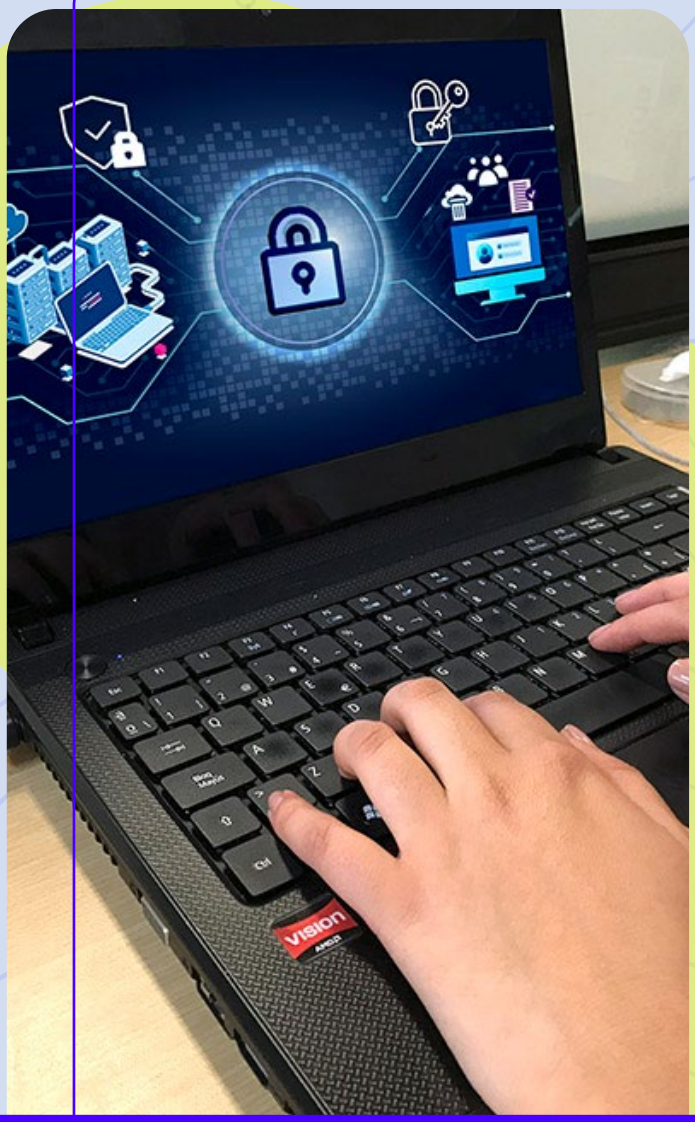
# ABC

El futuro es de todos

Gobierno de Colombia

# PROCESO DE GESTIÓN DE INCIDENTES

CSIRT
GOBIERNO DE COLOMBIA



Hechos QUE CONECTAN

# Política Pública en Seguridad Digital

La política pública en materia de Seguridad Digital se viene formalizando a través de documentos CONPES desde el año 2011, estos han sido:

- **CONPES 3701 de 2011 - LINEAMIENTOS DE POLÍTICA PARA CIBERSEGURIDAD Y CIBERDEFENSA.**
- **CONPES 3854 de 2016 - POLÍTICA NACIONAL DE SEGURIDAD DIGITAL.**
- **CONPES 3995 de 2020 - POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL.**

**¿Sabías que existen dos políticas en el Modelo Integrado de Planeación y Gestión de la Función Pública donde se incluye la Seguridad y Privacidad de la Información y la Seguridad Digital dentro de los procesos de gestión y desempeño de la entidad?, estas son:**

- **Política de Gobierno Digital - Habilitador trasversal de Seguridad y Privacidad de la Información.**
- **Política de Seguridad Digital.**

# Normatividad asociada:

**1. Decreto 1499 de 2017: (...) ARTÍCULO 2.2.22.1.5. Articulación y complementariedad con otros sistemas de gestión.** El Sistema de Gestión se complementa y articula, entre otros, con los Sistemas Nacional de Servicio al Ciudadano, de Gestión de la Seguridad y Salud en el Trabajo, de Gestión Ambiental y de Seguridad de la Información. (...)

**2. Decreto 612 de 2018: Artículo 1.** (...)Las entidades del Estado, de acuerdo con el ámbito de aplicación del MIPG, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año: (...) 11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, 12. Plan de Seguridad y Privacidad de la Información (...)


Hechos QUE CONECTAN

**3. Decreto 1008 de 2018:** "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".

**4. Resolución 500 del 10 de marzo de 2021,** "por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".

**5. Directiva Presidencial No. 3 del 15 de marzo de 2021,** respecto a lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

**6. Directiva Presidencial No. 02 del 24 de febrero de 2022,** cuyo asunto es la reiteración de la Política Pública en materia de Seguridad Digital.

## Responsabilidad de los representantes legales / directores de las entidades en la adopción de las políticas de Gobierno Digital y Seguridad Digital

- **Manual Operativo de MIPG:** (...) 3.1 Institucionalidad (...) Comité Institucional de Gestión y Desempeño: liderado por el viceministro o subdirector de departamento administrativo, y en el nivel descentralizado por los secretarios generales o administrativos. Estará a cargo de orientar la implementación y evaluación de MIPG en cada entidad u organismos público. La Secretaría Técnica será ejercida por el jefe de la oficina de planeación de la respectiva entidad o quien haga sus veces. Este Comité sustituye los demás comités que tengan relación con los sistemas que se integran en el Sistema de Gestión y el Modelo y que no sean obligatorios por mandato legal.

- **Responsable Institucional de la Política de Gobierno Digital:** (...) es el representante legal de cada sujeto obligado y es el responsable de coordinar, hacer seguimiento y verificación de la implementación de la Política de Gobierno Digital. Como responsables de la política de Gobierno Digital, los representantes legales (ministros, directores, gobernadores y alcaldes, entre otros), deben garantizar el desarrollo integral de la política como una herramienta transversal que apoya la gestión de la entidad y el desarrollo de las políticas de gestión y desempeño institucional del Modelo Integrado de Planeación y gestión. (...)

▪ **Circular Presidencial No. 2 de febrero de 2022:** Los representantes legales de las entidades públicas, deberán tomar las decisiones necesarias para contar con el correspondiente soporte en cuanto a las plataformas tecnológicas requeridas para garantizar el adecuado funcionamiento y la prestación de servicios a cargo de cada entidad, así como efectuar la evaluación y priorización del aprovisionamiento de capacidades informáticas haciendo uso de entornos en la nube, atendiendo las recomendaciones y guías que para el efecto disponga el Ministerio de Tecnologías de la Información y las Comunicaciones.

## Herramientas de apoyo

### 1. Habilitador Transversal de Seguridad y Privacidad de la Información Política de Gobierno Digital

Este habilitador se desarrolla a partir de dos herramientas básicas:

▪ El Modelo de Seguridad y Privacidad de la Información (MSPI) y sus guías para implementación.

▪ El Modelo de Riesgos de Seguridad Digital - Guía para la Administración del Riesgo y diseño de controles para las entidades públicas (DAFP).

A través de éstos, las entidades encuentran lineamientos y buenas prácticas de cómo ajustar cada uno de los elementos en los procesos de planeación y gestión de la seguridad de la información.

### 2. Equipo de Respuesta a Incidentes Cibernéticos para las Entidades del Gobierno (CSIRT Gobierno):

Ofrece a través de su portafolio de servicios (proactivos, reactivos y de Gestión de las Seguridad), las capacidades para apoyar a las entidades del Gobierno en la identificación de amenazas actuales, gestión de incidentes y concientización en gestión de incidentes.

# Definiciones

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).

- **Activos de Información y recursos:** se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 2016).

- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Ataque:** Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo (NIST, ISO 27000).

- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

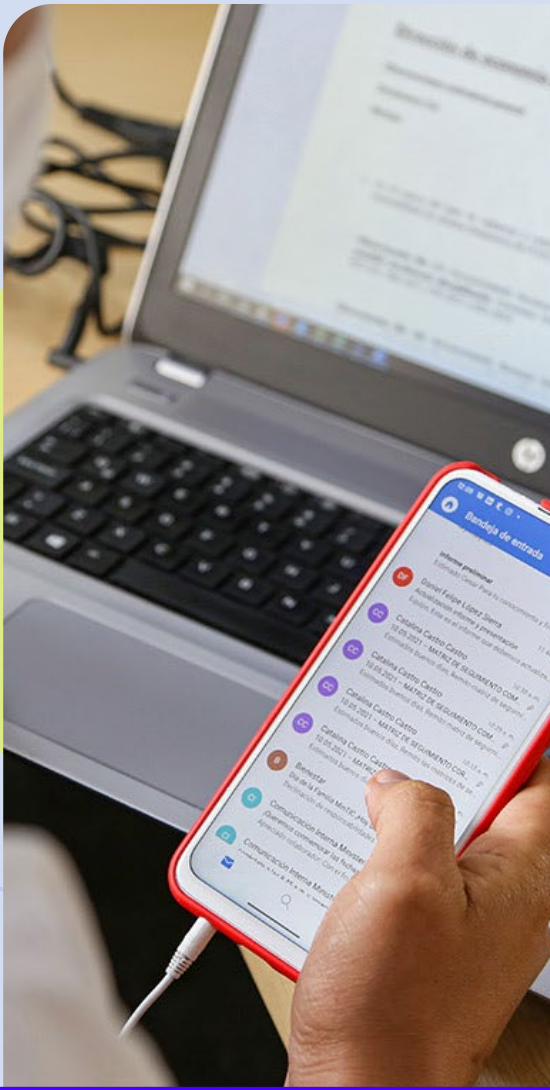
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Evento :** Es cualquier acontecimiento observable en un sistema o red. Los eventos incluyen un usuario que se conecta a un archivo compartido, un servidor que recibe una solicitud de una página web, un usuario que envía un correo electrónico y un firewall que bloquea un intento de conexión. Los eventos son neutrales, no necesariamente implican un impacto negativo. (NIST)

- **Incidentes cibernéticos:** Es la materialización de una violación o amenaza inminente de violación a las políticas de seguridad, políticas de uso aceptable o las prácticas de seguridad estándar (NIST).

- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).



Hechos QUE CONECTAN

- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25).

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

- **Seguridad digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

## Cómo entidad, ¿cómo me preparo para la gestión de un incidente de seguridad digital?

Para lograr estos objetivos, la gestión de incidentes de seguridad de la información involucra los siguientes procesos de manera cíclica:

1. Planificación y preparación.
2. Detección y análisis.
3. Contención, erradicación y recuperación.
4. Actividades Post-Incidente.

▪ **Planificación y preparación para la gestión del Incidente:** la entidad debe preparase antes de la materialización de una amenaza.

**Nota:** La etapa de preparación debe ser apoyada por la dirección de tecnologías de la información o quien haga sus veces, incluyendo las mejores prácticas para el aseguramiento de redes, sistemas, y aplicaciones, por ejemplo.

En la entidad debe existir un listado de fuentes generadoras de eventos que permitan la identificación de un incidente de seguridad de la información.

▪ **Detección y análisis:** En esta fase se determina si ha ocurrido un incidente, se validan los reportes de los equipos de seguridad, se indaga sobre información relacionada con el incidente, se documenta la investigación, se recopila la evidencia, se prioriza la gestión del incidente según su impacto y se reporta el incidente al interior y al CSIRT Gobierno.

▪ **Contención, erradicación y recuperación:** en esta etapa se recomienda a la entidad dependiendo de la criticidad del evento y de sus consecuencias, adquirir, preservar y asegurar la evidencia, identificar el vector de ataque, eliminar el malware, deshabilitar la cuenta de usuario comprometida, entre otros, mitigar todas las vulnerabilidades que fueron explotadas, devolver los sistemas afectados a un estado operativo y confirmar si los sistemas afectados funcionan con normalidad.

## Recursos de Comunicación

En este numeral se pretende enunciar los elementos necesarios para la comunicación del equipo de atención de incidentes dentro de la entidad.

▪ Información de Contacto: Se debe tener una lista de información de contacto de cada una de las personas que conforman el grupo de gestión de incidentes o quienes realicen sus funciones.

▪ Información de Escalamiento: Se debe contar con información de contacto para el escalamiento de incidentes según la estructura de la entidad.

▪ Información de los administradores de la plataforma tecnológica (Servicios, Servidores).

▪ Contacto con el área de recursos humanos o quien realice sus funciones (por si se realizan acciones disciplinarias).

▪ Contacto con áreas interesadas o grupos de interés **csirtgob@mintic.gov.co.**

**Nota 1:** La entidad debe tener una política de comunicación de los incidentes de seguridad para definir que incidente puede ser comunicado a los medios y cual no.

**Nota 2:** En algunas ocasiones durante el proceso de Atención de Incidentes de Seguridad Informática específicamente en la fase de "Contención, Erradicación y Recuperación" se puede hacer necesario activar el BCP (Plan de Continuidad del Negocio) o el DRP (Plan de Recuperación de Desastres) en el caso que un incidente afecte gravemente a un determinado sistema.

- **Actividades Post-Incidente:** Las lecciones aprendidas siempre se deben tomar en cuenta en el plan de mejoramiento de la entidad, una vez se identifican las brechas de seguridad y vulnerabilidades en el entorno tecnológico; también se realiza un seguimiento periódico establecido en las políticas de la entidad para observar los factores que aún se deben mejorar.

**Nota:** Es recomendable que las entidades implementen un SOC y creen un equipo de atención de incidentes de seguridad en cómputo CSIRT o un grupo que haga sus veces, quienes se encargaran de definir los procedimientos a la atención de incidentes, realizar la atención, manejar las relaciones con entes internos y externos, definir la clasificación de incidente.

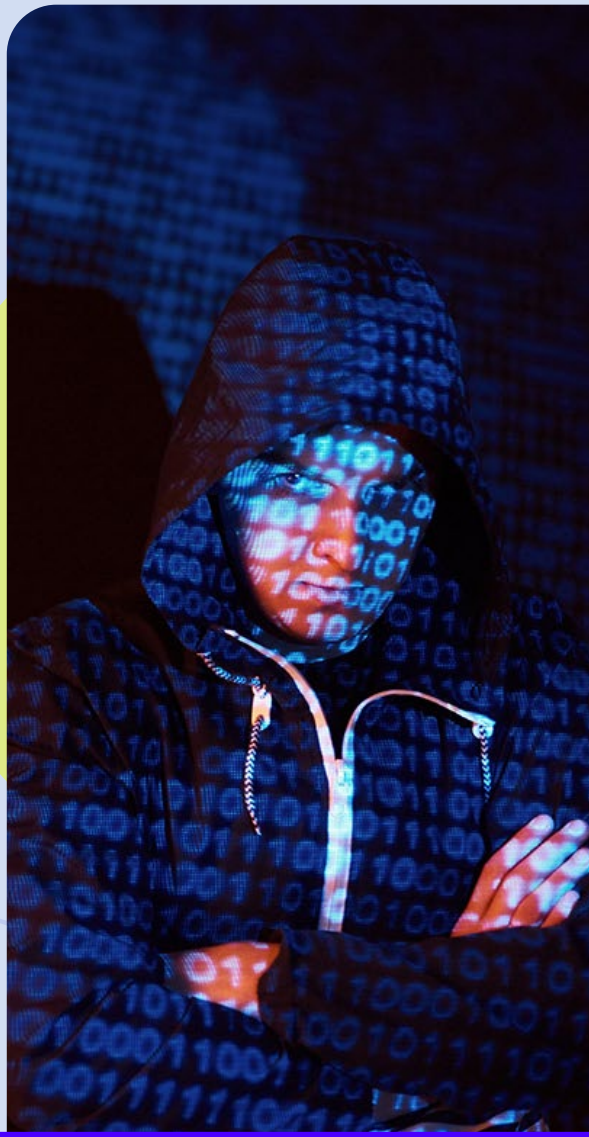
## ¿Si tengo un incidente de seguridad digital cómo debo actuar?

A continuación, se describe un proceso de notificación de incidentes de seguridad que podría ser adoptado por la entidad:

1. Un usuario, tercero o contratista que sospeche sobre la materialización de un incidente de seguridad deberá notificarlo al primer punto de contacto definido por la entidad (Ej: Soporte de primer nivel) a través de los canales definidos por la entidad.

2. El primer punto de contacto identificará el tipo de incidente (de acuerdo con la tabla de clasificación de incidentes que realiza la entidad). Analizará si el incidente reportado corresponde a un incidente de seguridad de la información y será el encargado de realizar el seguimiento del Incidente hasta su cierre definitivo.

3. El punto de contacto es la persona encargada de la atención de estos, el cual coordina y asignar las actividades con las partes interesadas.



4. La persona encargada de la atención de incidentes tendrá la potestad para decidir sobre las acciones que se deban ejecutar ante la presencia de un incidente de seguridad y es la persona que notificará a las altas directivas de la entidad.

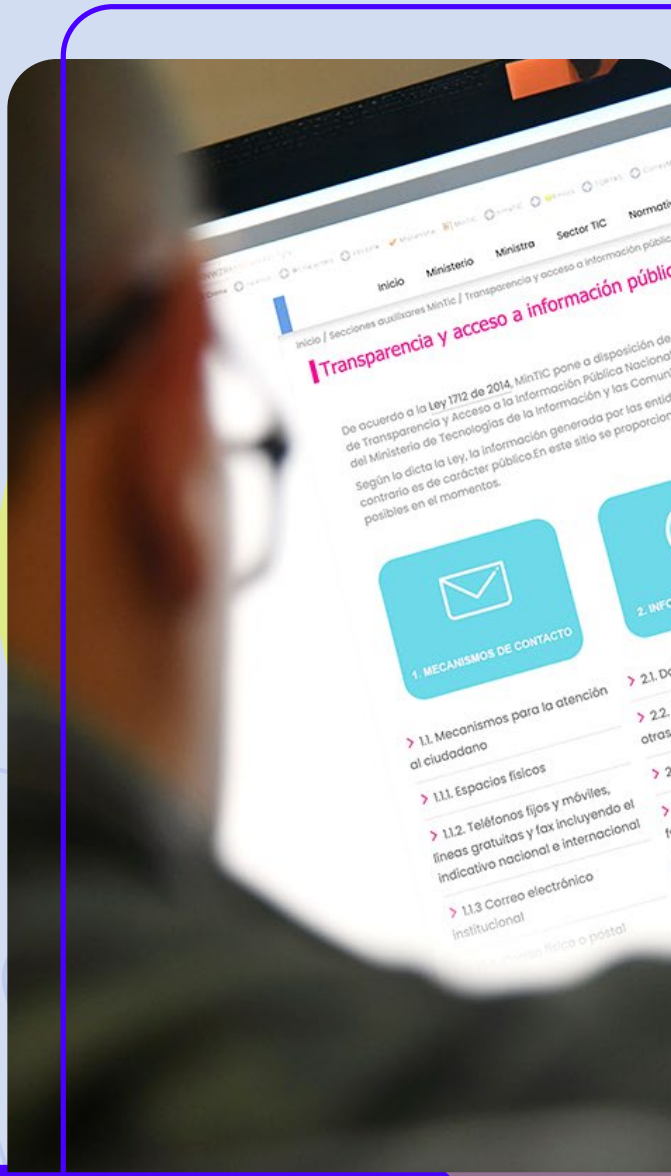
5. Identificado el incidente cibernético, por el CISO o encargado de seguridad digital de la entidad, se debe reportar el incidente diligenciando el formato de reporte de incidentes en su totalidad y enviarlo al CSIRT Gobierno - csirtgob@mintic.gov.co para realizar el apoyo en su gestión, acompañamiento y coordinación con otras instancias.

## Una vez identificado el incidente, ¿a quién debo reportar?

Los incidentes se deberán reportar ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno, teniendo en cuenta lo siguiente:

1. Los incidentes catalogados por el responsable de seguridad digital de la entidad, como **Menos Grave y Menor,** deben ser comunicados al CSIRT Gobierno en el formulario establecido una vez sea gestionado, con el fin de poder llevar una estadística de los incidentes y conocer las tipologías de estos.

2. Por otro lado, los incidentes catalogados como **Muy Grave y Grave** por la entidad, para el respectivo apoyo y coordinación en la gestión de estos a través del formato de reporte establecido por el CSIRT Gobierno, el cual estará disponible por los canales de comunicación autorizados:




**Contactando a la mesa de servicio, llamando a la línea gratuita**
**018000 910 742,**
**Opción 2, seguridad digital.**

**Correo electrónico: Enviando un mensaje de correo electrónico informando el incidente al buzón csirtgob@mintic.gov.co, adjuntando el Formato de Reporte de incidentes debidamente diligenciado.**

**Micrositio:**
**gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno/**

Hechos QUE CONECTAN

## Recomendaciones Finales

1. Actualizar todos los datos de contacto relativos al nombre de dominio de la entidad, de tal forma que queden reflejados en el servicio público de información de registros de nombres de dominio **WHOIS.CO.** Esta información es de suma importancia para contactar a la entidad, en caso de presentarse un incidente.

Cabe aclarar que, según lo indicado en **el artículo 5 de la Resolución 1652 del 2008,** cuando el Registrante o titular de un nombre de dominio bajo ".CO" suministre información "falsa, incorrecta o inexacta", el nombre de dominio podrá ser suspendido e incluso dado de baja.

Si se requiere información para realizar dicha actividad de actualización, favor ingresar a la página **www.cointernet.com.co/panel-de-control** o comunicarse al siguiente número telefónico en Bogotá **601 616 99 61.**

2. Según el análisis e investigación de los incidentes y teniendo en cuenta la causa raíz, deben realizar los respectivos planes de mejoramiento, para lo cual el responsable de seguridad digital de la entidad supervisará y hará seguimiento a su cumplimiento.

**Ministerio de Tecnologías de la Información y las Comunicaciones**
Edificio Murillo Toro Cra. 8 entre calles 12A y 12B
Bogotá, D.C. - Colombia - Código Postal 111711
Tel: (+57) 601 344 34 60 - Línea Gratuita:
01-800-0914014
Correo: minticresponde@mintic.gov.co
Horario de Atención:
Lunes a Viernes 8:30 am - 4:30 p.m.

**www.mintic.gov.co**

Hechos QUE CONECTAN