DIRECTRIZ N° 133-MP-MICITT

EL PRESIDENTE DE LA REPÚBLICA,
LA MINISTRA DE LA PRESIDENCIA Y
LA MINISTRA DE CIENCIA, INNOVACION, TECNOLOGÍA Y TELECOMUNICACIONES

En uso de las facultades conferidas en los artículos 140 incisos 3) y 18) y 146 de la Constitución Política; artículos 25 inciso 1) y 28 inciso 2.b), 99 y 100 de la Ley N° 6227, "Ley General de la Administración Pública", publicada en el Alcance N° 90 al Diario Oficial La Gaceta N.º 102 del 30 de mayo de 1978; artículos 4 y 100 de la Ley N ° 7169, del 26 de junio de 1990, "Ley de Promoción del Desarrollo Científico y Tecnológico", publicada en el Alcance N° 23 al Diario Oficial La Gaceta N° 144 del 01 de agosto de 1990 y sus reformas; artículo 281 de la Ley 7594, del 10 de abril de 1996, "Código Procesal Penal", publicado en el Alcance N° 31 al Diario Oficial La Gaceta N° 106 del 04 de junio de 1996 y el Decreto N.º 37052-MICIT, del 9 de marzo del 2012, "Crea Centro de Respuesta de incidentes de Seguridad Informática CSIRT-CR", publicado en el Diario Oficial La Gaceta N.º 72 del 13 de abril del 2012.

Considerando:

1º-Que existe un conjunto de amenazas concretas derivadas del uso malicioso de las tecnologías digitales y de sus limitaciones y vulnerabilidades intrínsecas, cuyo fin último es lesionar la integridad individual en favor del crimen cibernético y que lleva al Estado a extender las nociones de derecho, jurisprudencia y soberanía hacia el espacio tecnológico para definir de manera integral el concepto de bienestar social.

2°- Que de conformidad con el artículo 1° del Decreto Ejecutivo número 37052-MICIT del 9 de marzo de 2012, el Estado costarricense cuenta con el Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) con sede en las instalaciones del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, con facultades suficientes para coordinar con los Poderes del Estado, instituciones autónomas, empresas y bancos del Estado todo lo relacionado con la materia de seguridad informática, el cual trabaja para prevenir y responder ante los incidentes de seguridad cibernética e informática que afecten a las instituciones gubernamentales.

3º-Que el Estado tiene como uno de sus objetivos fundamentales el aumentar el aprovechamiento de las oportunidades que brinda la ciencia y la tecnología para incrementar el nivel de desarrollo del país, incluyendo la protección del capital de información del país y de especial relevancia, la correspondiente a las personas ciudadanas, con el fin de garantizar las condiciones suficientes y necesarias para la competitividad.

4º-Que la Ley de Promoción del Desarrollo Científico y Tecnológico en su artículo 3º, inciso b), contempla como un deber y una responsabilidad del Estado: "*Apoyar la actividad científica, tecnológica y de innovación que realice cualquier entidad privada o pública, nacional o extranjera, que contribuya a la productividad, al intercambio científico y tecnológico con otros países, o que esté vinculada con los objetivos del desarrollo nacional. Asimismo, generar las políticas públicas que garanticen el derecho de los habitantes a obtener servicios de telecomunicaciones, así como asegurar la aplicación de los principios de universalidad y solidaridad del servicio de*

telecomunicaciones y fortalecer los mecanismos de universalidad y solidaridad de las telecomunicaciones, garantizando el acceso a los habitantes que lo requieran".

5º-Que el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones tiene como parte de sus obligaciones el apoyar los programas de transformación y modernización del sector estatal, así como establecer áreas temáticas estratégicas, dentro de las que se haya la formulación y ejecución de políticas y estrategias relacionadas con la seguridad en las Tecnologías de la Información y la Comunicación en el ámbito del Sector Público costarricense, con el objetivo de alcanzar mayores niveles de eficiencia en los servicios del Estado, y a la vez contribuir a crear una infraestructura de las tecnologías de la información y la comunicación que potencien al sector productivo nacional.

6º. Que el Poder Ejecutivo en el ejercicio de su potestad de dirección dentro de la Administración Pública, particularmente a través del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, como rector en materia de gobernanza digital, debe procurar las medidas necesarias para establecer las mejores prácticas y lineamientos en pro de mejorar la ciberseguridad nacional

Por tanto, emiten la siguiente:

DIRECTRIZ

" DIRIGIDA A LA ADMINISTRACIÓN PÚBLICA CENTRAL Y DESCENTRALIZADA SOBRE LAS MEJORAS EN MATERIA DE CIBERSEGURIDAD PARA EL SECTOR PÚBLICO DEL ESTADO "

Artículo 1 - Se instruye a la Administración Pública Central y se insta a la Administración Pública Descentralizada a cumplir las recomendaciones y medidas técnicas que emanen del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, por medio de la Dirección de Gobernanza Digital y el Centro de Respuesta de Incidentes de Seguridad Informática (en adelante CSIRT-CR), como ente coordinador de la ciberseguridad nacional, referentes a ciberseguridad y seguridad de la información, con el fin de mejorar las capacidades técnicas, de atención y de gestión de la ciberseguridad y seguridad de la información en las instituciones.

Artículo 2 - Se instruye a la Administración Pública Central y se insta a la Administración Pública Descentralizada a realizar los procesos internos para promover de manera inmediata las acciones que favorezcan la resiliencia de la infraestructura tecnológica, sea que la misma corresponda a la Administración Pública directamente o esté contratada de manera total o parcialmente, incluyendo como mínimo actualizaciones permanentes de todos los sistemas institucionales, cambiar contraseñas de todos los sistemas institucionales (correos electrónicos, sistemas operativos, servidores, VPN, redes sociales, entre otros posibles), deshabilitar servicios y puertos no necesarios y monitorear la infraestructura de red, con el fin de garantizar que los eventos adversos relacionados con incidentes de ciberseguridad sean detectados, registrados y gestionados de forma que se pueda limitar el impacto de los mismos en cada institución o entidad.

Artículo 3 - Se instruye a la Administración Pública Central y se insta a la Administración Pública Descentralizada a autorizar a los contactos de ciberseguridad, equipos de tecnologías de la información, Centro de Respuesta de Incidentes de Seguridad Informática (CSIRTs internos) o grupos que en sus efectos se hayan creado para atender la ciberseguridad institucional, para que asistan a las actividades de formación, capacitación, u otra actividad que organice el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, por medio de la Dirección de Gobernanza Digital y el CSIRT-CR, relacionada con la atención y mejora en las capacidades de ciberseguridad y seguridad de la información.

Artículo 4 - Se instruye a la Administración Pública Central y se insta a la Administración Pública Descentralizada a informar al Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) de Costa Rica sobre los incidentes que ocurran en sus instituciones que afecten la confidencialidad, disponibilidad e integridad de servicios disponibles al público, o la continuidad de las funciones institucionales, o la suplantación de identidad de la institución en redes sociales, incluso aquellos incidentes que a lo interno de la institución se consideren bajo control. Dichos incidentes se deberán informar a la dirección csirt@micit.go.cr proporcionando, al menos, los siguientes datos: nombre, vía de contacto, institución del estado afecta y descripción del problema. Adicionalmente, se instruye a la Administración Pública Central y se insta a la Administración Pública Descentralizada a respaldar la información referente al incidente acontencido, para las investigaciones correspondientes.az

Artículo 5 - Se instruye a la Administración Pública Central y se insta a la Administración Pública Descentralizada a informar al Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) al correo csirt@micit.go.cr, todo los dominios de sus sitios web en un plazo de 3 días hábiles a partir de la entrada en vigencia de la presente Directriz, esto con el fin de hacer un levantamiento de los sitios oficiales de las instituciones del Estado para generar y validar los sitios web oficiales de sus instituciones, para incluirlos dentro del validador de sitios oficiales de gobierno https://sitiosoficiales.gob.go.cr/, con la finalidad de prevenir las acciones de suplantación y phishing contra las instituciones del Estado que afecten a los usuarios. En caso de generar nuevos sitios oficiales de gobierno deberán ser reportados para incluirlos dentro del monitoreo de sitios web públicos que realiza el CSIRT-CR al validador de sitios oficiales de Gobierno. De igual forma a los sitios web reportados al CSIRT-CR se les realizará al menos dos veces al año, correspondiendo uno por semestre, un análisis de vulnerabilidades para emitir al contacto de ciberseguridad de cada institución un informe con las vulnerabilidades encontradas para que proceda a su atención; a partir de dicho informe, se intruye a la Administración Pública Central y se insta a la Administración Pública Descentralizada a realizar las correcciones y acciones correspondientes, de conformidad con el resultado de este análisis, para disminuir el riesgo de sus sitios web públicos.

Artículo 6 - Se instruye a la Administración Pública Central y se insta a la Administración Pública Descentralizada a que las alertas técnicas emitidas por el CSIRT-CR sean aplicadas, según corresponda en cada institución y sus sistemas, esto con el fin de disminuir las vulnerabilidades tecnológicas en las instituciones del país. Se instruye a la Administración Pública Central y se insta a la Administración Pública Descentralizada a valorar la alerta técnica recibida y realizar los procedimientos respectivos para poder aplicarla dentro de su institución.

Artículo 7 – La presente Directriz rige a partir del 21 de abril de 2022.

Dada en la Presidencia de la República, a los veintiún días del mes de abril del año dos mil veintidós.

CARLOS ANDRES ALVARADO QUESADA (FIRMA)

Firmado digitalmente por CARLOS ANDRES ALVARADO QUESADA (FIRMA)
Fecha: 2022.04.21 18:30:07 -06'00'

Carlos Alvarado Quesada

CARMEN GEANNINA DINARTE ROMERO (FIRMA)

Firmado digitalmente por CARMEN GEANNINA DINARTE ROMERO (FIRMA)
Fecha: 2022.04.21 17:58:52 -06'00'

Geannina Dinarte Romero
Ministra de la Presidencia

PAOLA VEGA CASTILLO (FIRMA)

Firmado digitalmente por PAOLA VEGA CASTILLO (FIRMA)
Nombre de reconocimiento (DN): serialNumber=CPF-01-0937-0493, sn=VEGA CASTILLO, givenName=PAOLA, c=CR, o=PERSONA FISICA, ou=CIUDADANO, cn=PAOLA VEGA CASTILLO (FIRMA)
Fecha: 2022.04.21 17:33:03 -06'00'

Paola Vega Castillo
Ministra de Ciencia, Innovación, Tecnología y Telecomunicaciones