



MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

RESOLUCIÓN NÚMERO

DE 2020

“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”

LA MINISTRA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

En ejercicio de sus facultades legales, en especial las que le confiere el parágrafo del artículo 16 del Decreto 2106 de 2019, y

CONSIDERANDO QUE

Conforme al principio de "masificación del gobierno en línea" hoy Gobierno Digital, consagrado en el numeral 8 del artículo 2 de la Ley 1341 de 2009, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones.

De acuerdo con el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015 (DUR-TIC), "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", la Política de Gobierno Digital será definida por MinTIC y se desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC.

Según el numeral 2, los habilitadores transversales de la Política de Gobierno Digital, son los elementos fundamentales de Seguridad y privacidad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los componentes y el logro de los propósitos de dicha Política.

El parágrafo del artículo 16 del Decreto 2106 de 2019, "Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública" señala que las autoridades deberán disponer de una estrategia de seguridad digital, para la gestión documental electrónica y preservación de la información, siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1. Objeto. La presente resolución tiene por objeto establecer los lineamientos generales y estándares para que las entidades dispongan de una estrategia de seguridad digital, para la gestión documental electrónica y preservación de la información, y adoptar el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

“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”

ARTÍCULO 2. *Ámbito de aplicación.* Son sujetos obligados de la presente resolución los señalados en el artículo 2.2.9.1.1.2. del Decreto 1078 de 2015 (DUR-TIC), "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"

ARTÍCULO 3. *Lineamientos generales.* Los sujetos obligados deben adoptar medidas técnicas, administrativas y de recurso humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos e incidentes cibernéticos relacionados con la protección y la privacidad de la información. Las entidades deben contar con políticas, procesos y procedimientos para gestionar efectivamente los riesgos de seguridad digital, protección y privacidad de la información. En ese sentido, deben adoptar, como mínimo, las medidas que se relacionan en la presente resolución en materia de seguridad Digital.

Para todos los procesos, tramites, sistemas de información, infraestructura tecnológica e infraestructura crítica de los sujetos obligados, se deben adoptar medidas de seguridad eficientes para prestar servicios de confianza, generando protección de la información de los ciudadanos, y apoyando la mitigación de incidentes cibernéticos o filtración de datos personales.

ARTÍCULO 4. *Sistema de gestión de seguridad de la información y seguridad digital.* Los sujetos obligados deben aplicar las guías, modelos y demás documentos técnicos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones a través del habilitador de seguridad y privacidad de la información en el marco de la política de gobierno digital, y propenderán por la incorporación de estándares internacionales como lo son ISO 27032, NIST con sus publicaciones SP800 y SP1800, ISF (Information Security Forum), CIS Critical Security Controls (CSC) o Cobit 5 for Information Security, y sus respectivas actualizaciones o modificaciones, u otro estándar internacional.

ARTÍCULO 5. *La estrategia de seguridad digital y de la información.* Los sujetos obligados deben adoptar la estrategia de seguridad digital y de la información en la que se integren los principios, políticas, procedimientos y lineamientos para la gestión de la seguridad digital y la gestión de riesgos de seguridad digital. Esta política debe incorporarse a través de la implementación del modelo de seguridad y privacidad de la información como uno de los habilitadores de la política de Gobierno Digital, además de:

1. Ser aprobada por la dirección de la entidad a través de un acto administrativo de carácter general.
2. Establecer una estrategia de seguridad digital alineada con el plan de seguridad de la información, los planes estratégicos y el apetito de riesgo de la Entidad.
3. Los sujetos obligados deben realizar un análisis de riesgos de seguridad digital e implementar los controles técnicos que permitan mitigar las vulnerabilidades en el análisis realizado.
4. Documentar las responsabilidades, procesos, procedimientos, etapas y la gestión relacionada con seguridad física y lógica. Para ello se deberá dar cumplimiento a los roles establecidos en el Título 35 del Decreto 1083 de 2015
5. Establecer los roles al interior de la entidad y responsabilidades asociados a seguridad digital y seguridad de la información.
6. Identificar y clasificar los activos de información e infraestructura acorde a su criticidad
7. Implementar los controles de seguridad digital de forma eficiente.

“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”

8. Establecer e implementar los principios, lineamientos y estrategias para promover una cultura para la seguridad digital y de la información que incluya actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y terceros que esta considere relevantes para mejorar habilidades y promover conciencia en la seguridad de la información. Estas actividades deben realizarse anualmente y pueden incluirse, adicionalmente, en el plan institucional de capacitaciones PIC.
9. La estrategia debe incluir todas las tecnologías de la información y las comunicaciones que utiliza la organización, incluida la adopción de nuevas tecnologías o tecnologías emergentes y de conformidad con su disponibilidad presupuestaria.

Parágrafo 1. Los sujetos obligados deben adoptar el modelo de seguridad y privacidad señalado en el Anexo 1 de la presente resolución, como habilitador de la política de Gobierno Digital.

Parágrafo 2. El modelo de seguridad y privacidad será actualizado cuando así lo determine la Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones a través de las sucesivas versiones de cada uno de dichos documentos y previo informe del equipo técnico.

ARTÍCULO 6. *La gestión de la seguridad de la información, seguridad digital y la gestión de riesgos de la entidad.* Los sujetos obligados deben determinar e implementar controles para mitigar los riesgos que pudieran afectar la seguridad de digital y física de acuerdo con el resultado del análisis y evaluación de riesgos y cumplir con las siguientes características y responsabilidades:

1. Definir controles considerando aspectos tales como la estructura, tamaño, canales de atención, volumen transaccional, número de usuarios, evaluación del riesgo y servicios prestados por la entidad.
2. Realizar una gestión efectiva de la seguridad de la información y la seguridad digital en la entidad.
3. Reportar los resultados del análisis de riesgos y gestión de incidentes al comité institucional de gestión y desempeño o quien haga sus veces.
4. Actualizarse permanentemente y de manera especializada para que esté al tanto de las nuevas modalidades de ciberataques que pudieran llegar a afectar a la entidad, según las políticas que establezca la entidad de acuerdo con su evaluación de riesgo y atendiendo criterios de razonabilidad.
5. Proponer las capacitaciones que recibirán los funcionarios de la entidad en temas relacionados con seguridad digital y mantenerlos actualizados sobre las nuevas amenazas cibernéticas.
6. Ser la principal responsable en el monitoreo del cumplimiento de las políticas y procedimientos que se establezcan en materia de seguridad digital y sin perjuicio de aquellas tareas que realizan las autoridades de control.
7. Asesorar a la dirección de la entidad sobre seguridad de la información y seguridad digital para que pueda hacer seguimiento y tomar las decisiones adecuadas en esta materia.

“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”

8. Realizar análisis de riesgo para determinar la pertinencia de contratar o implementar el servicio de un equipo especializado para atender incidentes de seguridad digital. El análisis debe identificar las características del proveedor, herramientas, servicios y privacidad de la información, entre otros.
9. Determinar los recursos técnicos, humanos y administrativos de seguridad de la información y seguridad digital, necesarios para la entidad. Dichos recursos deben manejarse de manera diferenciada a los de operaciones y tecnología de la información.
10. Cumplir los lineamientos de gestión del riesgo establecidos en la guía para la administración del riesgo y el diseño de controles en entidades públicas expedida en el marco del modelo integrado de planeación y gestión.

ARTÍCULO 7. Operaciones seguras. Los sujetos obligados deben implementar mecanismos de gestión y monitoreo que protejan la infraestructura de amenazas físicas y digitales.

ARTÍCULO 8. Controles e interoperabilidad. Los sujetos obligados deben implementar controles y procesos que habiliten la integración al servicio ciudadano digital de interoperabilidad de forma segura y cumpliendo de los lineamientos dados sobre el particular en el marco de la política de gobierno digital.

ARTÍCULO 9. Gestión de incidentes de seguridad digital. Los sujetos obligados deben establecer un proceso adecuado y una estrategia de comunicación e información ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Cibernética) de Gobierno de incidentes de seguridad digital que contemple, como mínimo, sin perjuicio de las obligaciones de reporte a las autoridades de investigación y control:

1. Reportar la información sobre incidentes que afecten de manera significativa la confidencialidad, integridad o disponibilidad de los procesos de la entidad o infraestructura crítica, a través de los canales de comunicación establecidos por el CSIRT de Gobierno.
2. Documentar los incidentes haciendo uso de los formatos y formularios establecidos por el CSIRT Gobierno, con el fin de conocer las actividades desarrolladas en las fases de la gestión de incidentes.
3. Dar información sobre las medidas adoptadas para recuperar la información que reportarán a los ciudadanos y usuarios de sus servicios.

ARTÍCULO 10. Privacidad de la información. Los sujetos obligados deben definir una estrategia que permita brindar servicios, controles y condiciones de protección de la privacidad de la información de la Entidad y los ciudadanos acorde con lo exigido en la Ley 1581 de 2012 y los decretos reglamentarios.

ARTÍCULO 11. Mecanismos de autenticación. Los sujetos obligados deben emplear mecanismos para la autenticación y segregar las funciones y responsabilidades de los usuarios con privilegios de administrador o que brindan soporte remoto, para mitigar los riesgos de seguridad de la información. Para ello, deberán seguir el modelo de servicios ciudadanos digitales en particular el modelo de autenticación digital.

ARTÍCULO 12. Retención y destrucción final de información. Los sujetos obligados deben establecer procedimientos para la retención y destrucción final de la información digital, para ello deben seguir las normas

“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”

de gestión documental digital dispuestas por el Archivo General de la Nación.

ARTÍCULO 13. Seguridad digital desde el proceso de desarrollo. Los sujetos obligados deben integrar la seguridad digital, dentro del ciclo de vida del desarrollo del software para todos los Sistemas de información, aplicaciones web y móviles, así como cualquier otro sistema que almacene, transmita o presente información, desde las etapas iniciales como el diseño y el levantamiento de requerimientos, hasta las pruebas de seguridad una vez el software se encuentre en producción, teniendo en cuenta los riesgos asociados a cada sistema de información. Dicho proceso deberá quedar documentado y estar alineado con las normas de responsabilidad demostrada en el tratamiento de datos personales señaladas en el Decreto 1074 de 2015.

ARTÍCULO 14. Terceros, colaboradores y seguridad digital. Los sujetos obligados deben incluir en su estrategia de seguridad digital y su plan de Seguridad y privacidad de la información las medidas y obligaciones pertinentes para la adopción y el cumplimiento de políticas y controles para la gestión de los riesgos de seguridad y privacidad de la información por parte de terceros y colaboradores. .

ARTÍCULO 15. Control de las actividades incluidas en la estrategia de seguridad digital y gestión de riesgos. Los sujetos obligados deben establecer los mecanismos de control al interior de su entidad que permitan verificar el cumplimiento de las disposiciones establecidas en su política de seguridad digital, realizando auditorías de seguridad de la información al menos una vez al año, que contemplen aspectos técnicos de la seguridad digital como análisis de vulnerabilidades a sistemas de información críticos, entre otros.

Así mismo, deben contar con indicadores para medir la eficacia y eficiencia de la gestión de la seguridad de la información y la seguridad digital.

ARTÍCULO 16. Seguridad digital y responsabilidad. Los sujetos obligados deben incluir en su estrategia de seguridad digital los elementos de valoración que se requerirán para determinar la conveniencia de contar con un seguro que cubra los costos asociados a ataques cibernéticos.

ARTÍCULO 17. Etapas de la estrategia de seguridad digital y gestión de incidentes de seguridad digital. Los sujetos obligados deben incluir en su estrategia de seguridad digital las actividades a realizar en las etapas de prevención; protección y detección; respuesta y comunicación; recuperación y aprendizaje, de conformidad con lo indicado a continuación:

1. Prevención

La función de prevención admite la capacidad de limitar o contener el impacto de un posible incidente de ciberseguridad. En esta etapa, los sujetos obligados deben cuando menos:

- 1.1. Establecer, mantener y documentar los controles de acceso (lógicos, físicos y procedimentales), protección de infraestructura y gestión de identidades, privacidad y protección de la información.
- 1.2. Adoptar políticas, procedimientos y mecanismos para evitar la fuga de datos e información.
- 1.3. Gestionar y documentar la seguridad de la plataforma tecnológica.
- 1.4. Contar con los recursos tecnológicos necesarios para realizar una adecuada gestión de seguridad de la información y la ciberseguridad.

“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”

- 1.5. Identificar y gestionar los riesgos que puedan llegar a afectar a la entidad y establecer controles para su mitigación.
- 1.6. Considerar dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques de seguridad de la información.
- 1.7. Realizar pruebas del plan de continuidad del negocio que simulen la materialización de ataques de seguridad de la información.
- 1.8. Determinar la necesidad de contar con herramientas o servicios que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad, entre otros, SIEM (Gestión de eventos de información de seguridad) o SOC (Centro de operaciones de seguridad).
- 1.9. De acuerdo con la estructura, infraestructura, canales de atención, volumen transaccional y número de clientes, monitorear diferentes fuentes de información institucionales oficiales tales como sistemas de información, infraestructuras críticas, correos electrónicos, sitios web, blogs, dispositivos y perfiles oficiales de redes sociales con el propósito de identificar posibles ataques cibernéticos contra la entidad.
- 1.10. Colaborar y articular con las autoridades que hacen parte del modelo nacional de gestión de ciberseguridad en los proyectos que se adelanten con el propósito de fortalecer la gestión de la ciberseguridad a nivel nacional.

2. Protección y detección

La función de protección y detección permite el descubrimiento oportuno de eventos e incidentes de ciberseguridad y cómo protegerse ante los mismos. Los sujetos obligados deben:

- 2.1 Adoptar procedimientos y mecanismos para identificar y analizar los incidentes de seguridad que se presenten.
- 2.2 Gestionar las vulnerabilidades de aquellas infraestructuras críticas o plataformas que soporten activos de información críticos y que estén expuestos en el ciberespacio.
- 2.3 Realizar un monitoreo continuo a su plataforma tecnológica e infraestructura crítica con el propósito de identificar y predecir comportamientos inusuales que puedan evidenciar ataques contra la entidad.
- 2.4 Implementar tecnologías que permitan a la entidad identificar el origen de los ataques, tipos de ataques, comportamientos y la detección predictiva de amenazas.

3. Respuesta y comunicación

Aún con las medidas de seguridad adoptadas, los sujetos obligados deben desarrollar e implementar planes de respuesta a incidentes de seguridad digital. Para hacerle frente a esta situación los sujetos obligados deben:

“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”

- 3.1 Establecer planes y procedimientos de respuesta a incidentes digitales y de seguridad de la información.
- 3.2 Establecer los procedimientos para reportar, cuando se considere pertinente, al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT) o quien haga sus veces, directamente o a través de CSIRT sectoriales, los incidentes de seguridad digital que requieran de su gestión.
- 3.3 Comunicar a los entes correspondientes después de una fuga o afectación a la privacidad de la información de la entidad o ciudadanos.
- 3.4 Dar un tratamiento adecuado a las evidencias forenses para que las áreas de seguridad digital y las autoridades puedan realizar su identificación, recolección, embalaje y disposición en las investigaciones correspondientes.

4. Recuperación y aprendizaje

Desarrollar e implementar actividades apropiadas para definir y mantener los planes de recuperación, resiliencia y restauración de las infraestructuras críticas, servicios, sistemas de información, procesos o en general de un activo de información que se haya deteriorado debido a un incidente de seguridad digital. Los sujetos obligados deben:

- 4.1 Adoptar los mecanismos necesarios para recuperar los sistemas de información e infraestructuras al estado en que se encontraban antes del ataque de seguridad.
- 4.2 Ajustar sus sistemas de gestión de riesgo y de seguridad de la información como consecuencia de los incidentes presentados, adoptando los controles que resulten pertinentes.
- 4.3 Socializar, cuando la entidad lo considere pertinente, las lecciones aprendidas al interior de la organización y con las entidades de su sector.

ARTÍCULO 18. Vigencia. La presente resolución rige a partir de la fecha de su publicación en el Diario Oficial.


PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá D.C. a los

KAREN ABUDINEN ABUCHAIBE

Ministra de Tecnologías de la Información y las Comunicaciones

Proyectó

Marco Emilio Sánchez – Equipo Dirección Gobierno Digital 
Angela Janeth Cortés Hernández - Equipo Dirección Gobierno Digital 
Danny Alejandro Garzón Aristizábal - Equipo Dirección Gobierno Digital 

Revisó: Juan Carlos Noriega – Asesor Viceministerio de Transformación Digital 

“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”

Aura María Cifuentes – Directora de Gobierno Digital 
Margarita Ricardo – Asesora Asesor Viceministerio de Transformación Digital 
Walid David – Asesor de despacho de la Ministra TIC
Manuel Domingo Abello Álvarez – Director Jurídico MinTIC
Vanessa Gallego –Asesora de despacho de la Ministra TIC
Aprobó: German Rueda – Viceministro de Transformación Digital