DIRECTRIZ

Directriz N° 064 -MICITT

EL PRESIDENTE DE LA REPÚBLICA Y

EL MINISTRO DE CIENCIA, TECNOLOGÍA Y TELECOMUNICACIONES

Con fundamento en las atribuciones que les confieren los artículos 140 incisos 3), 8), 18) y 20), y 146 de la "Constitución Política de la República de Costa Rica", emitida en fecha 7 de noviembre de 1949 y publicada en la Colección de Leyes y Decretos del Año: 1949, Semestre: 2, Tomo: 2, Página: 724 y sus reformas; los artículos 11, 16 inciso 1), 21, 25 inciso 1), 27 inciso 1), 28 inciso 2 subincisos a) y b), 240 inciso 1) y 361 inciso 3) de la Ley N° 6227, "Ley General de la Administración Pública", emitida en fecha 2 de mayo de 1978 y publicada en el Diario Oficial La Gaceta N° 102, Alcance N° 90, de fecha 30 de mayo de 1978 y sus reformas; el artículo 3, 4, 11, 20, 21 de la Ley N° 7169, "Ley de Promoción del Desarrollo Científico y Tecnológico y Creación del MICYT (Ministerio de Ciencia y Tecnología)", emitida en fecha 26 de junio de 1990 y publicada en el Diario Oficial La Gaceta N° 144, Alcance N° 23, de fecha 1 de agosto de 1990 y sus reformas; los artículos 1, 2, 3 y 6 de la Ley N° 8642, "Ley General de Telecomunicaciones", emitida en fecha 4 de junio de 2008 y publicada en el Diario Oficial La Gaceta N° 125 de fecha 30 de junio de 2008 y sus reformas; y en razón de lo dispuesto en los artículos 39 y 40 de la Ley N° 8660, "Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones", emitida en fecha 8 de agosto de 2008 y publicada en el Diario Oficial La Gaceta N° 156, Alcance N° 31, de fecha 13 de agosto de 2008 y sus reformas; la Directriz

N° 049-MICITT, "Define fecha límite para la implementación del Protocolo de Internet IPv6 en el Sector Público Costarricense," emitida en fecha 4 de marzo de 2013 y publicada en el Diario Oficial La Gaceta N° 98 de fecha 23 de mayo de 2013; el artículo 11 inciso d) del Decreto Ejecutivo N° 41187-MP-PLAN, "Reglamento Orgánico del Poder Ejecutivo", emitido en fecha 20 de junio de 2018 y publicado en el Diario Oficial La Gaceta N° 111, Alcance N° 121 de fecha 21 de junio de 2018 y el Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021 "Costa Rica: una sociedad conectada", emitido en fecha 5 de octubre de 2015.

CONSIDERANDO:

I. Que el artículo 11 de la Ley N° 7169, "Ley de Promoción del Desarrollo Científico y Tecnológico y Creación del MICYT (Ministerio de Ciencia y Tecnología)", emitida en fecha 26 de junio de 1990 y publicada en el Diario Oficial La Gaceta N° 144, Alcance N° 23 de fecha 1 de agosto de 1990, designó al Ministro de Ciencia, Tecnología y Telecomunicaciones como el Rector del Sistema Nacional de Ciencia y Tecnología.

II. Que el artículo 39 de la Ley N° 8660, "Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones", emitida en fecha 8 de agosto de 2008 y publicada en el Diario Oficial La Gaceta N° 156, Alcance N° 31, de fecha 13 de agosto de 2008, designó al Ministro de Ciencia, Tecnología y Telecomunicaciones como el Rector de las Telecomunicaciones, por lo que le

corresponde coordinar con fundamento en las políticas del Sector, la elaboración del Plan Nacional de Desarrollo de las Telecomunicaciones, así como formular las políticas para el uso y desarrollo de las telecomunicaciones; coordinar las políticas de desarrollo de las telecomunicaciones con otras políticas públicas destinadas a promover la sociedad de la información; y velar por que las políticas del Sector sean ejecutadas por las entidades públicas y privadas que participan en el Sector de Telecomunicaciones.

III. Que mediante el artículo 11 inciso d) del Decreto Ejecutivo N° 41187-MP-PLAN, "Reglamento Orgánico del Poder Ejecutivo", emitido en fecha 20 de junio de 2018 y publicado en el Diario Oficial La Gaceta N° 111, Alcance N° 121 de fecha 21 de junio de 2018, el Poder Ejecutivo estableció el Sector Ciencia, Tecnología, Telecomunicaciones y Gobernanza Digital y su rectoría a cargo del Ministro de Ciencia, Tecnología y Telecomunicaciones.

IV. Que el Poder Ejecutivo en el ejercicio de su potestad de dirección en materia de Gobierno, y el Ministerio de Ciencia, Tecnología y Telecomunicaciones como ente rector en materia de telecomunicaciones y gobernanza digital, debe procurar las medidas necesarias para aprovechar el alcance de su rectoría sobre el asunto público de la manera más eficiente y oportuna.

V. Que según el artículo 40 de la Ley N° 8660, el Plan Nacional de Desarrollo de las Telecomunicaciones es el instrumento de planificación y orientación general del Sector Telecomunicaciones y define las metas, los objetivos y las prioridades de éste.

VI. Que el Plan Nacional de Desarrollo de las Telecomunicaciones 2015-2021: "Costa Rica una sociedad conectada" establece dentro de las metas por desarrollar, a más tardar en el año 2021, el cumplimiento del *"100% del Proyecto de IPv6[1] y DNSSEC implementado en las Redes de Telecomunicaciones en los Ministerios del Gobierno Central"*.

VII. Que según lo establecido por la Corporación de Internet para la Asignación de Nombres y Números (del inglés *Internet Corporation for Assigned Names and Numbers*, ICANN), las Extensiones de Seguridad para el Sistema de Nombres de Dominio (del inglés *Domain Name System Security Extensions*, DNSSEC) corresponden a una tecnología que se ha desarrollado, entre otras cosas, para brindar protección contra ataques cibernéticos mediante la firma digital de los recursos numéricos y nombres, a fin de tener la seguridad de que son válidos.

VIII. Que mediante lo señalado por ICANN, la implementación integral de las DNSSEC permitirá asegurar que el usuario final se conecte al sitio web real, o a otro servicio, que corresponda a un nombre de dominio en particular.

---

[1] IPv6, acrónimo proveniente del inglés *Internet Protocol version 6*, o "Protocolo de Internet versión 6"

IX. Que el protocolo HTTPS (del inglés, *HyperText Transfer Protocol Secure* o Protocolo seguro de transferencia de hipertexto, en su traducción al español) protege la integridad y la confidencialidad de los datos de los usuarios entre sus computadoras y los sitios web, proporcionando protección frente a ataques cibernéticos tipo "*man-in-the-middle*" ("hombre en el medio", en su traducción al español), contribuyendo así a la confianza de los usuarios.

X. Que la infraestructura RPKI (del inglés, *Resource Public Key Infrastructure* o Infraestructura de clave pública de recursos, en su traducción al español) fue desarrollada para proporcionar un medio seguro que certifique la asignación de recursos numéricos de Internet, con el objetivo de tener un sistema de enrutamiento global seguro y que permita a su vez un Internet confiable en todo el mundo.

XI. Que los protocolos SPF (del inglés, *Sender Policy Framework,* o Marco de políticas del remitente, en su traducción al español, también conocido como Convenio de Remitentes), DKIM (del inglés, *DomainKeys Identified Mail* o Correo identificado con claves de dominio) y DMARC (del inglés, *Domain-based Message Authentication, Reporting & Conformance* o Autenticación de mensajes basada en dominio, informes y conformidad, en su traducción al español) permiten la autenticación del correo electrónico, ayudando a prevenir ataques cibernéticos tipo *phishing*.

XII. Que un nombre de dominio de Internet es el nombre que registran los usuarios de la red de Internet para identificar el sitio Web de una empresa o institución.

XIII. Que los nombres de dominio de las empresas o instituciones pueden registrarse dentro de los dominios de nivel superior geográfico denominados ccTLD, del inglés, "*country code top-level domain*" (dominio de nivel superior de código de país, en su traducción al español), tal como ".cr" para los dominios en Costa Rica; o es posible escoger entre los dominios de segundo nivel, especializados y limitados, si reúne determinadas condiciones, como el .go.cr reservado para las instituciones del Gobierno de Costa Rica.

XIV. Que según lo señalado por la Organización Mundial de la Propiedad Intelectual (OMPI) en su sitio web, los nombres de dominio han ido adquiriendo una importancia todavía mayor como identificadores comerciales, siendo que, las controversias se derivan en gran parte del problema de la ciberocupación indebida; es decir, el registro anticipado de marcas, en razón de que el sistema de registro de nombres de dominio funciona por un riguroso orden de solicitud y, por tanto, existe la posibilidad para un tercero de registrar nombres de marcas, personalidades, empresas e instituciones con las que no tiene relación alguna.

XV. Que de acuerdo con lo señalado por la OMPI en su sitio web, los ciberocupas en su calidad de titulares de los registros de nombres de dominio, suelen subastarlos o tratan de venderlos directamente a la compañía o a la persona interesada, a un precio muy

por encima del costo de registro. También pueden conservar el registro y aprovechar la popularidad de la persona o de la empresa con la que se asocia ese nombre de dominio para atraer clientes a sus propios sitios web.

XVI. Que resulta necesario proteger los nombres de dominio de Internet que corresponden a las instituciones públicas del Estado Costarricense de los ciberocupas, mediante el registro dentro del dominio de nivel superior geográfico ".cr" y el dominio de segundo nivel ".go.cr".

XVII. Que según el último reporte realizado por el Registro de Direcciones de Internet para Latinoamérica y el Caribe, del inglés *Latin American and Caribbean Internet Addresses* (LACNIC) y publicado en su sitio web, la región actualmente se encuentra en la fase 3 de agotamiento de direcciones IPv4; en esta etapa de reserva, las asignaciones de direcciones IPv4 son restringidas en tamaño y periodicidad, por lo que eventualmente LACNIC no va a tener suficientes direcciones para cubrir las necesidades de direccionamiento IPv4 para sus miembros, incluyendo a Costa Rica.

XVIII. Que la Directriz N° 049-MICITT denominada *"Define fecha límite para la implementación del Protocolo de Internet IPv6 en el Sector Público Costarricense."* emitida en fecha 4 de marzo de 2013 y publicada en el Diario Oficial La Gaceta N° 98 de fecha 23 de mayo de 2013, dispuso como fecha límite para concluir la implementación del Protocolo IPv6 para las instituciones del Estado, el 30 de junio de 2015, a fin de que los usuarios puedan acceder a los servicios que por medio de

Internet presten las instituciones y que todas las entidades puedan, asimismo, brindar sus servicios por medio del Protocolo IPv6.

XIX. Que, según los datos obtenidos por el Viceministerio de Telecomunicaciones al 22 de noviembre de 2018, únicamente el 38,9 % de los ministerios del Gobierno Central mantienen sus sitios web disponibles en IPv6. Esta baja adopción limita el crecimiento de Internet, pues las direcciones de IP son recursos esenciales para su evolución y funcionamiento, así como del desarrollo de las economías digitales.

XX. Que según lo señalado por la Sociedad de Internet (del inglés, *Internet Society*, ISOC) las infraestructuras nacionales que utilizan IPv6 están mejor equipadas para apoyar las oportunidades económicas y la innovación en áreas tales como el Internet de las cosas, las redes inteligentes, la infraestructura y los edificios inteligentes.

XXI. Que es de interés público para el Gobierno de la República emitir la siguiente Directriz, con el objetivo de que se habiliten las tecnologías DNSSEC, RPKI, HTTPS, SPF, DKIM, DMARC y continúe el proceso de implementación de IPv6 en las entidades públicas, a fin de preservar la confianza de los usuarios que acceden a los sitios web y redes gubernamentales, así como, garantizar el acceso mediante el Protocolo IPv6.

POR TANTO,

EMITEN LA SIGUIENTE DIRECTRIZ DIRIGIDA A AL PODER EJECUTIVO:

"LINEAMIENTOS PARA EL FORTALECIMIENTO Y LA ESCALABILIDAD DE LA INFRAESTRUCTURA DE RED EN EL SECTOR PÚBLICO COSTARRICENSE"

Artículo 1°.- Objeto

El objeto de esta Directriz es fortalecer y permitir la escalabilidad de la infraestructura de red en el sector público costarricense, así como, contribuir al establecimiento de conexiones seguras, mediante la implementación de las medidas indicadas en los artículos 4 y 5 de la presente norma.

Artículo 2°.- Ámbito de Aplicación

Esta Directriz es de acatamiento obligatorio para el Poder Ejecutivo. Asimismo, se insta al Sector Público Descentralizado que en la medida de sus posibilidades adopte lo establecido en esta Directriz.

Artículo 3°. - Acrónimos y Definiciones

Para los efectos de esta Directriz, se define lo siguiente:

1. **DKIM:** Del inglés *DomainKeys Identified Mail* - Correo con Identificación por *DomainKeys* o Claves de Dominio. Es un método de autenticación de correo electrónico, que permite a una organización responsabilizarse del envío de un mensaje, de manera que éste pueda ser validado por un destinatario.
2. **DMARC:** Del inglés *Domain-based Message Authentication, Reporting & Conformance* - Autenticación de Mensajes basada en Dominio, Informes y Conformidad. Es un protocolo de autenticación, política y reporte de correo electrónico. Provee un mecanismo escalable mediante el cual una organización de origen de correo puede expresar políticas y preferencias a nivel de dominio para la validación, disposición e informe de mensajes, que una organización de recepción de correo puede usar para mejorar el manejo del correo.
3. **DNS:** Del inglés *Domain Name System* - Sistema de Nombres de Dominio. Es un sistema que se utiliza para resolver nombres de Internet en direcciones IP, mediante un protocolo simple de solicitud-respuesta.
4. **DNSSEC:** Del inglés *Domain Name System Security Extensions* - Extensiones de Seguridad para el Sistema de Nombres de Dominio. Proporciona autenticación de origen y protección de integridad para los datos DNS, así como un medio de distribución de clave pública. Estas extensiones no proporcionan confidencialidad.
5. **Dominio de primer nivel geográfico ccTLD:** Del inglés *Country Code Top-Level Domain*, son dominios de Internet correspondientes a códigos de países, por ejemplo, .cr para Costa Rica. La administración de los ccTLD se lleva a cabo de forma independiente e incumbe a las autoridades de registro designadas en el ámbito nacional.

6. **HTTPS:** Del inglés *HyperText Transfer Protocol Secure* - Protocolo Seguro de Transferencia de Hipertexto. Es un protocolo de capa de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto.
7. **ICANN:** Del inglés *Internet Corporation for Assigned Names and Numbers* - Corporación de Internet para la Asignación de Nombres y Números. Es una organización sin fines de lucro, cuyo objetivo es asegurar que Internet sea segura, estable e interoperativa. Esta asociación además promueve la competencia y desarrolla políticas de identificadores únicos de Internet.
8. **IP:** Del inglés *Internet Protocol* - Protocolo de Internet. Corresponde a un protocolo de la capa de red que define el mecanismo de direccionamiento en Internet para permitir la transmisión de datos.
9. **IPv4:** Versión 4 del Protocolo de Internet.
10. **IPv6:** Versión 6 del Protocolo de Internet.
11. **ISOC:** Del inglés *Internet Society* – Sociedad de Internet. Es una organización global sin fines de lucro, dedicada a asegurar que Internet siga siendo abierta, transparente y definida para que todos puedan disfrutar de esta.
12. **MICITT:** Ministerio de Ciencia, Tecnología y Telecomunicaciones.
13. **Nombre de dominio de Internet:** es el nombre que permite identificar el sitio Web de una empresa o institución.
14. **RPKI**: Del inglés *Resource Public Key Infrastructure* - Infraestructura de Clave Pública de Recursos. Es un marco especializado de infraestructura de clave pública, diseñado para proteger la infraestructura de enrutamiento de Internet. Proporciona

una manera de conectar información de recursos de números de Internet (como números de sistemas autónomos y direcciones IP) a un ancla de confianza.

15. **SPF**: Del inglés *Sender Policy Framework* - Convenio de Remitentes. Es un protocolo de autenticación de correo electrónico que verifica que un mensaje de correo electrónico es remitido desde una dirección IP autorizada.

Artículo 4°.– Implementación de tecnologías

Los jerarcas de las entidades que conforman el Poder Ejecutivo deberán girar las instrucciones al Departamento competente, con el fin de que, a más tardar el 31 de diciembre de 2021, se dé la implementación o uso de lo siguiente:

a) Las Extensiones de Seguridad DNSSEC en los servidores DNS institucionales.
b) Los Protocolos SPF, DKIM y DMARC en los servidores de correo electrónico.
c) El Protocolo HTTPS en el sitio web institucional.
d) El sistema RPKI para la validación de recursos de Internet o en su defecto solicitar al Proveedor de Servicios de Internet su uso.
e) El Protocolo de Internet IPv6 en la red institucional.
f) El Registro de Nombres de Dominio de Internet.

Artículo 5°. – Registro de Nombres de Dominios de Internet

Con el fin de evitar un uso indebido de los nombres de dominio de Internet en el Estado costarricense, se ordena el registro de los dominios dentro de las extensiones .cr y .go.cr. En el caso de los ministerios se debe implementar de la siguiente forma:

Institución	**Dominio.cr**	**Dominio.go.cr**
Ministerio de Agricultura y Ganadería	mag.cr	mag.go.cr
Ministerio de Ambiente y Energía	minae.cr	minae.go.cr
Ministerio de Ciencia, Tecnología y Telecomunicaciones	micitt.cr	micitt.go.cr
Ministerio de Condición de la Mujer	inamu.cr	inamu.go.cr
Ministerio de Comercio Exterior	comex.cr	comex.go.cr
Ministerio de Cultura y Juventud	mcj.cr	mcj.go.cr
Ministerio de Deportes y Recreación	icoder.cr	icoder.go.cr
Ministerio de Economía, Industria y Comercio	meic.cr	meic.go.cr
Ministerio de Educación Pública	mep.cr	mep.go.cr
Ministerio de Gobernación y Policía	mgp.cr	mgp.go.cr
Ministerio de Hacienda	hacienda.cr	hacienda.go.cr
Ministerio de Justicia y Paz	mjp.cr	mjp.go.cr
Ministerio de Obras Públicas y Transportes	mopt.cr	mopt.go.cr
Ministerio de Planificación Nacional y Política Económica	mideplan.cr	mideplan.go.cr
Ministerio de la Presidencia	presidencia.cr	presidencia.go.cr

Ministerio de Relaciones Exteriores y Culto	rree.cr	rree.go.cr
Ministerio de Salud	ministeriodesalud.cr	ministeriodesalud.go.cr
Ministerio de Seguridad Pública	seguridadpublica.cr	seguridadpublica.go.cr
Ministerio de Trabajo y Seguridad Social	mtss.cr	mtss.go.cr
Ministerio de Turismo	ict.cr	ict.go.cr
Ministerio de Vivienda y Asentamientos Humanos	mivah.cr	mivah.go.cr

Las instituciones deberán tomar las previsiones necesarias para la aplicación de esta medida ante la creación, fusión o modificación de instituciones pertenecientes al Poder Ejecutivo y/o modificaciones del nombre de dominio de una institución existente.

Artículo 6°.- Proceso de Verificación de Cumplimiento

Para verificar el cumplimiento de la implementación de la Directriz, el MICITT realizará anualmente un informe de los resultados de la implementación, el cual será publicado en el sitio web del MICITT.

Artículo 7°. – Implementación por parte de otras instituciones.

Se insta a los jerarcas del Poder Legislativo, Poder Judicial, el Tribunal Supremo de Elecciones, las instituciones autónomas, las semiautónomas, municipalidades y concejos

municipales, las empresas públicas, y entes públicos no estatales a considerar la implementación de lo dispuesto en la presente directriz.

Artículo 8°.- Vigencia.

Rige a partir de su publicación.

Dada en la Presidencia de la República. San José, a los seis días del mes de setiembre del año dos mil diecinueve.

CARLOS ALVARADO QUESADA

LUIS ADRIÁN SALAZAR SOLÍS

MINISTRO DE CIENCIA, TECNOLOGÍA Y TELECOMUNICACIONES

1 vez.—Solicitud N° 005-2019TEL.—O. C. N° 4600024703.—(IN2019410236).