ESTADO DE CAROLINA DEL NORTE

ROY COOPER

GOBERNADOR

Marzo 16, 2022

ORDEN EJECUTIVA NÚM. 254

ESTABLECIMIENTO DEL GRUPO ESPECIALIZADO DE CIBERSEGURIDAD CONJUNTA DE CAROLINA DEL NORTE

POR CUANTO, a raíz del aumento de amenazas a la seguridad cibernética tanto en volumen como en sofisticación, hecho que requiere tener una comprensión del panorama de lo que las amenazas representan y de esa manera prevenir ataques, proteger de actos de terrorismo y delictivos, del crimen organizado o de actividades de grupos vandálicos a las redes de tecnología de información y la infraestructura crítica del estado; y

POR CUANTO, eventos geopolíticos, como la reciente invasión ilegal de Ucrania por parte de Rusia, pueden conducir al aumento de amenazas y ataques a la seguridad cibernética; y

POR CUANTO, los quebrantamientos a la seguridad cibernética tienen el potencial de afectar la prestación de servicios públicos esenciales y también los servicios privados que se ofrecen al pueblo de Carolina del Norte, y por cuanto amenazan la confidencialidad, integridad y disponibilidad de datos estatales, y por cuanto pueden causar la pérdida de reputación, daños y trastornos económicos significativos; y

POR CUANTO, el Estado debe identificar, proteger y responder a los ataques cibernéticos destinados a causar transgresiones a la privacidad, robo de identidad e interrupción a la continuidad comercial; y

POR CUANTO, a fin de proteger la seguridad pública y los datos de los individuos, las agencias estatales, los gobiernos locales, los gobiernos tribales, el sector privado, las instituciones académicas, las agencias federales y otras entidades estatales más deben mitigar los riesgos de seguridad cibernética mediante el intercambio de información, el seguimiento, la investigación forense e impulsar la respuesta ante incidentes; y

POR CUANTO, para prepararse y combatir dichas amenazas a la seguridad pública, el Departamento de Tecnología de Información de Carolina del Norte[1]/Oficina de Control de Riesgos y Seguridad Empresarial[2], la División de Manejo de Emergencias de Carolina del Norte[3], la Guardia Nacional de Carolina del Norte[4] y el Equipo de Blindaje de Ciberseguridad de la Asociación de Sistemas de Información del Gobierno Local[5] han creado un Grupo Especializado de Ciberseguridad Conjunta[6] (“Grupo Especializado”); y

POR CUANTO, el Grupo Especializado ofrece a Carolina del Norte servicios de importancia crucial para prevenir y responder a transgresiones y ataques de seguridad cibernética, incluyendo el aumento de amenazas de ciberseguridad derivadas de la reciente invasión ilegal de Ucrania por parte de Rusia; y

POR CUANTO, la seguridad cibernética de infraestructura de importancia crítica de Carolina del Norte se verá mejorada a través de una mayor interacción y comunicación entre este Grupo Especializado y las diversas partes interesadas, tanto del sector público como privado, a fin de identificar y responder a toda amenaza de ciberseguridad; y

---

[1] *North Carolina Department of Information Technology, NCDIT*
[2] *Enterprise Security and Risk Management Office*
[3] *North Carolina Division of Emergency Management, NCEM*
[4] *North Carolina National Guard, NCNG*
[5] *North Carolina Local Government Information Systems Association Cybersecurity Strike Team*
[6] *Joint Cybersecurity Task Force*

POR CUANTO, existen dieciséis Sectores de Infraestructura Crítica, según lo define la Directriz Presidencial de Políticas[7] ("PPD-21"), cuyos activos, sistemas y redes, ya sean físicos o virtuales, son factores vitales para el Estado de Carolina del Norte y, por cuanto su incapacitación o destrucción tendría un efecto debilitante en la protección, en la seguridad económica, en la salud o seguridad pública, o en cualquier combinación de las mismas; y

POR CUANTO, en Carolina del Norte existe una amplia variedad de instalaciones pertenecientes al Sector de Infraestructura Crítica, algunas de las cuales están abiertas al público o resguardan operaciones comerciales altamente sensibles e incluyen elementos cibernéticos como inmuebles de oficinas de uso general, instalaciones militares, juzgados, laboratorios estatales, y otras estructuras más que pudieran contener equipamientos críticos, sistemas, redes y operaciones esenciales para el Estado de Carolina del Norte; y

POR CUANTO, en los Estados Unidos la Infraestructura Crítica y Recursos Clave[8] ("CIKR") están bajo la amenaza constante de actividad maliciosa por parte de ejecutores de amenazas en lo individual, tales como terroristas, bandas de delincuentes cibernéticos y otros ejecutores maliciosos más; y

POR CUANTO, el enfoque de "Estado Integral" para abordar la seguridad cibernética adoptado por el Grupo Especializado es una estrategia comprobada y efectiva que prioriza la protección de la infraestructura CIKR; y

POR CUANTO, para mitigar los riesgos de la mejor manera, Carolina del Norte necesita tener una comprensión precisa de las entidades de infraestructura CIKR existentes en todo el estado, así como el estatus de sus programas de seguridad cibernética; y

POR CUANTO, existe la necesidad de que las entidades de infraestructura CIKR coordinen el abordaje y notifiquen acerca de incidentes de seguridad cibernética que sean significativos, a fin de remediar y plantear las causas fundamentales de un incidente de seguridad cibernética que sea significativo durante la fase de recuperación de algún incidente; y

Autoridad estatutaria y determinaciones

POR CUANTO, de conformidad con el Artículo III de la Constitución de Carolina del Norte y con el estatuto N.C. Gen. Stat.[9] §§ 143A-4 y 143B-4, el Gobernador es el Funcionario Ejecutivo del Estado y es el responsable de formular y administrar las políticas del poder ejecutivo del gobierno estatal; y

POR CUANTO, de conformidad con el estatuto N.C. Gen. Stat. § 147-12, el Gobernador tiene la autoridad y el deber de supervisar la conducta oficial de todos los funcionarios ejecutivos, ministeriales o secretariados; y

POR CUANTO, de conformidad con el estatuto N.C. Gen. Stat. § 166A-19.12(23), la División de Manejo de Emergencias de Carolina del Norte ("NCEM"), el Funcionario en Jefe de Información del Estado [10]("CIO del Estado") del Departamento de Tecnología de Información de Carolina del Norte ("NCDIT") y el General Adjunto de la Guardia Nacional de Carolina del Norte ("NCNG") se coordinan para plantear la respuesta a nivel estatal ante incidentes de seguridad cibernética y ante incidentes de seguridad cibernética que sean significativos, tal como se define en el estatuto N.C. Gen. Stat. § 143B-1320 y ese ámbito incluye, entre otros, la clasificación y el control de datos de acceso restringido, o altamente restringido, a través de las Políticas Estatales de Clasificación y Control de Datos[11], e incluye el desarrollo y la promulgación de políticas, planes y procedimientos necesarios para la seguridad cibernética y la protección de infraestructura crítica, así como la revisión anual, actualización y realización de pruebas a los planes y procedimientos de respuesta ante incidentes de seguridad cibernética; y

POR CUANTO, de conformidad con el estatuto N.C. Gen. Stat. § 143B-1321(a)(5) NCDIT debe planificar y coordinar los esfuerzos de tecnología de información conjuntamente con agencias estatales, con organizaciones sin fines de lucro y con organizaciones del sector privado según se requiera; y

POR CUANTO, de conformidad con el estatuto N.C. Gen. Stat. §§ 143B-1322(c)(5) y (11), el Funcionario CIO del Estado debe velar por la seguridad de los sistemas y redes de tecnología de información del Estado y por los datos asociados a tales sistemas, y por cuanto debe desarrollar sistemas y procesos estandarizados y por cuanto es responsable del control y protección de datos del Estado; y

---

[7] *Presidential Policy Directive, PPD*

[8] *Critical Infrastructure and Key Resources, CIKR*

[9] *North Carolina General Statute,* Estatuto General de Carolina del Norte, *N.C. Gen. Stat*

[10] *State Chief Information Officer, State CIO*

[11] *Statewide Data Classification and Handling Policy*

POR CUANTO, de conformidad con el estatuto N.C. Gen. Stat. § 143B-1376, el Funcionario CIO del Estado es responsable de la seguridad y privacidad de los sistemas y redes de tecnología de información del Estado y por los datos asociados a tales sistemas; y

POR CUANTO, de conformidad con el estatuto N.C. Gen. Stat. § 143B-1376, el Funcionario CIO del Estado administrará toda la esfera de seguridad de tecnología de información del poder ejecutivo y establecerá estándares estatales de seguridad y privacidad de tecnología de información a fin de maximizar la funcionalidad, la seguridad y la interoperabilidad de los activos distribuidos de tecnología de información del Estado, incluyendo, entre otros, la clasificación y control de datos, comunicaciones y tecnologías de encriptación y cifrado de información.

AHORA, POR LO TANTO, por los poderes conferidos a mí como Gobernador por la Constitución y las leyes del Estado de Carolina del Norte, **SE ORDENA:**

Sección 1. Establecimiento del Grupo Especializado de Ciberseguridad Conjunta

Por el presente documento, queda establecido el Grupo Especializado de Ciberseguridad Conjunta del Estado de Carolina del Norte.

a. El Grupo Especializado está conformado por miembros de las siguientes entidades:

   1. Departamento de Tecnología de Información de Carolina del Norte/Oficina de Control de Riesgos y Seguridad Empresarial

   2. División de Manejo de Emergencias de Carolina del Norte

   3. Guardia Nacional de Carolina del Norte

   4. Equipo de Blindaje de Ciberseguridad de la Asociación de Sistemas de Información del Gobierno Local de Carolina del Norte

b. Se invita a participar en el Grupo Especializado a un miembro de las siguientes agencias:

   1. Centro de Análisis e Intercambio de Información de Carolina del Norte.

   2. Buró Federal de Investigaciones.

   3. Servicio Secreto de los Estados Unidos

   4. Otras agencias federales, agencias estatales de Carolina del Norte o a diversas partes interesadas, según sea requerido y por invitación del Grupo Especializado.

Sección 2. Establecimiento de alianzas para proteger la infraestructura crítica y los recursos clave de Carolina del Norte

1. Se exhorta fuertemente a las entidades de infraestructura CIKR de Carolina del Norte, tanto del sector público como privado, que informen al Grupo Especializado acerca de direcciones protocolarias de Internet (dirección IP) orientadas al público para que el Grupo Especializado ayude a tales entidades a identificar y responder a vulnerabilidades de seguridad cibernética.

2. Se exhorta fuertemente a las entidades de infraestructura CIKR de Carolina del Norte, tanto del sector público como privado, que informen al Grupo Especializado acerca de incidentes de seguridad cibernética que sean significativos a fin de mitigar los efectos en cascada derivados de un incidente de seguridad cibernética.

3. Se exhorta fuertemente a las entidades de infraestructura CIKR de Carolina del Norte, tanto del sector público como privado, que participen con el Grupo Especializado en la coordinación de esfuerzos de respuesta y recuperación de incidentes de seguridad cibernética que sean significativos.

Sección 3. Sin derecho de acción privada

La presente Orden Ejecutiva no tiene la intención de crear, y no crea, ningún derecho, privilegio o beneficio individual, ya sea sustantivo o de procedimiento, exigible por ley o en equidad por cualquier parte contra el Estado de Carolina del Norte, sus agencias, departamentos, subdivisiones políticas u otras entidades, ni funcionarios, empleados o agentes de los mismos.

Sección 4. Fecha de vigencia y duración

La presente Orden Ejecutiva entra en vigencia de inmediato. La Orden permanecerá en vigencia hasta que se rescinda, siempre y cuando, el Grupo Especializado de Ciberseguridad Conjunta pueda continuar operando al momento del vencimiento o revocación de esta Orden Ejecutiva.

EN TESTIMONIO DE LO CUAL, firmo mi nombre y hago estampar el Gran Sello del Estado de Carolina del Norte en el Capitolio de la Ciudad de Raleigh, este 16º de marzo del año de Nuestro Señor dos mil veintidós.

(firma)

_____

Roy Cooper
Gobernador

DOY FE: *(Gran Sello del Estado de Carolina del Norte)*

(firma)

_____

Elaine F. Marshall
Secretaria de Estado

The Governor's Office is providing this Spanish translation of Executive Order Number 254 to serve North Carolina's Spanish-speaking population.

The English language version is the original document, and it takes precedence over any discrepancies due to nuance in translation.

Con el fin de brindar un servicio a la población hispanoparlante de Carolina del Norte, la Administración del Gobernador ofrece la presente traducción al español de esta Orden Ejecutiva Núm. 254.

La versión en inglés es el documento original; por lo tanto, es la versión que prevalecerá en caso de discrepancias debidas a los matices propios de la traducción.