

Asunto: Ataque cibernético

COMPETENCIA:

Previo a absolver la consulta, se señala que de conformidad con la Resolución No. 796 del 02 de noviembre de 2017 "Por la cual se suprime un grupo interno de trabajo, se conforman los grupos internos de Trabajo en el Archivo General de la Nación Jorge Palacios Preciado y se establecen sus funciones ", la Subdirección de Tecnología de la Información Archivística y Documento Electrónico, es competente para absolver las peticiones y consultas que se dirijan a esta Entidad.

MOTIVO DE LA CONSULTA:

"Les solicito información pertinente de:

1- ¿Cuáles procesos o procedimientos deben tener una E.P.S. ¿E frente a un eventual ataque cibernético?

2. ¿Se debe reportar el incidente al AGN? normatividad."

DE LA NORMATIVA APLICABLE

- **Ley 594 de 2000** "Ley General de Archivos"
- **Ley 599 de 2000** "Código Penal Colombiano"
- **ISO 27001** "Seguridad de la Información"
- **Ley 962 de 2005** "Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del estado y de los particulares que ejercen funciones públicas o prestan servicios públicos"
- **Ley 1273 de 2009** "Por medio de la cual se modifica el Código Penal"
- **Ley 1341 de 2009** "Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones"
- **Decreto 1008 de 2018** "Establece los lineamientos generales de la Política de Gobierno Digital para Colombia"

CONSIDERACIÓN:

Conviene precisar que las consultas que se presenten a esta Entidad se resuelven de manera general, abstracta e impersonal, de acuerdo con las facultades conferidas en el ejercicio de las atribuciones de dirección y coordinación de la función archivística del Estado Colombiano expresamente señaladas en la Ley 594 de 2000, y se circunscribe a hacer claridad en cuanto al texto de las normas de manera general, para lo cual armoniza las disposiciones en su conjunto de acuerdo al asunto que se trate y emite su concepto, ciñéndonos en todo a las normas vigentes sobre la materia.

En el marco de la seguridad digital, es importante mencionar el CONPES 3995 de 2020 sobre Política nacional de confianza y seguridad digital, el cual formula una política nacional que tiene como objetivo establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital. Para alcanzar este objetivo, en primer lugar, se fortalecerán las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado del país; en segundo lugar, se actualizará el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y finalmente, se analizará la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías.

A través de la Política Nacional de Seguridad Digital CONPES 3854, se busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia.

CONCLUSIÓN:

Conforme a las preguntas planteadas en su comunicación el Archivo General de la Nación le informa lo siguiente en cuanto a:

1. *¿Cuáles procesos o procedimientos deben tener una E?S.E frente a un eventual ataque cibernético*

En primera instancia el Ministerio de Tecnologías de la Información y las Comunicaciones es la entidad líder en materia de seguridad digital, junto con otras entidades responsables de la seguridad digital nacional como:

- Colbert -Grupo de Respuesta a Emergencias Cibernéticas de Colombia: es el organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa y tiene como misión la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional. Url: <http://www.colcert.gov.co/>
- CSIRT-PONAL- Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional: Es 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. <https://cc-csirt.policia.gov.co/>

- CCP – Centro Cibernético Policial. <https://caivirtual.policia.gov.co/>
- CCOCI - Comando Conjunto Cibernético: Se desempeña como unidad élite en aspectos relacionados con la Ciberseguridad y Ciberdefensa, incluida la protección de las Infraestructuras Críticas Cibernéticas Nacionales. <https://www.ccoc.mil.co/>

Por lo tanto, se recomienda realizar la respectiva consulta con las entidades anteriormente mencionadas y las entidades competentes en materia de seguridad digital y ataques cibernéticos.

2. ¿Se debe reportar el incidente al AGN? normatividad.”

En cuanto a esta inquietud, le informamos que el Archivo General de la Nación es el ente rector de la política archivística nacional conforme a la Ley 80 de 1989 y dentro de sus funciones se encuentran la de inspección, vigilancia y control de las entidades públicas en todos los niveles y a las entidades privadas que cumplen funciones públicas en la aplicación de la normatividad archivística, así como el de generar lineamientos para la gestión, autenticación, integridad y disponibilidad de los documentos y expedientes electrónicos de las entidades, entre otras funciones. Sin embargo no es competente en la resolución de eventos que signifiquen la vulneración de la seguridad digital como ataques cibernéticos de dichas entidades.

Por lo anterior, el reporte de incidentes en seguridad digital se debe realizar a las entidades anteriormente mencionadas y a las instancias competentes.

Finalmente, como complemento de la información brindada en este concepto recomendamos consultar recursos, herramientas, lineamientos y estándares que sirven de apoyo para el desarrollo del proceso relacionado con la gestión de documentos electrónicos y preservación digital de archivo, disponibles en: en nuestro sitio web <http://www.archivogeneral.gov.co/>.

En los anteriores términos se resuelve la consulta planteada, la cual debe considerarse dentro de los parámetros establecidos en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo, artículo 28, del Título II, Conceptos, capítulos I, II y III, sustituidos por la Ley 1755 de 2015, sobre el Alcance de los Conceptos.

Cordialmente,

 Firmado digitalmente
por ERIKA LUCIA
RANGEL PALENCIA
Fecha: 2020.11.03
19:31:47 -05'00'

ERIKA LUCIA RANGEL PALENCIA

Subdirectora de Tecnologías de la Información Archivística y Documento Electrónico

Copia: N/A

Proyectó: Gladys Narita García – Contratista Grupo de Documento Electrónico y Preservación Digital

Revisó: Sandra Milena Díaz Bermúdez – Coordinadora Grupo de Documento Electrónico y Preservación Digital

Archivado en: Conceptos técnicos.