MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

RESOLUCIÓN NÚMERO 00500 DE MARZO 10 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"

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, del artículo anteriormente citado, 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.

Por lo anterior, es necesario que MinTIC establezca los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1. *Objeto*. La presente resolución tiene por objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad 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.*** Serán 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 talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital. Las entidades deben contar con políticas, procesos, procedimientos, guías, manuales y formatos para garantizar el cumplimiento al ciclo PHVA del MSPI. En ese sentido, deben adoptar los lineamientos del MSPI, guía de riesgos y gestión de incidentes de seguridad digital que se relacionan en el Anexo 1 de la presente resolución.

Para todos los procesos, trámites, sistemas de información, infraestructura tecnológica e infraestructura critica de los sujetos obligados, se deben adoptar medidas de seguridad eficientes alienadas al MSPI, para prestar servicios de confianza, generando protección de la información de los ciudadanos, gestionando los riesgos y los incidentes de seguridad digital.

ARTÍCULO 4. Sistema de gestión de seguridad de la información y seguridad digital. Los sujetos obligados deben aplicar los modelos, guías, 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 y sus respectivas actualizaciones o modificaciones, al igual que otros marcos de trabajo que defina mejores prácticas en la materia.

ARTÍCULO 5. ***La estrategia de seguridad digital*****.** Los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia se debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue.

El Plan de Seguridad y Privacidad de la Información contempla la protección de la información digital, medios impresos y físicos digitales y no digitales.

La estrategia de seguridad digital debe definirse en la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes de seguridad digital, incorporadas en el Anexo 1 de la presente resolución y estar debidamente articulada al habilitador de seguridad y privacidad de la Política de Gobierno Digital.

Adicionalmente, la estrategia de seguridad digital debe:

1. Ser aprobada a través de un acto administrativo de carácter general.
2. Contar con un análisis y tratamiento de riesgos de seguridad digital e implementar controles que permitan gestionarlos.
3. Establecer los roles y responsabilidades al interior de la entidad asociados a la seguridad digital.
4. 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 ésta 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, o el que haga sus veces.
5. 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.

"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"

6. Aplicar las demás consideraciones que a juicio de la entidad contribuyan a elevar sus estándares de seguridad digital.

Parágrafo 1. Los sujetos obligados deben adoptar el Modelo de Seguridad y Privacidad de la Información – MSPI 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 de la Información – MSPI señalado en el Anexo 1 será actualizado por el MinTIC a través de las sucesivas versiones de cada uno de los documentos que lo componen y previo informe del equipo técnico. La actualización se publicará en la sede electrónica de MinTIC.

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 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. Estar 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. Establecer las capacitaciones que recibirán los funcionarios de la entidad en temas relacionados con seguridad digital y mantenerlos actualizados sobre las nuevas amenazas cibernéticas.

6. Realizar el monitoreo del cumplimiento de las políticas y procedimientos que se establezcan en materia de seguridad de la información 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.

8. Realizar un 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. Implementar y gestionar un Sistema de Gestión de Seguridad de la Información de acuerdo a lo establecido en el Modelo de Seguridad y Privacidad de la Información, que permita gestionar los riesgos de seguridad de la información de la entidad de una manera adecuada y oportuna.
11. 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 TI de amenazas físicas y digitales.

"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 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 procedimiento de gestión de incidentes de seguridad digital, para realizar el tratamiento, investigación y gestión de los incidentes de seguridad digital que se presente en relación con los activos de información de cada proceso, para lo cual deben:

1. Gestionar los incidentes de seguridad digital, según el procedimiento establecido por MinTIC, para lo cual deben crear una bitácora que contenga la descripción de cada una de las actividades desarrolladas en la gestión de estos.
2. Designar dentro de la entidad los responsables de gestionar y dar respuesta a los incidentes de seguridad digital, liderado por el responsable de seguridad digital.
3. Una vez identificado el incidente de seguridad digital se deberá reportar ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno, 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 del CSIRT Gobierno.
4. 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.
5. Los sujetos obligados, 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.

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, deben 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 procesos y procedimientos para la retención y destrucción final de la información digital, para ello seguirán las normas de gestión documental digital dispuestas por el Archivo General de la Nación.

ARTÍCULO 13. ***Seguridad digital desde el proceso de desarrollo de software*****.** 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 la Ley 1581 de 2012, el Decreto 1074 de 2015 y demás normas que las desarrollan, adicionen o modifiquen

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.

"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 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 la entidad que permitan verificar el cumplimiento de las disposiciones establecidas en la política de seguridad de la información que hayan aprobado internamente, realizando auditorias 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, deberán contar con indicadores para medir la eficacia, efectividad y eficiencia de la gestión de la seguridad de la información y la seguridad digital.

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

ARTÍCULO 17. ***Etapas generales de la 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. Como mínimo deberán incorporar:
1. Prevención

La función de prevención admite la capacidad de limitar o contener el impacto de un posible incidente de seguridad digital. 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.

1.5. Identificar, y gestionar los riesgos de seguridad de la información 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.

"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"

1.10. 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:

1.1. Adoptar procedimientos y mecanismos para identificar y analizar los incidentes de seguridad que se presenten.

1.2. Gestionar las vulnerabilidades de aquellas infraestructuras criticas o plataformas que soporten activos de información críticos y que estén expuestos en el ciberespacio.

1.3. Realizar un monitoreo continuo a su plataforma tecnológica e infraestructura critica con el propósito de identificar y predecir comportamientos inusuales que puedan evidenciar ataques contra la entidad.

1.4. Implementar tecnologías que permitan a la Entidad identificar el origen de los ataques, tipos de ataques, comportamientos y la detección predictiva de amenazas.

1.5. Realizar periódicamente auditorias de seguridad de la información tanto para los aspectos de gestión como para los aspectos técnicos, como podrían ser: auditorías internas y externas al modelo de Seguridad y Privacidad de la Información, análisis de vulnerabilidades, Hacking ético, pruebas de penetración a sistemas informático y pruebas de ingeniería social entre otras.

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:

1.1. Establecer planes y procedimientos de respuesta a incidentes digitales y de seguridad de la información.

1.2. Establecer los procedimientos para reportar, cuando se considere pertinente, al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT) o quien haga sus veces, a través del CSIRT sectorial, los incidentes de seguridad Digital que requieran de su gestión.

1.3. Comunicar a las autoridades competentes después de una fuga o afectación a la privacidad de la información de la Entidad o ciudadanos.

1.4. 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:

"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"

1.1. Adoptar los mecanismos necesarios para recuperar los sistemas de información e infraestructuras al estado en que se encontraban antes del ataque de seguridad.
1.2. 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.
1.3. 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

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

Revisó: Juan Carlos Noriega – Asesor

Aura María Cifuentes – Directora de Gobierno Digital VoBo
Andrés Diaz Molina– Oficial de Seguridad y Privacidad de la Información
Margarita Ricardo – Asesora Viceministerio de Transformación Digital
Manuel Domingo Abello Álvarez – Director Jurídico MinTIC
Vanessa Gallego Pelaez –Asesora despacho ministra

Aprobó: German Rueda – Viceministro de Transformación Digital

REGISTRO DE FIRMAS ELECTRONICAS

Resolución número 00500 de 2021

Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20210310-103016-6d25f2-85541215 Creación: 2021-03-10 10:30:16

Estado: Finalizado Finalización: 2021-03-10 10:34:01

Escanee el código para verificación

Firma: Firmante del Acto Administrativo

KAREN CECILIA ABUDINEN ABUCHAIBE

kabudinen@mintic.gov.co
MINISTRA
MINTIC

REPORTE DE TRAZABILIDAD

Resolución número 00500 de 2021

Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20210310-103016-6d25f2-85541215 Creación: 2021-03-10 10:30:16

Estado: Finalizado Finalización: 2021-03-10 10:34:01

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Firma	KAREN CECILIA ABUDINEN ABUCHAIBE kabudinen@mintic.gov.co MINISTRA MINTIC	Aprobado	Env.: 2021-03-10 10:30:16 Lec.: 2021-03-10 10:31:27 Res.: 2021-03-10 10:34:01 IP Res.: 200.91.211.130