Los rectores de las universidades públicas y el ministro de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) anunciaron que trabajarán de manera conjunta con el Consejo Nacional de Rectores (CONARE) en temas de ciberseguridad.

# MICITT y CONARE unen esfuerzos en temas de ciberseguridad

27 de Junio 2022 Por: Redacción [1]

CSIRT-CR sigue vigilante ante alertas e incidentes a nivel nacional.

Universidades estatales se suman a los esfuerzos nacionales para atender emergencia de ciberseguridad.

Este lunes el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) anunció que trabajará de manera conjunta con el Consejo Nacional de Rectores (CONARE) y

las universidades estatales en temas de ciberseguridad.

La semana anterior se sostuvo una reunión entre el Ministro Carlos Enrique Alvarado Briceño y los rectores de las universidades estatales, donde el jerarca del MICITT solicitó al CONARE la posibilidad de colaborar con el fortalecimiento del CSIRT-CR mediante el conocimiento y las herramientas tecnológicas que disponen las universidades estatales para el control de los ciberataques.

“Nos interesa muchísimo trabajar con las universidades estatales este tipo de iniciativas conjuntas porque demuestra la capacidad que tiene el talento humano costarricense en transferencia e innovación, además del trabajo con la sociedad civil que sin duda son prioridad para el Gobierno de la República” dijo Carlos Enrique Alvarado, Ministro del MICITT.

Ante la situación de emergencia nacional de ciberseguridad y la solicitud del Ministerio, el Consejo Nacional de Rectores acordó encargar a la Comisión de Directores de Tecnologías de Información y Comunicación, el análisis del decreto Nº 37052-MICITT, referente a la creación del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) para definir necesidades y posibles aportes que las universidades estatales puedan realizar en la ruta de fortalecimiento del CSIRT-CR.

Se acordó conformar un equipo de trabajo con los miembros de la Comisión de Directores de Tecnologías de Información y Comunicación y en conjunto con representantes del MICITT, para desarrollar una estrategia en la búsqueda de soluciones de la emergencia de ciberseguridad que enfrenta el país y manifestar el apoyo total de las universidades estatales.

Para el presidente de CONARE y rector de la Universidad Estatal a Distancia (UNED), Rodrigo Arias Camacho “reiteró que el país puede contar con la universidad pública para la atención de los diferentes intereses nacionales.  La función de las universidades estatales es colaborar con el país a través de su talento humano especializado, por esta razón nos sumamos a los esfuerzos y coadyuvando con el MICITT para la atención de los diferentes problemas nacionales”.

## Avances alcanzados

Entre el lunes 16 de mayo y el 27 de mayo de 2022 se visitó y entrevistó a 226 instituciones del sector público, incluyendo municipalidades, para aplicar el instrumento de recopilación de información en seguridad digital diseñado por el MICITT.

El Grupo ICE brindó apoyo logístico en realizar la visita a las instituciones sobre todo a los gobiernos locales más alejados. Sin embargo, toda la información recopilada está siendo analizada y procesada por profesionales del MICITT, ésta será un insumo para las medidas de protección que se están estableciendo en el Plan de Emergencia, así como en recomendaciones específicas que se realizarán a cada institución en función de su nivel de vulnerabilidad.

Entre los principales hallazgos se encuentran: No contar con personal especializado en ciberseguridad que administren los sistemas; sistemas desarrollados por terceros, pero que no contemplan aspectos de seguridad; no realizar copias de seguridad de los sistemas que tienen alojados por un tercero; no implementar sistemas de protección y seguridad DNS; no implementar doble factor de autenticación en sus sistemas; no realizar auditorías de seguridad en sus servidores; no tener políticas definidas para las copias de seguridad; no realizar pruebas de restauración de copias de seguridad realizadas; no tener configurado el sitio para evitar ataques de tipo SQL injection; no cuentan con servicios innecesarios activos como SSH, FTP, telnet, además de que instituciones no han configurado un límite de accesos concurrentes para evitar ataques de denegación de servicios DDoS.

Si desea acceder más información sobre Ciberseguridad puede ingresar a: www.micitt.go.cr/ciberseguridad [2].

*Redacción: CONARE-MICITT.*

---



**Enlaces**
[1] https://www.tec.ac.cr/hoyeneltec/users/redaccion
[2] http://www.micitt.go.cr/ciberseguridad