ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA GENERAL

ALCALDÍA MAYOR DE BOGOTÁ - SECRETARÍA GENERAL
Rad. No. 2-2018-11773
Fecha: 25/05/2018 17:08:10
Destino: ENTIDADES DISTRITALES
Copia: N/A
Anexos: 6 FOLIOS

CIRCULAR N°. 037

Para: **SECRETARIOS(AS) DE DESPACHO, DIRECTORES(AS) DE DEPARTAMENTOS ADMINISTRATIVOS, GERENTES Y DIRECTORES(AS) DE UNIDADES ADMINISTRATIVAS ESPECIALES, GERENTES PRESIDENTES(AS) Y DIRECTORES(AS) DE ESTABLECIMIENTOS PÚBLICOS, EMPRESAS INDUSTRIALES Y COMERCIALES, SOCIEDADES PÚBLICAS, SOCIEDADES MIXTAS, ENTES UNIVERSITARIOS, HOSPITALES, ALCALDES LOCALES, VEEDOR DISTRITAL, CONTRALOR DISTRITAL Y LOCALES, DE BOGOTÁ, PERSONERO DE BOGOTÁ.**

De: **ALTA CONSEJERÍA DISTRITAL DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES.**

Asunto: **INCIDENTES DE CIBERSEGURIDAD Y MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MPSI) DEL MINTIC**

Su entidad tiene el deber de adoptar medidas de protección de la información. Si ésta se contiene en medios digitales, debe incrementar la ciberseguridad y prepararse para atender oportunamente los incidentes que se puedan presentar, para lo cual resulta fundamental que se cumplan los lineamientos definidos por las autoridades nacionales sobre la materia[1].

En este sentido, es clave que desde la alta dirección de su entidad se impulsen y fortalezcan las iniciativas de ciberseguridad que lidere la Dirección de TI[2] y en especial aquellas orientadas a cumplir el Modelo de Seguridad y Privacidad de la Información

[1] El artículo 2.2.35.6. del Decreto Único del Sector TIC, Decreto 1078 de 2015, recuerda que existe el deber legal de seguir las *"estrategias, políticas, planes, estándares, programas y lineamientos que para el efecto establezca el Ministerio de Tecnologías de la Información y las Comunicaciones"*.

[2] Figura obligatoria según el Decreto Único del Sector TIC, artículo Artículo 2.2.35.4.

("MPSI") y su Guía de Incidentes de Seguridad (los cuales están disponibles en la página del Ministerio de Tecnologías de la Información y las Comunicaciones, "MinTIC")[3].

Recuerde que las directrices nacionales exigen que su entidad tenga un enfoque preventivo y proactivo de ciberseguridad, que le permita estar preparado para la atención de un incidente, lo cual implica que por ejemplo su Dirección de TI debe contar con planes, herramientas y equipos calificados que le permitan saber cómo responder ante un eventual ataque cibernético. Dado que cualquier entidad está expuesta a un ataque cibernético, sería errado esperar a ser víctima de un incidente para tomar medidas de ciberseguridad.

Con el fin de apoyar estos deberes que tiene cada una de las entidades Distritales, la Alta Consejería Distrital de TIC recapitula en el documento anexo algunos elementos que deben ser tenidos en cuenta para este propósito de incrementar los niveles de ciberseguridad y de poder responder ante un eventual incidente de ciberseguridad. Allí recordaremos que, por ejemplo, las normas nacionales exigen que el equipo de TI de su entidad, tenga habilidades para actuar como primer respondiente y para ejercer la auditoría forense, de tal forma que cuenten con conocimientos que les permitan actuar adecuadamente, no sólo para atender el incidente, sino para manejar adecuadamente la evidencia que se reporta a las entidades respectivas.

Cordialmente,

SERGIO MARTÍNEZ MEDINA
Alto Consejero Distrital de TIC

Anexos: **6** folios

Proyectó: Erick Camilo Castellanos
Revisó: Iván Mauricio Hernández Lanao

[3] http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

ANEXO A LA CIRCULAR No.

REFERIDA A INCIDENTES DE CIBERSEGURIDAD Y MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL MINTIC

1. Conozca las entidades enfocadas en dar Respuesta a Incidentes de Seguridad Digital

Desde el año 2011 el Estado Colombiano generó iniciativas enfocadas en aumentar los niveles de ciberseguridad y en este marco creó instancias que brindan acompañamiento a las entidades en materia de prevención y atención de incidentes de ciberseguridad[4]. Incluso, algunas tienen competencias para recibir las denuncias respectivas, para dar paso a la investigación de posibles delitos contra la información o los datos.

Por lo tanto, sugerimos que su entidad y en particular su equipo de TI tenga conocimiento de la existencia de tales instancias y visite sus páginas de internet, para conocer el apoyo que pueden brindar. A continuación citamos algunas[5]:

- Grupo de respuesta a emergencias cibernéticas de Colombia del Ministerio de Defensa Nacional ("**colCERT**") http://www.colcert.gov.co/
- El Centro Cibernético Policial de la Policía Nacional de Colombia ("**CCP**") https://caivirtual.policia.gov.co/
- El Equipo de respuesta a incidentes de seguridad informática de la Policía Nacional ("**CSIRT PONAL**") https://cc-csirt.policia.gov.co/index.php

2. MinTIC como entidad líder en materia de seguridad digital

Mediante el Documento Conpes 3854 de 2016 el Estado Colombiano adoptó el "Conpes de Seguridad Digital", que contiene la política pública del Estado sobre el particular. Allí,

[4] Sobre el particular fue importante el Conpes 3701 de 2011, denominado "Política Pública de Ciberseguridad y Ciberdefensa".

[5] Además de las instancias que reseñamos en el cuerpo de este documento, tenga en cuenta que también se constituyó el Comando Conjunto Cibernético del Comando General de las Fuerzas Militares de Colombia ("**CCOC**"), la Delegatura de protección de datos en la Superintendencia de Industria y Comercio o el Comité de ciberdefensa de las Fuerzas Militares.

encargó a entidades del orden nacional la función de "Implementar en el Gobierno nacional un modelo de gestión de riesgos de seguridad digital" y en particular obligó al MinTIC a diseñar un *"modelo de gestión de riesgos de seguridad digital, teniendo en cuenta el marco conceptual de esta política, los estándares de seguridad internacionales y el marco de gestión de riesgos integral a nivel nacional"*[6].

En cumplimiento de este mandato y actuando como la entidad líder sobre el particular en todo el territorio nacional, el MinTIC definió el Modelo de Seguridad y Privacidad de la Información ("**MPSI**") y además cuenta con una **Subdirección de Seguridad y Privacidad de TI**, que se encarga de *"crear lineamientos y políticas de seguridad para las Entidades del Estado"* y de brindar *"acompañamiento a las entidades en la implementación del MPSI y fortalece las capacidades de los funcionarios y responsables en temas de seguridad a través educación formal y no formal"*[7].

Por lo anterior, es fundamental recordar que las entidades del Distrito deben observar los lineamientos definidos por el MinTIC, no sólo por ser la autoridad competente sino además porque ese Ministerio tiene el deber de contar con un equipo experto en Seguridad y Privacidad de TI que esté al tanto de los últimos avances en la materia. Lo anterior significa que los esfuerzos de las entidades del Distrito en materia de seguridad digital deben orientarse a cumplir lo que señale el MPSI y el MinTIC.

3. Importancia del Director de TI de su entidad

Habiendo visto que los lineamientos del MinTIC en materia de seguridad son obligatorios para el Distrito y que su entidad debe enfocar sus esfuerzos en cumplirlos, es fundamental que tal objetivo se materialice con el liderazgo del **Director de TI**, que como bien se sabe no sólo es una figura obligatoria, sino que además debe tener un rol

[6] Conpes de Seguridad Digital, numeral E.1.2.
[7] http://www.mintic.gov.co/portal/604/w3-propertyvalue-6198.html

transversal y habilitador en toda la organización y con influencia en la dirección de la organización, tal como lo señala el Decreto Único del Sector TIC[8].

Por lo tanto, es aconsejable que la implementación del MPSI y la prevención y atención de riesgos cibernéticos esté apoyada en la labor del Director de TI, razón por la cual es necesario que su entidad apoye las iniciativas que tenga este funcionario para proteger la información de la entidad Distrital.

Tenga en cuenta que su Dirección de TI es quien conoce las particularidades de la organización y sus sistemas de información y por lo tanto no sólo es el indicado para definir la mejor forma de mitigar los riesgos particulares o de proceder en caso de un incidente, sino que además debe ser visto como un aliado estratégico de las diversas áreas de la entidad, teniendo en cuenta que la tecnología y los sistemas de información no son un fin en sí mismos, sino habilitadores transversales.

4. "MPSI" expedido por el MinTIC y Guía de Incidentes de Seguridad

Tal como lo anuncia el MinTIC, el Modelo de Seguridad y Privacidad de la Información ("MPSI") *"se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL"*[9]. Esto ratifica que para las entidades Distritales obligadas a cumplirlo el MPSI no debe ser un aspecto novedoso, sino que debe hacer parte integral de la implementación de la normatividad de Gobierno en Línea (Gobierno Digital). El Modelo de Seguridad y Privacidad de la Información (MPSI) está disponible en la página del MinTIC[10] y contiene Guías que abordan diversos temas que permiten su implementación.

Para efectos de esta Circular cobra especial relevancia la **Guía de Incidentes de Seguridad (Guia 21)** y por lo tanto resaltamos la importancia de que su entidad y en

[8] Decreto Único del Sector TIC, artículo Artículo 2.2.35.4. "Cuando la entidad cuente en su estructura con una dependencia encargada del accionar estratégico de las Tecnologías y Sistemas de la Información y las Comunicaciones, **hará parte del comité directivo** y **dependerán del nominador o representante legal** de la misma".
[9] http://www.mintic.gov.co/gestionti/615/w3-article-5482.html
[10] http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

especial su Director de TI conozcan esta guía y que ella sea implementada. Los invitamos a acceder a este documento a través del siguiente enlace: http://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf.

4.1. Guía de Incidentes de Seguridad del MinTIC

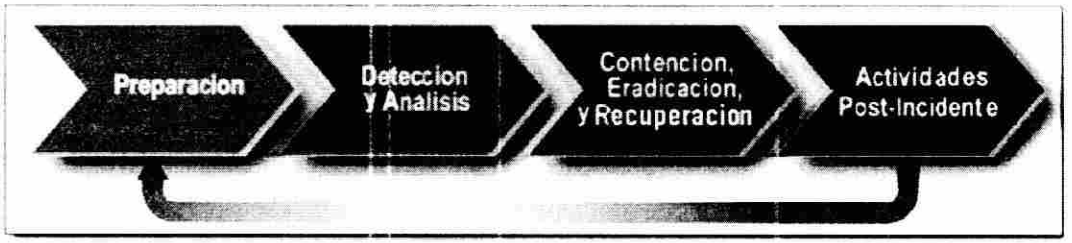
El propósito de esta Circular de la Alta Consejería Distrital de TIC no es sustituir la **Guía de Incidentes de Seguridad (Guía 21)**, que hace parte del MPSI, expedida por la autoridad competente sobre esta materia (el MinTIC) ni presentar una reseña exhaustiva de la misma. En este aparte reseñamos algunos aspectos de la Guía de Incidentes de Seguridad (Guía 21), para recordar la importancia de que su Entidad adopte un enfoque preventivo y proactivo que le permitan tener una adecuada gestión de incidentes de seguridad.

Recuerde que para hacer frente a un eventual incidente de seguridad que afecta la confidencialidad, integridad o disponibilidad de la información, se recomienda tener un enfoque estructurado y planificado en el cual se definan los roles y responsabilidades dentro de la Entidad, igualmente se requiere evaluar los riesgos y tener planeado como mantener la operación, la continuidad y la disponibilidad del servicio.

a. Recuerde que el *"objetivo principal del Modelo de Gestión de Incidentes de seguridad de la información es tener un enfoque estructurado y bien planificado que permita manejar adecuadamente los incidentes de seguridad de la información"*[11].

b. Tenga en cuenta que la gestión del incidente no inicia cuando ocurre o se detecta, sino mucho antes, desde la fase de planificación y allí es donde se debe concentrar el enfoque preventivo y proactivo:

[11] Guía de Incidentes de Seguridad del MinTIC, numeral 4.1.



Fuente MinTIC - Guía de Incidentes de Seguridad, numeral 4.2.

De esta manera, el propósito no sólo es tener un modelo que permita a la entidad estar en capacidad de responder ante un incidente, sino también en *"la forma como pueden ser detectados, evaluados y gestionar las vulnerabilidades para prevenirse, asegurando que los sistemas, redes, y aplicaciones son lo suficientemente seguros"*[12]. La Guía del MinTIC resalta el papel protagónico que tiene la Dirección de TI de cada entidad y señala algunos ejemplos de medidas que puede adoptar en esta fase de preparación, así como sugerencias sobre planes de comunicación, herramientas de software y hardware y recursos que permitan el análisis, mitigación y remediación de incidentes[13].

c. La Guía de Incidentes de Seguridad del MinTIC sugiere que con anterioridad cada entidad pueda determinar el grado de severidad que podrían tener los incidentes y a partir de ellos prever los tiempos de respuesta que debe implementar; definir los canales internos de comunicación de la situación para poder actuar oportunamente; prever estrategias de contención y erradicación de incidentes[14].

d. El MinTIC resalta la importancia de que su entidad cuente con roles definidos que le permitan atender un incidente. Sin perjuicio de los diversos roles señalados en la Guía de Incidentes de Seguridad del MinTIC, destacamos los siguientes:

	Descripción General	Requisitos

[12] Guía de Incidentes de Seguridad del MinTIC, numeral 4.2.
[13] Guía de Incidentes de Seguridad del MinTIC, numerales 4.2. y siguientes
[14] La guía presenta algunos ejemplos, como por ejemplo el bloqueo de una cuenta de un usuario que tenga sucesivos intentos fallidos de login, para prevenir un acceso no autorizado. Guía de Incidentes de Seguridad del MinTIC, numeral 5.6.

Agente Primer Punto de Contacto (Primer Respondiente)	Centraliza los incidentes reportados por los usuarios; da un tratamiento inicial y escala el incidente para que sea tratado.	• Estar capacitado en Seguridad de la Información (componente tecnológico) • Conocer clasificación de incidentes y procedimientos • Conocimiento básico de técnicas forenses (recolección y manejo de evidencia)
Analista forense	Apoyo para atender dudas de otros actores sobre los procedimientos. Ejerce liderazgo técnico en la atención de Incidentes de seguridad de la información	Disponible en caso de incidentes de alto impacto o con características particulares, para investigación completa orientada a solucionar el Incidente y determinar sus causas y características.
Líder del Grupo de Atención de Incidentes	Responsable del modelo de Gestión de incidentes. Tiene una visión general e interactúa con los diversos intervinientes	• Responde consultas sobre incidentes • Evalúa indicadores de gestión a la atención de incidentes y el cumplimiento de los procedimientos • Está en capacidad de convocar a otros funcionarios o actores • Puede activar planes de contingencia y/o continuidad

Extracto tomado de **Guía de Incidentes de Seguridad de MinTIC, numeral 6**

e. El MinTIC, como máxima autoridad en la materia, resalta en su Guía de Incidentes de Seguridad, la importancia de afrontar en debida forma un eventual incidente y de efectuar los reportes que resulten pertinentes. En particular, resalta la importancia que cobran dos instancias: El Grupo de Respuesta a Emergencias Cibernéticas de Colombia del Ministerio de Defensa Nacional ("**colCERT**")[15] y El Centro Cibernético Policial de la Policía Nacional de Colombia ("**CCP**")

	Lo que dice la Guía de Incidentes de Seguridad del MinTIC[16]

[15] Así lo señala también la Comisión de Regulación de Comunicaciones, quien recuerda que "el CONPES 3854 ha dispuesto que sea el colCERT el encargado de coordinar las acciones relacionadas con ciberataques", por lo que resalta la importancia de que se realice un reporte inicial al colCERT "para que luego esa entidad coordine las acciones necesarias dentro de la institucionalidad para dar respuesta a los mismos en caso de necesitar respuesta. https://www.crcom.gov.co/uploads/images/files/Dto%20Rtas%20Comentarios%20Seguridad%20redes_publicar.pdf

[16] Guía de Incidentes de Seguridad del MinTIC, numeral 7, puntos 4 y 5.

Reporte a COLCERT **www.colcert.gov.co/**	*"En el evento de que algún componente de la infraestructura tecnológica (sitios Web, aplicaciones, servicios en línea, sistemas de información, entre otros) de la Entidad, haya sido vulnerado o comprometido,* ***reportar en primera instancia al ColCERT*** *(Grupo de respuesta a emergencias cibernéticas de Colombia) por medio de correo electrónico a:contacto@colcert.gov.co o al Teléfono: (+571) 2959897"*
Su equipo experto en gestión de incidentes de seguridad	"En SEGUNDA instancia, adoptar las medidas y acciones necesarias para mitigar y resolver el incidente **con el apoyo del personal encargado de la gestión de incidentes de la entidad**, teniendo en cuenta la relevancia de ejecutar todos los procedimientos técnicos y operativos que faciliten la conservación (preservación) de las evidencias de naturaleza digital y soportes del incidente, fundamentales para tramitar su posterior judicialización ante la autoridad competente"
CCP **www.ccp.gov.co**	Cuando se tenga evidencia de un incidente informático, la entidad afectada se pondrá en contacto con el **Cai Virtual de la Policía Nacional www.ccp.gov.co, Centro Cibernético Policial** de la Policía Nacional al teléfono 4266900 ext. 104092, para recibir asesoría del caso en particular y posterior judicialización.

Extracto tomado de **Guía de Incidentes de Seguridad de MinTIC, numeral 7**

5. El Gobierno Nacional deberá expedir la Guía de Evidencia Digital

Como se vio, las políticas nacionales de seguridad digital (documentos CONPES 3854 de 2016 y 3701 de 2011) radican en entidades nacionales, como el MinTIC y el Ministerio de Defensa. Estas autoridades deben coordinar sus gestiones con las entidades competentes en materia de investigación y judicialización, particularmente con la Fiscalía General de la Nación, que de hecho adoptó un manual de procedimientos para cadena de custodia, el cual es de carácter general (no enfocado específicamente en evidencia digital) y probablemente será consultado por el MinTIC[17]

En el marco del Modelo de Seguridad y Privacidad de la Información ("MPSI"), el MinTIC elaboró la Guía 13 "Evidencia Digital". No obstante, dicha guía no está disponible para consulta, debido a que se encuentra en actualización al momento de la expedición de la

[17] **El manual de la Fiscalía está** esta dirigido "A los servidores públicos y particulares que tengan contacto con los elementos materia de prueba o evidencias físicas involucrados en el aseguramiento y conservación de las características originales y registro de las modificaciones que surjan dichos elementos, desde su recolección hasta su disposición final". Está **disponible en** www.fiscalia.gov.co/colombia/wp-content/uploads/2012/01/manualcadena2.pdf.

presente circular. tal como se observa en el enlace correspondiente al MPSI del Ministerio: http://www.mintic.gov.co/gestionti/615/w3-article-5482.html.

Dado que el Ministerio está en la obligación de publicar la guía correspondiente y es la autoridad encargada de tener el conocimiento más actualizado en la materia, invitamos a que su entidad haga seguimiento a portal del Modelo de Seguridad y Privacidad de la Información ("MPSI") del MinTIC (enlace de Internet antes señalado), para que una vez el Ministerio publique nuevamente la guía de "Evidencia Digital", su entidad cuente con un lineamiento sobre el particular.

En todo caso, se hace fundamental que se prepare para atender un incidente de ciberseguridad atendiendo a las recomendaciones formuladas por entidades como el Grupo de respuesta a emergencias cibernéticas de Colombia del Ministerio de Defensa Nacional ("**colCERT**", http://www.colcert.gov.co/); el Centro Cibernético Policial de la Policía Nacional de Colombia ("**CCP**", https://caivirtual.policia.gov.co/) o el Equipo de respuesta a incidentes de seguridad informática de la Policía Nacional ("**CSIRT PONAL**" https://cc-csirt.policia.gov.co/index.php). Por lo tanto, ratificamos lo dicho en capítulos anteriores, acerca de la importancia de que su entidad esté familiarizada con dichas entidades y se apoye en ellas antes, durante y después del incidente.

5.1. Policía Nacional y Delitos Informáticos

Como se vio atrás, la Guía de Incidentes de Seguridad del MinTIC resalta que en caso de un incidente, su entidad debe reportarlo de inmediato y en primera instancia al **ColCERT** (Grupo de Respuesta a Emergencias Cibernéticas de Colombia). Para el efecto, en el siguiente enlace el ColCERT publicó información relevante acerca de aspectos que deben ser reportados: http://www.colcert.gov.co/?q=contenido/reportar-un-incidente.

Ahora bien, es posible que un incidente de seguridad involucre la presunta comisión de un delito, como por ejemplo aquellos que afecten la protección de la información y de los

datos[18]. Por lo tanto, su equipo de atención de incidentes (que como se vio, debe involucrar por ejemplo un Agente Primer Punto de Contacto o primer respondiente; Analista Forense; y Líder del Grupo de Atención de Incidentes)[19] debe adelantar actividades orientadas a recoger los soportes del incidente y facilitar la cadena de custodia de las evidencias digitales[20], pues esto será de utilidad para que las autoridades competentes puedan adelantar la investigación y judicialización correspondiente.

Para el efecto es fundamental que su entidad se ponga en contacto con el Centro Cibernético Policial de la Policía Nacional (CCP) www.ccp.gov.co, al teléfono 4266900 ext. 104092,[21] para recibir asesoría especializada técnica y jurídica del incidente en particular y gestionar con ellos la posterior judicialización.

Tenga en cuenta que es posible presentar la denuncia de la presunta comisión de un delito a través de la página dispuesta para el efecto por parte de la Policía Nacional[22] y que existe un enlace especial para delitos informáticos[23] https://adenunciar.policia.gov.co/adenunciar/default.aspx y que dicha página incluye unos términos y condiciones acerca del trámite cue se le da a la denuncia (por ejemplo verificación por parte de la Policía, asignación de un Número Único de Noticia Criminal, entre otros).

Igualmente, el portal permite que incluya los "soportes que apoyan la denuncia", por lo cual podrá incluir distintos tipos de elementos, como fotografías, videos y otros documentos. Dado que esta evidencia será importante para que la Policía y la Fiscalía puedan adelantar sus actividades de investigación y posterior judicialización de los presuntos delitos, se

[18] **Código Penal, Título VIIBIS**, denominado "De la Protección de la información y de los datos", que fue adicionado por la Ley 1273 de 2009.
[19] MinTIC, Guía de Incidentes de Seguridad de MinTIC, numeral 6
[20] MinTIC, Guía de Incidentes de Seguridad de MinTIC, numeral 7
[21] MinTIC, Guía de Incidentes de Seguridad de MinTIC, numeral 7
[22] https://adenunciar.policia.gov.co/adenunciar/frm_denuncia_di.aspx. **En dicho portal se resalta la siguiente definición:** *"Denunciar es poner en conocimiento ante la autoridad competente un comportamiento que puede ser contrario a la ley penal, el cual será investigado por la fiscalía general de la nación con el fin de impartir justicia".* **Igualmente, resalta que** ***"al presentar la denuncia o querella, ya sea verbal o escrita, usted se encuentra bajo la gravedad del juramento, con implicaciones penales en caso de realizar una falsa denuncia (art. 69, Ley 906 de 2004)".***
[23] **Esta página web de la Policía Nacional señala:** *"Los delitos informáticos son conductas en que el o los delincuentes se valen de programas informáticos para cometer delitos como implantación de virus, suplantación de sitios web, estafas, violación de derechos de autor, piratería, etc".* Igualmente cuenta con un link a la normatividad pertinente.

ratifica la importancia de que su labor se realice de la mano de la Policía Nacional, haciendo uso del apoyo que brinda el Centro Cibernético Policial de la Policía Nacional (CCP) www.ccp.gov.co y que además esté atento a cualquier novedad acerca de la Guía de Evidencia Digital que debe expedir el MinTIC, para lo cual puede hacer seguimiento permanente al siguiente enlace: http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

6. Conclusiones

- La seguridad digital es un elemento fundamental para su entidad y por lo tanto debe apoyar los esfuerzos de su Director de TI para dar cumplimiento al Modelo de Seguridad y Privacidad de la Información ("MPSI") definido por el MinTIC, el cual hace parte de la normatividad de Gobierno en Línea (Gobierno Digital).
- La política nacional de seguridad digital, plasmada en dos documentos CONPES, asigna a autoridades nacionales como el MinTIC y el Ministerio de Defensa la función de expedir lineamientos sobre la materia.
- Al ser la autoridad competente, el MinTIC expidió la **Guía de Incidentes de Seguridad (Guía 21)** y deberá expedir una versión actualizada de su **Guía de Evidencia Digital (Guía 13)**.
- La **Guía de Incidentes de Seguridad del MinTIC** resalta la importancia de adoptar una visión preventiva y no simplemente reactiva frente a tales incidentes. Por lo tanto, es fundamental que su Director de TI esté familiarizado con esta guía y cuente con herramientas y un equipo humano que le permita atender eventuales incidentes (por ejemplo Agente Primer Punto de Contacto o primer respondiente; Analista Forense; y Líder del Grupo de Atención de Incidentes).
- Colombia cuenta con autoridades especializadas en incidentes de seguridad digital, como son Grupo de Respuesta a Emergencias Cibernéticas de Colombia del Ministerio de Defensa Nacional ("**colCERT**", http://www.colcert.gov.co/); el Centro Cibernético Policial de la Policía Nacional de Colombia ("**CCP**", https://caivirtual.policia.gov.co/) o el Equipo de respuesta a incidentes de seguridad informática de la Policía Nacional ("**CSIRT PONAL**" https://cc-csirt.policia.gov.co/index.php), es fundamental que su equipo de TI esté

familiarizado con su existencia, conozca de antemano la información que publican y que acuda a ellos en caso de un incidente de seguridad.

* * *