812.43.00.1485.19

RESOLUCIÓN No. 1485 DE 2019

Del 28 de Octubre de 2019

"Por la cual se adopta la Política de Gestión de Riesgos de Seguridad Digital para la Empresa de Acueducto, Alcantarillado y Aseo de Yopal EICE-ESP, complemento a la resolución No. 0525 del 18 de mayo de 2018 Política Del Gestión Del Riesgo"

El Gerente de la Empresa de Acueducto, Alcantarillado y Aseo de Yopal, en uso de sus facultades legales, atribuciones estatutarias y en concordancia con la Ley 1474 de 2011.

CONSIDERANDO:

El 6 de marzo de 2014 el Congreso de la República estableció la Ley 1712 por medio de la cual se creó la ley de transparencia y del derecho de acceso a la información pública nacional. Por lo cual se convierte en un derecho constitucional para la personas el poder acceder a la información de carácter público que les permita realizar estudios de tipo estadísticos, científico o que simplemente les permita estar informados. En razón a esto, la Empresa de Acueducto, Alcantarillado y Aseo de Yopal está comprometida con la identificación y clasificación de todo tipo de información que es creada, almacenada, administrada y publicada, permitiendo así dar correcto cumplimiento a lo establecido en esta ley

Por su parte, el Ministerio de Tecnologías de la Información y las Comunicaciones **MINTIC** el 14 de Junio de 2018 estableció el decreto 1008 *"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"* que por medio del uso de tecnologías de la información y las comunicaciones permita lograr una mejor competitividad, proactividad e innovación en la ciudadanía y el Estado, por lo que la EAAAY desempeña un papel importante con la implementación de recursos tecnológicos que le permita alcanzar los propósitos que dispone esta ley, gestionando los riesgos y amenazas que traigan consigo la implementación de nuevas tecnologías de la información o avances tecnológicos.

El EAAAY posee una estructura organizacional con procesos estratégicos, misionales, de Soporte, de verificación y mejora de Gestión que permiten realizar la identificación, tratamiento, monitoreo y revisión de los riesgos de seguridad digital más críticos de la entidad que pueden impactar de manera considerable el desarrollo de funciones y logros de objetivos propuestos. Adicionalmente, se cuenta con distintos sistemas de información y servicios tecnológicos que soportan los procesos y por lo cual es necesario velar por la protección y seguridad de estos activos de información.

En razón a esto, la Gestión De Riesgos De Seguridad Digital se alinean en función de velar por la disponibilidad, confidencialidad e integridad de los datos e información que se encuentran en los Sistemas de Información de la Empresa. Logrando con esto poder atender de forma ágil y oportuna los requerimientos de los funcionarios

Que, en virtud de lo anterior, se hace necesario Adoptar la Política de Gestión de Riesgos de Seguridad Digital en la Empresa de Acueducto, Alcantarillado y Aseo de Yopal EICE-ESP articulado con el MIPG, como complemento a la resolución No. 0525 del 18 de mayo de 2018 "Política Del Gestión Del Riesgo"

En mérito de lo expuesto,

RESUELVE

ARTÍCULO 1. Adoptar la Política de Gestión de Riesgos de Seguridad Digital en la Empresa de Acueducto, Alcantarillado y Aseo de Yopal EICE-ESP, como complemento a la resolución No. 0525 del 18 de mayo de 2018 "Política Del Gestión Del Riesgo"

ARTÍCULO 2. OBJETIVO GENERAL

Establecer un marco de Gestión de Riesgos Digitales a través del cual se mitiguen las vulnerabilidades y amenazas asociados a los activos de información de la Empresa de Acueducto, Alcantarillado y Aseo de Yopal EICE-ESP, con el fin de lograr niveles de aceptación razonable del riesgo en relación con los atributos de disponibilidad, integridad y confidencialidad de la información de la entidad.

ARTÍCULO 3. OBJETIVOS ESPECÍFICOS

- Evaluar y analizar los Riesgos de Seguridad Digital relacionados a los activos de información.
- Identificar las amenazas e impactos de seguridad digital asociadas a los procesos de la Empresa.
- Identificar e implementar controles que atiendan la gestión de riesgos y facilite la toma de decisiones sobre el riesgo residual.
- Definir el plan de tratamiento de Riesgos Digitales en la Empresa.

ARTÍCULO 4. ALCANCE

El alcance del plan de gestión de riesgos de seguridad digital inicia con la definición del contexto estratégico de los riesgos de seguridad digital a los que está expuesta la entidad dando cubrimiento a los procesos estratégicos, misionales, de soporte, de verificación y mejora; y concluye con el plan de acción mediante el cual se realizará el tratamiento, monitoreo y revisión de los riesgos de seguridad digital identificados.

ARTÍCULO 5. DEFINICIÓN DE LA POLÍTICA

Definiciones

Para la adecuada gestión de riesgos de seguridad digital se debe manejar con propiedad los siguientes términos:

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

- **Amenaza:** [Según **ISO 27000**]: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

- **Análisis del riesgo:** [NTC ISO 31000:2011]: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

- **Apetito de riesgo**: Es el nivel máximo de riesgo que la Empresa está dispuesta a asumir.

- **Consecuencia:** [NTC ISO 31000:2011]: Resultado o impacto de un evento que afecta a los objetivos.

- **Controles:** [Según ISO 27000]: 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.

- **CSIRT:** Equipo de Respuesta a Incidentes de Seguridad Informática

- **Criterios del riesgo:** [Según NTC ISO 31000:2011]: Términos de referencia frente a los cuales se evalúa la importancia de un riesgo.

- **Evaluación del riesgo:** [Según NTC ISO 31000:2011]: Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

- **Identificación del riesgo:** [Según NTC ISO 31000:2011]: Proceso para encontrar, reconocer y describir el riesgo.

- **Impacto:** [Según ISO 27000]: El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

- **Inventario de activos:** [Según ISO 27000.ES]: Sigla en inglés: Assets inventory. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos.

- **Nivel de riesgo:** [Según NTC ISO 31000:2011]: Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad.

- **Perfil del riesgo:** [Según NTC ISO 31000:2011]: Descripción de cualquier conjunto de riesgos.

- **Política:** [Según ISO/IEC 27000:2016]: Intenciones y dirección de una organización como las expresa formalmente su alta dirección.

- **Política:** para la gestión del riesgo [Según NTC ISO 31000:2011]: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.

- **Reducción del riesgo:** [Según NTC ISO 31000:2011]: Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo.

- **Riesgo:** [Según ISO 27000]: 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.

- **Riesgo Residual:** [Según ISO 27000]: El riesgo que permanece tras el tratamiento del riesgo.

- **Vulnerabilidad:** [Según ISO 27000]: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

ARTÍCULO 6: PLAN DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

La Empresa siguiendo los lineamiento trazados por el Gobierno Nacional con lo expuesto en la Ley de transparencia 1712 de 2014, la Estrategia Gobierno en Línea y la Política de Gobierno Digital. Establece un plan de gestión de riesgos de seguridad digital en el cual se identifiquen las amenazas, las vulnerabilidades, el impacto y el nivel de riesgo asociados a los activos de información sin importar el nivel de criticidad que tienen para la entidad.

En la gestión de riesgos de seguridad digital resulta importante lograr una aceptación de los riesgos con base en las posibles consecuencias de afectación; establecer una estrategia de mitigación adecuada que logre un entendimiento y aceptación del riesgo residual así como de los recursos empleados en relación costo-beneficio con el fin de emplear medidas para salvaguardar, proteger y custodiar la información de las aplicaciones, servicios tecnológicos, bases de datos, redes de comunicaciones, equipos de cómputo y documentos físicos garantizando la disponibilidad, confidencialidad e integridad de la información.

Por consiguiente, resulta indispensable definir actividades que de manera articulada permitan implementar medidas de control que coadyuven a la prevención, contención y mitigación de amenazas a las que se encuentran expuestos los activos de información de la entidad por medio de una metodología descrita a continuación:

ARTÍCULO 7. IMPLEMENTACIÓN DE LA POLÍTICA

La Política de Gestión de Riesgos de Seguridad Digital, en esta fase se seguirá la ruta definida para la aplicación de controles, los cuales estarán a cargo de su implementación en los tiempos definidos, los responsables o líderes de proceso con el apoyo de la Oficina de Sistemas en lo concerniente a controles tecnológicos e informáticos, también será necesario contar con el apoyo y compromiso del responsable de la seguridad digital que brinde conocimiento, apoyo y experticia en la aplicación de los controles.

ARTÍCULO 8. FASE DE MONITOREO Y REVISIÓN

Dado que el origen y tipos de riesgos son variables, el monitoreo constante será necesario para detectar cambios respecto a nuevos activos de información, nuevos procesos o procedimientos, nuevos factores o amenazas que afecten los activos de información, nuevas vulnerabilidades, incremento del impacto e incluso la materialización de incidentes de seguridad digital.

ARTÍCULO 9. TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DIGITAL

De acuerdo a la valoración de los riesgos de seguridad digital realizada, se determinan las opciones para tratar los riesgos a través de políticas que permitan controlar y hacer seguimiento sobre la gestión realizada a los riesgos con estrategias de tratamiento en donde se tome decisiones para mitigar, retener, transferir o asumir los riesgos. En razón a esto, la formulación de políticas deberán contemplar los objetivos a alcanzar, una estrategia de cómo se desarrollarán las políticas a corto, mediano y largo plazo, indicar qué riesgos se van a priorizar y controlar, estimar los recursos necesario y finalmente hacer seguimiento a la efectividad de las políticas de administración de riesgos de seguridad digital definidas, con el propósito de integrar los objetivos, estrategias, la comunicación, la revisión y ciclo de control de los riesgos a los que se ve expuesta la Empresa

ARTÍCULO 10. RESPONSABLES

El profesional de la Oficina De Sistemas de la Empresa junto con la alta Gerencia serán responsables de la seguridad digital que también será responsable de la seguridad de la información y las responsabilidades que deberá cumplir respecto a la gestión del riesgo de seguridad digital serán las siguientes:

- ✓ Definir el procedimiento para la Identificación y Valoración de Activos.
- ✓ Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).
- ✓ Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.
- ✓ Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.
- ✓ Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

Nota: Como complemento de esta actividad, la Empresa debe tomar como referencia lo definido en la **Guía Roles y responsabilidades del MSPI -**Modelo de Seguridad y Privacidad de la Información- de la Estrategia de Gobierno Digital del MINTIC, en complemento a lo anterior. "http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html Guía # 4 - Roles y Responsabilidades "

ARTÍCULO 11. POLÍTICA DE SEGURIDAD DIGITAL

En materia de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las Empresas

La implementación de la política, se hará a través de la adopción e implementación del Modelo de Gestión de Riesgos de Seguridad Digital, que será desarrollado y socializado por MinTic, por parte de las entidades y departamentos administrativos de la rama ejecutiva inicialmente, para los entes territoriales y demás partes interesadas, se adelantarán jornadas de sensibilización en temas de Seguridad Digital.

La implementación de esta política permite establecer reglas, lineamientos y buenas prácticas que coadyuven a la confidencialidad, seguridad y disponibilidad de la información digital que permita minimizar el riesgo de pérdida de datos, accesos no autorizados, divulgación no controlada, y duplicación e interrupción intencional de la información.

El desarrollo de las estrategias de la Política de Seguridad Digital buscan contrarrestar el incremento de las amenazas informáticas que pueden afectar significativamente la Empresa y el correcto desarrollo normativo y legal de las mismas fortaleciendo la institucionalidad de la entidad.

ARTÍCULO 12. SEGUIMIENTO

La oficina de control interno de gestión realizará seguimiento periódico a la implementación de la política. Igualmente de identificar las acciones de mejora necesarias para lograr una efectiva gestión de riesgos de seguridad digital y permita esto salvaguardar los activos de información de la Empresa.

ARTÍCULO 13. DIVULGACIÓN DE LA POLÍTICA

La Política de Gestión de Riesgos de Seguridad Digital en la Empresa de Acueducto, Alcantarillado y Aseo de Yopal EICE-ESP, se divulgarán a todos los trabajadores de la Empresa EAAAY EICE-ESP" y comunidad en general a través de la página web www.eaaay.gov.co, Redes Sociales, Correos Institucionales, QFDocument y charlas presenciales.

COMUNIQUESE Y CUMPLASE

Dada en Yopal, veintiocho (28) día del mes de octubre de 2019.

YAHAIRA INDIRA DE JESUS DIAZ QUESADA
Gerente – EAAAY EICE - ESP

Revisó: Miguel Ángel Castiblanco // Asesor Jurídico

Elaboró: Cesar Barrera // Profesional Oficina Sistemas

Adriana Cristina Rosas Valderrama // Profesional Planeación