

## CSIRT PARA LA AGRICULTURA COLOMBIANA, UN NUEVO PASO PARA LA RECONSTRUCCIÓN DE NUESTRA HISTORIA

CSIRT for Colombian agriculture, a new step for the reconstruction of our history

*Karen Julieth Mogollón Gelvis\**  
Ganador Concurso de Ponencias  
VII Congreso Carlos Martínez Silva  
Unisangil  
San Gil, Santander, Colombia

### **PONENCIA**

La audaz campaña libertadora de Bolívar ingresó victoriosamente a Santa Fe “Bajo un sol espléndido, en medio de una muchedumbre delirante que daba interminables triunfos al ejército patriota” (Muñoz, 2019). Nobles, campesinos, hombres del común, mujeres, ancianos, mucha gente salió a recibirlos. Bolívar entró a Santa Fe lleno de flores. La batalla legendaria había culminado, pero nacía con ello la compleja labor de dejar a un lado el pasado colonial y asumir las diferencias políticas para armar una República.

Doscientos años más tarde se ve el evidente uso, cada vez más grande, del entorno digital, en nuestro país con el cual se impulsa y promueve un aumento exponencial de la economía digital que ha pasado de 2.1 millones en

2010 a 10.11 millones de conexiones a internet en 2015 (MinTIC, 2015), lo cual refleja un aumento en el 482% en este período de tiempo. Todo ello conlleva repercusiones tanto jurídicas como sociales, algo que hace dos siglos no hubiera sido ni imaginable. Este cambio trae consigo nuevas amenazas (no enfrentamientos a muerte como lo fue la batalla liberadora, sino ahora riesgos de tipo cibernético) que involucran entidades públicas, privadas y la población en general. El no tener una administración adecuada de estos riesgos de seguridad digital puede llevar a la materialización de amenazas o ataques cibernéticos, generando efectos indeseables de naturaleza económica y social para el país, que afectan la integridad de los ciudadanos en este entorno. Es por ello esencial llevar a cabo acciones preventivas y correctivas

---

\*Estudiante de Quinto Semestre, Universidad de Pamplona, Norte de Santander.

para brindar tratamiento y manejo de estos peligros mencionados.

Entendiendo que cada vez son más las actividades socioeconómicas que sientan sus bases en el uso de las Tecnologías de la Información y las Comunicaciones (TIC), es fácil identificar la necesidad de ampliar el campo de acción de los esfuerzos por mantener la integridad de los activos de información de las organizaciones, la ciudadanía y el mismo Estado. Esto, con el fin de afianzar el crecimiento económico y social del país apoyado en el uso efectivo de las TIC. Una de las estrategias con mayor repercusión que se ha venido implementando a nivel mundial son los Equipos de Respuesta a Incidentes de Seguridad Informática, conocidos como CSIRT, Computer Security Incident Response Team (Conpes 3854, 2016).

### ***CASO ESPECÍFICO:***

De acuerdo con ello y entrando en materia, al tener en cuenta que el Ministerio de Agricultura es un departamento de gobierno encargado del sector agropecuario, pesquero y de desarrollo rural del país (Min Agricultura, 2017), este se encuentra contemplado dentro del catálogo de infraestructura crítica cibernética del país, elaborado por el Comando Conjunto Cibernético, CCOC. Requiere de un tratamiento especial de sus activos de información, y la concentración de todos los recursos necesarios para salvaguardar los procesos que desde allí se adelantan, y que son soportados por las TIC.

La inexistencia de una entidad organizacional que se haga responsable de coordinar y respaldar la respuesta a un evento o incidente de seguridad informática se traduce en la incapacidad de garantizar el bienestar de sus activos de información, toda vez que la información es el activo más importante para cualquier institución o empresa.

### ***PLANTEAMIENTO DE LA NECESIDAD:***

De aquí, la necesidad de definir las directrices y políticas para la creación y el lanzamiento de un CSIRT de Equipo de Respuesta a Incidentes de Seguridad Informática en el sector de agricultura de Colombia. Pero en su caso particular atendiendo sus necesidades y requerimientos específicos, ello en pro de garantizar la correcta operatividad y despliegue dentro del sector.

### ***¿Qué es un CSIRT?***

Un CSIRT es una entidad organizacional concreta (es decir, uno o más miembros del personal) a la que se le asigna la responsabilidad de coordinar y respaldar la respuesta a un evento o incidente de seguridad informática. Los CSIRT se pueden crear para Estados o economías nacionales, gobiernos, organizaciones comerciales, instituciones educativas e incluso entidades sin fines de lucro.

El objetivo de un CSIRT es minimizar y controlar el daño resultante de los incidentes, proporcionar una guía efectiva para las

actividades de respuesta y recuperación, y trabajar para evitar que ocurran incidentes en el futuro (Jaroszewski, 2003). Como se evidencia, la necesidad de tener una respuesta a los incidentes cibernéticos no da espera. Las empresas y las organizaciones se exponen al riesgo de ver comprometidos sus activos de información.

Uno de los aspectos más atractivos de tener una capacidad de respuesta a incidentes es que admite la respuesta a incidentes de forma sistemática, permite la documentación de incidentes para adelantar labores de retroalimentación y nuevas fases de planeación para fortalecer una base de conocimientos que permite un mejor despliegue de respuestas en un futuro (Nist, 2012).

En Colombia se han establecido algunos CSIRT tales como:

El Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional CSIRTPONAL, un grupo creado para atender las necesidades de prevención, atención e investigación de los eventos e incidentes de seguridad informática, con el fin de proteger la infraestructura tecnológica, los activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones (Ponal, 2019).

CSIRT Asobancaria, es un equipo de apoyo para la respuesta a incidentes cibernéticos, comunidad de intercambio, centro de excelencia en investigación y colaboración para anticipar y mitigar riesgos derivados de amenazas cibernéticas (Asobancaria, 2019).

El CSIRT-CCIT, es un centro de coordinación de atención a incidentes de seguridad informática colombiano, el cual está en contacto directo con los centros de seguridad de sus empresas afiliadas y está en capacidad de coordinar el tratamiento y solución de las solicitudes y denuncias sobre problemas de seguridad informática (CCIT, 2019).

Esto refleja la diversidad de necesidades que puede atender un CSIRT correctamente constituido y operable en los diferentes campos de acción.

## **CONCLUSIONES**

Alrededor del mundo, los Estados se han dado cuenta de la importancia de garantizar la supremacía en el ciberespacio y asegurar sus activos de información. Es por ello por lo que se han hecho grandes esfuerzos para capacitar personal y conformar diferentes entidades que permiten consolidar capacidades cibernéticas con el fin de enfrentar amenazas y hacer una gestión adecuada del riesgo cibernético.

Aunque el presupuesto proyectado para la implementación de un equipo de respuesta a incidentes cibernéticos CSIRT puede ser alto, con el desarrollo de los años es ampliamente compensado con el ahorro reflejado en tiempo, capacidad cibernética y recursos monetarios comprometidos en reparaciones a la hora de afrontar un incidente de naturaleza digital.

Al tener en cuenta que la conformación de los CSIRT es una tendencia mundial, cada equipo debe atender a necesidades específicas, por tal

razón es indispensable que el sector agricultura del Estado cuente con su propio CSIRT promoviendo así la gestión del riesgo en el ámbito cibernético específico para el agro colombiano, toda vez que esto facilita la toma de decisiones y el uso adecuado de los recursos tecnológico.

### REFERENCIAS:

Asobancaria. (2019). CSIRT Asobancaria. Retrieved from <https://www.asobancaria.com/csirt/>

CCN-Cert. (2019). *Defensa frente a las ciberamenazas*. Retrieved from <https://www.ccn-cert.cni.es/>

Cert-EE. (2019). Cert-EE. Retrieved from <https://www.ria.ee/en/cybersecurity/certee.html>

Conpes 3854. (2016). Política Nacional de Seguridad Digital, 91. Retrieved from <https://colaboracion.dnp.gov.co/CDT/Conpes/Econmicos/3854.pdf>

CSIRT.es. (2019). CSIRT.es. Retrieved from <https://www.csirt.es>

Felipe, E. & Rayas, U. (2014). Proceso para la definición de servicios iniciales en un equipo de respuesta ante incidencias de seguridad informática (CSIRT).

Jaroszewski, P. (2003). Why do I need a CSIRT? Why bother with security? (1) Security threats are

real, (May). Retrieved from <https://www.terena.org/activities/tfcsirt/meeting9/jaroszewski-assistancecsirt.pdf>

Killcrece, G., Kossakowski, K. P. & Ruefle, R. M. (2003). State of the practice of computer security incident response teams (CSIRTs). *Cmu*, 12(October), 1– 51. <https://doi.org/10.1109/MS.2005.158>

MinTIC. (2015). Colombia cerró 2015 con 12,4 millones de conexiones a internet banda ancha. Retrieved February 8, 2018, from <http://www.mintic.gov.co/portal/604/w3article-15180.html>

Muñoz, H. (2019) La batalla que aseguró la independencia de Colombia. *El Espectador*. Recuperado de <https://www.elespectador.com/libertadoras/la-batalla-que-aseguro-la-independencia-de-colombia>

Ponal. (2019). CSIRT Ponal. Retrieved from <https://cc-csirt.policia.gov.co/>