

Promueven iniciativa público-privada para producir equipos e insumos de protección a personal de salud



Entidades públicas y privadas del sector de ciencia y tecnología harían parte de una iniciativa que busca soluciones que apoyen al Ministerio de Salud y a la CCSS en la producción de equipos e insumos de protección para personal de salud ante la emergencia COVID -19.

[Ver detalles](#)

Industria de Telecomunicaciones redobla esfuerzos para mantener servicios de Internet

Ante aumento de la demanda en Costa Rica, durante la emergencia nacional. Medidas enfocadas en atender necesidades de teletrabajo, información, trámites y entretenimiento. MICITT asegura que no se analiza regular el Internet, ni restringir contenido.

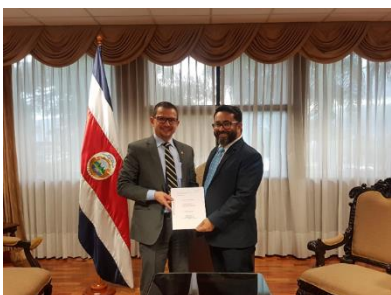
[Ver detalles](#)



MICITT informa sobre buenas prácticas del teletrabajo para laborar de forma segura desde su hogar

Ante la directriz y la alerta amarilla emitida por el Gobierno de la República por el coronavirus (COVID-19), se está impulsando para que las empresas públicas y privadas realicen teletrabajo para así evitar mayor propagación del virus.

[Ver detalles](#)



Reforma al Plan Nacional de Atribución de Frecuencias, habilita las comunicaciones con aviones, trenes y embarcaciones

Como parte de los esfuerzos que realiza el MICITT para mejorar los servicios de telecomunicaciones que se brindan en el país y que benefician a toda la población, se llevó a cabo la Reforma al Plan Nacional de Atribución de Frecuencias denominada “Banda Ka y Uso Libre”.

[Ver detalles](#)

OTRAS NOTICIAS

Costa Rica participa en encuentro mundial para buscar soluciones científicas y tecnológicas a COVID-19

El ministro de MICITT, Luis Adrián Salazar Solís, participó en el diálogo ministerial virtual junto a 79 ministros y 200 representantes de organismos internacionales, científicos y delegaciones convocados por la Directora General de UNESCO.

[Ver detalles](#)

MICITT alerta de estafas en nombre de la OMS

Si recibe un correo usando el nombre de la Organización Mundial de la Salud (OMS) tenga cuidado, podrían ser estafadores que están usando el nombre de la OMS para robar dinero y datos delicados.

[Ver detalles](#)

Sector de Telecomunicaciones se une para garantizar la continuidad de servicios ante Covid-19

En función de generar una mesa de trabajo en el área de las telecomunicaciones para la atención de la pandemia del COVID-19, el MICITT en su calidad de rector, convocó a esta Industria, con apoyo de la SUTEL en su calidad de regulador, a una reunión el pasado lunes 16 de marzo, para establecer acciones direccionadas a dar continuidad, mantenimiento y seguridad de servicios.

[Ver detalles](#)

Tigo completa devolución de frecuencias del espectro radioeléctrico

El MICITT y Tigo, firmaron un acuerdo mutuo para la devolución de seis frecuencias, necesarias para el ordenamiento y uso eficiente del espectro radioeléctrico, como parte de los esfuerzos del Poder Ejecutivo.

[Ver detalles](#)

CIENTÍFICA DESTACADA 2020

El Ministerio de Ciencia, Tecnología y Telecomunicaciones y la Academia Nacional de Ciencias invitan a la ciudadanía a postular los nombres de aquellas científicas STEM que consideren merecedoras del reconocimiento.

Criterios de elegibilidad

- Ser costarricense radicada en Costa Rica
- Realizar aportes al conocimiento y a la sociedad derivados de investigaciones
- Contar con publicaciones científicas
- No ser miembro de la ANC.

Debe incluir un breve motivo por el cual se considere que la candidata debe ser la Científica del año 2020.

Fecha límite de postulaciones:
12 de Julio
Al correo: anc@anc.cr

Mujeres dedicadas a la ciencia y tecnología pueden ser reconocidas como la Científica Destacada 2020

Con el objetivo reconocer la trayectoria de las mujeres y sus aportes al desarrollo costarricense en la generación y transmisión de conocimiento, se reconoce bianualmente a la Científica Destacada del Año y se invita a la ciudadanía a presentar sus postulaciones para la edición 2020.

[Ver detalles](#)












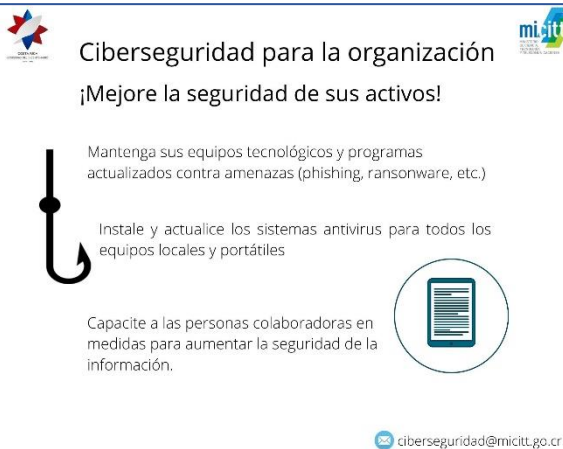





EN IMÁGENES

CIBERSEGURIDAD PARA EL TELETRABAJO

<h4>Ciberseguridad para la persona teletrabajadora</h4> <p>El teletrabajo es posible gracias a</p> <ul style="list-style-type: none">herramientas digitalesmensajería, aplicacionesla internetla nube <p>Esto nos permite mantener una conexión tecnológica por eso es importante....</p> <p> Ser más cautelosos</p> <p> Seguir actualizaciones de canales oficiales</p> <p> Tener higiene digital</p> <p>ciberseguridad@micitt.go.cr</p>	<h4>Ciberseguridad para la persona teletrabajadora</h4> <h3>¡Combata la desinformación!</h3> <p>Infórmese únicamente con fuentes oficiales de su organización.</p> <p></p> <p> No saturemos los medios de comunicación con reenvío de mensajes de dudosa autenticidad.</p> <p>Verifique la seguridad y privacidad del sitio donde se encuentra realizando teletrabajo, ya que estará usando información sensible.</p> <p></p> <p>➔ ¡Evite ser víctima de engaños!</p> <p>ciberseguridad@micitt.go.cr</p>
<h4>Ciberseguridad para la persona teletrabajadora</h4> <h3>Salud Digital</h3> <p> No utilizar accesos que no sabemos de donde vienen.</p> <p> Se debe tener y conocer el procedimiento ante un incidente de ciberseguridad.</p> <p> Utilizar al menos dos factores de autenticación en los equipos, eso brinda una mayor seguridad.</p> <p> En caso de dudas relacionadas con la parte tecnológica, consulta a los encargados de TI.</p> <p>ciberseguridad@micitt.go.cr</p>	<h4>Ciberseguridad para la organización</h4> <h3>¡Controle quién entra a su casa!</h3> <p>Implemente varios métodos de autenticación para el acceso a sus servicios (autenticación de múltiples factores)</p> <p>Implemente el uso de redes privadas virtuales (VPN) para acceso a los datos fuera del centro de trabajo.</p> <p> Ofrezca a las personas colaboradoras vías para obtener soporte técnico de la organización.</p> <p>ciberseguridad@micitt.go.cr</p>
<h4>Ciberseguridad para la persona teletrabajadora</h4> <h3>Higiene Digital</h3> <p> En caso de utilizar equipos personales, aunque no es lo más adecuado, solicitar ayuda de su organización para que lo preparen para el teletrabajo.</p> <p> Realizar los reportes pertinentes a los encargados de TI.</p> <p> No compartir información de dudosa procedencia, ya que los cibercriminales han creado noticias falsas.</p> <p> No utilizar la misma contraseña en todos los equipos.</p> <p>ciberseguridad@micitt.go.cr</p>	<h4>Ciberseguridad para la persona teletrabajadora</h4> <h3>¡Confidencialidad para su trabajo!</h3> <p> Utilice únicamente el correo institucional para la comunicación oficial y para sus labores.</p> <p> Establezca contraseñas robustas para evitar accesos no autorizados a los recursos de trabajo.</p> <p> No haga uso de correos personales para fines laborales, así evita amenazas a su seguridad.</p> <p>ciberseguridad@micitt.go.cr</p>

EN IMÁGENES

CIBERSEGURIDAD PARA EL TELETRABAJO

 <p>Ciberseguridad para la persona teletrabajadora</p> <p>Aumente su seguridad con las siguientes recomendaciones</p> <table border="0"><tr><td><p>Evite redes inalámbricas públicas, son inseguras porque exponen su equipo y la información en el.</p></td><td><p>Bloquea los equipos que utilizas para el teletrabajo si no los estas utilizando.</p></td><td><p>Mantén actualizado tu computador, teléfono o tableta, así como las aplicaciones que utilices.</p></td><td><p>Realiza respaldos periódicamente y conservalos en lugar seguro, así previenes la perdida de datos de trabajo.</p></td></tr></table> <p>ciberseguridad@micitt.go.cr</p>	 <p>Evite redes inalámbricas públicas, son inseguras porque exponen su equipo y la información en el.</p>	 <p>Bloquea los equipos que utilizas para el teletrabajo si no los estas utilizando.</p>	 <p>Mantén actualizado tu computador, teléfono o tableta, así como las aplicaciones que utilices.</p>	 <p>Realiza respaldos periódicamente y conservalos en lugar seguro, así previenes la perdida de datos de trabajo.</p>	 <p>Ciberseguridad para la organización</p> <p>¡Mejore la seguridad de sus activos!</p> <p>Mantenga sus equipos tecnológicos y programas actualizados contra amenazas (phishing, ransomware, etc.)</p> <p>Instale y actualice los sistemas antivirus para todos los equipos locales y portátiles</p> <p>Capacite a las personas colaboradoras en medidas para aumentar la seguridad de la información.</p>  <p>ciberseguridad@micitt.go.cr</p>
 <p>Evite redes inalámbricas públicas, son inseguras porque exponen su equipo y la información en el.</p>	 <p>Bloquea los equipos que utilizas para el teletrabajo si no los estas utilizando.</p>	 <p>Mantén actualizado tu computador, teléfono o tableta, así como las aplicaciones que utilices.</p>	 <p>Realiza respaldos periódicamente y conservalos en lugar seguro, así previenes la perdida de datos de trabajo.</p>		

Si requiere acceder a las infografías puede acceder en <https://micitt.go.cr/infografias-ciberseguridad-el-teletrabajador>