecomunicaciones/TIC son de gran importancia para la integración de la Sociedad de la Información y del Conocimiento, por lo que los países de la región, particularmente los países en desarrollo, requieren un constante intercambio de experiencias y mejores prácticas para la creación de políticas nacionales, regionales e internacionales en temas como la ciberseguridad;
- d) Que es necesario fortalecer la difusión y conocimiento de la cuestión de Seguridad Informática y la atención a ésta en los distintos países de América Latina y el Caribe, especialmente en el ámbito privado de las empresas y organizaciones de la sociedad civil; y
- e) Que se requieren lineamientos para la creación de Equipos de Respuesta a Incidentes de Seguridad Informática en las organizaciones (empresas, instituciones, etc.) de los diferentes sectores productivos de cualquier país, incluidas las entidades estatales,

RECONOCIENDO:

- a) Que en la Resolución 58 (Johannesburgo,2008) “Fomento de la creación de equipos nacionales de intervención en caso de incidente informático, especialmente para los países en desarrollo” de la Asamblea Mundial de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones se invita a los Estados Miembros a considerar la posibilidad de crear Equipos de Intervención en caso de Incidente Informático (CSIRT) con carácter de alta prioridad;
- b) Que en la Resolución 69 (Hyderabad, 2010) “Creación de equipos nacionales de intervención en caso de incidente informático, especialmente para los países en desarrollo, y cooperación entre los

¹ CCP.I-TIC/doc.2482/11

mismos” de la Conferencia Mundial de Desarrollo de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones se invita a los Estados Miembros a crear CIRT nacionales cuando sea necesario;

c) Que el Comité Interamericano Contra el Terrorismo (CICTE) de la Organización de los Estados Americanos cuenta con un programa de “Seguridad Cibernética” cuyo objetivo es ayudar a los Estados Miembros en el establecimiento de un equipo nacional de "alerta, vigilancia y advertencia", también conocidos como Equipos de Respuesta a Incidentes de Seguridad Cibernética (CSIRT),

TENIENDO EN CUENTA:

a) Que es necesario continuar fortaleciendo los mecanismos bilaterales, subregionales, regionales e internacionales de cooperación, en conformidad con los principios establecidos en la Carta de la OEA, a fin de enfrentar, prevenir y combatir de manera integral y efectiva la delincuencia organizada transnacional, la trata de personas, el terrorismo, el secuestro, las pandillas delictivas y los delitos relacionados con el uso de tecnologías, incluido el delito cibernético, por cuanto éstos pueden afectar, en algunos casos, el desarrollo social, económico, político y el orden jurídico e institucional;

b) Que la creciente digitalización de la economía y de la sociedad traen aparejados desafíos significativos. El correo basura (*spam*), el acceso indebido a datos confidenciales y el robo son algunos de los perjuicios que criminales y terroristas causan a organizaciones e instituciones, particularmente a las de países sin capacidad institucional para protegerse;

c) Que para contrarrestar esos problemas, uno de los mecanismos más utilizados consiste en contar con un grupo en la empresa, el servicio y/o el país que tenga la capacidad para enfrentar los incidentes de seguridad de las redes,

RECOMIENDA:

1. Que los Estados Miembros tomen nota de la necesidad urgente de establecer equipos de Respuesta a Incidentes de Seguridad Informática como elemento necesario para que promover la confianza y seguridad en la utilización de las Telecomunicaciones/TIC como una de las bases para la creación de la Sociedad de la Información y del Conocimiento.

2. Que los Estados Miembros utilicen los instrumentos de política pública a su alcance para impulsar la creación de dichos equipos, siguiendo las recomendaciones específicas para su implementación y entrada en servicio.

3. Que las Administraciones difundan a diversos niveles (empresa, servicio y/o país) información relacionada con la necesidad de crear Equipos de Respuesta a Incidentes de Seguridad Informática como instrumento necesario para responder a tales incidentes.

4. Que los Estados Miembros de la CITEL consideren tener en cuenta la siguiente documentación al establecer los CSIRT nacionales:

- El documento del CCP.I (CCP.I-TIC/doc.-2342/11) recientemente finalizado sobre “Mejores prácticas para la seguridad cibernética nacional: creación de una capacidad nacional de respuesta a incidentes de seguridad informática”;
- Los tres estudios de casos nacionales (Argentina, República Dominicana, Venezuela) que figuran en los Capítulos 1-3 del Apéndice 2 de la Carpeta Técnica 4 “Seguridad cibernética”;
- El estudio de caso procedente de México (CCP.I-TIC/doc.2334/11), “Lineamientos para

la formación de equipos de respuesta a incidentes de seguridad informática (CSIRT) - (se añadirá como Capítulo 4 del Apéndice 2 de la Carpeta Técnica 4 “Seguridad cibernética”).

ENCARGA A LA SECRETARÍA DE LA CITEL:

Que envíe la presente Recomendación a los Estados Miembros de la CITEL y a la Secretaría del CICTE para su información.