

- 2.1.9 Carta de la designación del Auditor Interno del grupo significativo de ciudadanos, junto con la carta de aceptación suscrita por el responsable encargado de rendir los informes.
- 2.2 Segunda Carpeta:
- 2.2.1 Copia del Formulario individual 5B y anexos con contenido contable
- 2.2.2 Carta de designación del Contador de Campaña, junto con la carta de aceptación suscrita por el candidato
- 2.2.3 Carta de designación del Gerente de Campaña, junto con la carta de aceptación suscrita por el candidato –cuando hubiere lugar–
- 2.2.4 Soportes contables originales, organizados por fecha y consecutivo
- 2.2.5 Libro de ingresos y gastos de campaña
- 2.2.6 Nota: Se deberán registrar hojas continuas como libro ante la Organización Electoral, en estas hojas se debe imprimir exclusivamente el libro contable del aplicativo “Cuentas Claras”.

Parágrafo 1°. Los movimientos sociales que postulen candidatos a las circunscripciones especiales correspondientes, deberán sujetarse a los lineamientos establecidos en el artículo 25 de la Ley 1475 de 2011, en tanto a saber que, los candidatos están obligados a rendir el informe de ingresos y gastos de campaña dentro del mes inmediatamente siguiente a la contienda electoral, y a su turno, el movimiento que los inscribió será responsable ante el Consejo Nacional Electoral de presentar el informe consolidado dentro de los dos (2) meses siguientes al certamen electoral.

Parágrafo 2°. Las candidaturas que se postulen a través de coalición, deberán indicar expresamente el responsable designado para la presentación de los informes consolidados ante el Consejo Nacional Electoral, sin perjuicio de las consecuencias sancionatorias para los grupos políticos que integren a la coalición que no acaten en debida forma los postulados contenidos en el artículo 25 de la Ley 1475 de 2011.

Artículo 5°. *Requerimiento para la subsanación de informes.* De conformidad con el inciso primero del artículo décimo segundo de la Resolución número 0330 de 2007, el contador a cargo realizará el requerimiento correspondiente respecto del informe presentado en el que se evidencien inconsistencias o carencias de documentación necesarias para su certificación. El requerimiento se realizará por una única vez, y se comunicará a las direcciones físicas y electrónicas de los partidos y movimientos políticos registradas ante esta Corporación, y, a su turno, a los grupos significativos de ciudadanos.

Artículo 6°. *Términos para la subsanación.* Los partidos y movimientos políticos y grupos significativos de ciudadanos, tendrán un término de dos (2) meses contados a partir del día siguiente de la comunicación del requerimiento para su efectiva contestación, la cual deberá atender a cabalidad las indicaciones realizadas por esta Corporación.

Artículo 7°. *Archivo de los informes.* Los informes que no cumplan con el lleno de los requisitos contemplados en la Resolución número 0330 de 2007, serán archivados previo examen del Fondo Nacional de Financiación Política.

Parágrafo 1°. Las sustentaciones extemporáneas y las que no cumplan con la documentación solicitada en el requerimiento de subsanación, se desestimarán y se ordenará su archivo inmediato, de acuerdo con lo expuesto en los acápites considerativos del presente acto administrativo.

Parágrafo 2°. Para los informes de ingresos y gastos de campaña que han sido oficiados y no han presentado respuesta al requerimiento de subsanación hasta el momento de la expedición de la presente resolución, tendrán un término de seis (6) meses contados a partir de la misma para cumplir con los requisitos exigidos, *so pena* de la aplicación de los efectos contemplados en el presente artículo.

Parágrafo 3°. Para los informes de ingresos y gastos de campaña generados a raíz de pasadas contiendas electorales que no hayan sido oficiados, se aplicarán los términos del parágrafo primero e inciso primero del presente artículo.

Artículo 8°. *Reporte sobre la destinación de los recursos provenientes de la reposición de gastos.* Una vez efectuado el desembolso de los dineros certificados a través de resolución concernientes a la reposición de votos por gastos de campaña, las agrupaciones políticas tendrán un término de tres (3) meses para rendir informe detallado de la distribución de los recursos asignados con sus debidos soportes, *so pena* de las sanciones contempladas en el artículo 12 de la Ley 1475 de 2011, referente al incumplimiento grave de los deberes de diligencia en la aplicación de las disposiciones constitucionales o legales que regulan la organización, funcionamiento y financiación.

Artículo 9°. *Vigencia.* La presente resolución rige a partir de su publicación y deroga en su integridad el inciso 2° del artículo décimo segundo de la Resolución número 0330 de 2007 y todas las disposiciones que les sean contrarias.

Comuníquese y cúmplase.

Dada en Bogotá, D. C., a 21 de agosto de 2019.

El Presidente R.,

César Augusto Abreo Méndez.
(C. F.).

Jurisdicción Especial para la Paz

ACUERDOS

ACUERDO AOG NÚMERO 045 DE 2019

(septiembre 10)

por el cual se adopta la Política de Seguridad y Privacidad de la Información.

El Órgano de Gobierno de la Jurisdicción Especial para la Paz, Jurisdicción especial para la Paz, en ejercicio de sus facultades constitucionales, legales y reglamentarias, en especial el parágrafo 2° del artículo transitorio 5 del Acto Legislativo 01 de 2017, precisado en sus alcances por la Corte Constitucional en Sentencia C-674 de 2017, la Ley 1922 del 18 de julio de 2018, la Ley 1957 de 2019, el artículo 12 del Reglamento General de la Jurisdicción Especial para la Paz, y

CONSIDERANDO:

Que el artículo 5° transitorio del Acto Legislativo 01 del 2017, que creó la Jurisdicción Especial para la Paz, con autonomía administrativa, presupuestal y técnica, señala que la Jurisdicción Especial para la Paz estará sujeta a un régimen legal propio y se encargará de administrar justicia de manera transitoria y autónoma, con conocimiento preferente sobre las demás jurisdicciones.

Que el artículo 15 del Acto Legislativo 01 del 2017 estipula que la Jurisdicción Especial para la Paz “(...) entrará en funcionamiento a partir de la aprobación de este Acto Legislativo sin necesidad de ninguna norma de desarrollo, sin perjuicio de la aprobación posterior de las normas de procedimiento y lo que establezca el reglamento de dicha jurisdicción (...)”.

Que mediante, el Acuerdo 001 del 9 de marzo de 2018, proferido por la Plenaria de la Jurisdicción Especial para la Paz adoptó su Reglamento General. En el mismo se estableció que el Órgano de Gobierno de la Jurisdicción Especial para la Paz tendría como funciones las señaladas en la Constitución, la ley estatutaria de la Jurisdicción Especial para la Paz, la ley de procedimiento de la Jurisdicción Especial para la Paz, la ley y las referidas en el artículo 12 de ese reglamento.

Que el artículo 12 del Reglamento General de la Jurisdicción Especial para la Paz establece que le corresponde al Órgano de Gobierno de la Jurisdicción Especial para la Paz, definir las políticas públicas, los lineamientos y criterios generales necesarios para su funcionamiento y regular los trámites administrativos que se adelanten en la Jurisdicción Especial para la Paz.

Que el artículo 110 de la Ley 1957 del 6 de junio de 2019 “*Estatutaria de la Administración de justicia en la jurisdicción Especial para la Paz*”, establece que “*En tanto los magistrados de la JEP no definan una instancia de Gobierno conforme a lo previsto en el parágrafo 2° del artículo transitorio 5 del Acto Legislativo 01 de 2017, la JEP tendrá un Órgano de Gobierno cuyo objeto será el establecimiento de los objetivos, planificación, orientación de la acción y fijación de estrategia general de la Jurisdicción. De tal forma, se enfocará en la toma de decisiones de planeación, diseño y/o mejoramiento organizacional, definición de herramientas, lineamientos y criterios generales necesarios para el funcionamiento, así como la definición de políticas públicas que involucren a la jurisdicción*”. Que asimismo, el numeral 1 del referenciado artículo señala que es función del Órgano de Gobierno: “*Establecer las políticas generales de Gobierno de la JEP*”.

Que el numeral 13 del artículo 112 de la mencionada Ley Estatutaria establece como funciones de la Secretaría Ejecutiva:

“13. *Proponer al Órgano de Gobierno las políticas, programas, normas y procedimientos para la administración del talento humano, seguridad del personal, gestión documental, gestión de la información, recursos físicos, tecnológicos y financieros de la JEP, así como asegurar su ejecución.*

17. *Elaborar y coordinar la ejecución de los Planes Estratégico, Cuatrienal y de Acción Anual, así como las demás propuestas de políticas, planes y programas para someterlos al Órgano de Gobierno para su aprobación*”.

Que el artículo 116 de la Ley 1957 del 6 de junio de 2019 “*Estatutaria de la Administración de Justicia en la Jurisdicción Especial para la Paz*”, establece que la Secretaría Ejecutiva tendrá una dependencia encargada de los procesos y procedimientos relacionados con la Gestión Documental, el manejo del archivo de la JEP y la memoria judicial, que garantice la conservación y la seguridad de la información y que cumpla con los principios rectores de la ley de archivo.

Que la Ley Estatutaria 1581 de 2012 establece las disposiciones generales para la protección de datos personales en desarrollo de los derechos constitucionales previstos en los artículos 15 y 20 de la Constitución Política, y su relación con la Seguridad de la Información se encuentra definido en los principios de Seguridad y Confidencialidad¹.

Que el artículo 20 de la Ley 1922 de 2018 establece que en las Salas y Secciones de la Jurisdicción Especial para la Paz se podrán adoptar medidas, con el fin de proteger y preservar la información que obre en archivos públicos o privados.

¹ Artículo 4° Ley 1581 de 2012, “por la cual se dictan disposiciones generales para la protección de datos personales”.

Que el numeral 8 del artículo 2° de la Ley 1341 de 2009 establece que el Gobierno nacional fijará los mecanismos y condiciones para garantizar la masificación del Gobierno en Línea, con el fin de lograr la prestación de servicios eficientes a los ciudadanos.

Que el artículo 2.2.9.1.1.1 del Decreto 1008 de 2018 establece lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual debe ser entendida como: el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.

Que el artículo 2.2.9.1.1.3. del Decreto 1008 de 2018, establece los principios de la política de Gobierno digital que rigen la función y los procedimientos administrativos consagrados en los artículos 209 de la Constitución Política, 3 de la Ley 489 de 1998, 3 de la Ley 1437 de 2011, 2 y 3 de la Ley 1712 de 2014, así como los que orientan el sector TIC de acuerdo con el artículo 2 de la Ley 1341 de 2009. En particular el principio de Seguridad de la Información se entiende como aquel que busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

Que el Conpes 3854 de 2016 establece la Política Nacional de Seguridad Digital para Colombia, y contempla la defensa y seguridad nacional en el entorno digital, por lo cual las entidades deben incorporar y adoptar las mejores prácticas internacionales en gestión de riesgos digitales, además de los lineamientos y directrices de seguridad digital.

Que la Ley Estatutaria 1712 de 2014 “por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones” establece la clasificación de la información en pública, pública clasificada y pública reservada.

En mérito de lo expuesto,

ACUERDAN:

Artículo 1°. Adoptar la Política de Seguridad y Privacidad de la Información de la Jurisdicción Especial para la Paz, cuyo documento técnico se anexa y forma parte integral del presente acuerdo.

Artículo 2°. Este acuerdo rige a partir de su publicación.

Publíquese y cúmplase,

Dado en Bogotá D. C., a 10 de septiembre de 2019.

La Presidenta, Jurisdicción Especial Para la Paz,

Patricia Linares Prieto.

La Magistrada Sección de Apelación,

Ausente con excusa.

Sandra Rocío Gamboa Rubiano.

El Magistrado, Sección de Revisión de Sentencias,

Adolfo Murillo Granados.

La Magistrada, Sección de Ausencia de Reconocimiento de Verdad y Responsabilidad,

Reinere de los Ángeles Jaramillo Chaverra.

El Magistrado, Sección de Reconocimiento de Verdad y Responsabilidad,

Camilo Suárez Aldana.

Sala de Reconocimiento de Verdad, de Responsabilidad y de Determinación de los Hechos y Conductas,

Ausente con excusa.

Catalina Díaz Gómez.

El Magistrado Sala de Definición de Situaciones Jurídicas,

Mauricio García Cadena.

El Magistrado Sala de Amnistía o Indulto,

Juan José Cantillo Pushaina.

El Director Unidad de Investigación y Acusación

Giovanni Álvarez Santoyo.

La Secretaria Ejecutiva,

María del Pilar Bahamón Falla.

ACUERDO AOG NÚMERO 045 DE 2019

En ejercicio de sus facultades constitucionales, legales y reglamentarias, en especial el parágrafo 2° del artículo transitorio 5 del Acto Legislativo 01 de 2017, precisado en sus alcances por la Corte Constitucional en Sentencia C-674 de 2017, Ley 1922 de julio de 2018, el artículo 12 del Reglamento General de la Jurisdicción Especial para

la Paz, mediante Acuerdo AOG número 045 del 10 de septiembre de 2019, el Órgano de Gobierno de la Jurisdicción Especial para la Paz - Jurisdicción Especial para la Paz adoptó la presente:

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CAPÍTULO PRIMERO

Disposiciones generales

Artículo 1°. *Objeto.* El objeto de la Política de Seguridad y Privacidad es la protección de la confidencialidad, integridad, disponibilidad y continuidad de la información de la Jurisdicción Especial para la Paz - Jurisdicción Especial para la Paz.

Artículo 2°. *Ámbito de aplicación.* Las disposiciones de esta Política serán aplicables a los siguientes grupos de interés de la Jurisdicción Especial para la Paz, en tanto sean usuarios con acceso a la información de la Entidad:

- a) Víctimas.
- b) Comparecientes de la exguerrilla de las Farc.
- c) Comparecientes de la Fuerza Pública.
- d) Comparecientes agentes del Estado.
- e) Comparecientes protesta social.
- f) Comparecientes terceros civiles.
- g) Público general.
- h) Servidores públicos de la Jurisdicción Especial para la Paz.
- i) Contratistas.
- j) Comunidad internacional.
- k) Entidades concernidas.
- l) Medios de comunicación.
- m) Otras entidades del Estado.

Artículo 3°. *Definiciones.*

- a) Activo de información: Es todo aquello que posee valor para la organización².
- b) Comparecientes de la exguerrilla de las Farc: Son titulares de derechos en la Jurisdicción Especial para la Paz y se refiere a las personas excombatientes de las Farc³.
- c) Comparecientes de la Fuerza Pública: Son titulares de derechos en la Jurisdicción Especial para la Paz y se refiere a los miembros de la fuerza pública que han comparecido a la Jurisdicción Especial para la Paz⁴.
- d) Comparecientes agentes del Estado: Son titulares de derechos en la Jurisdicción Especial para la Paz y se refiere a los Agentes del Estado que han comparecido a la Jurisdicción Especial para la Paz⁵.
- e) Comparecientes terceros civiles: Son titulares de derechos en la Jurisdicción Especial para la Paz y se refiere a las personas que, sin formar parte de las organizaciones o grupos armados, hubieren contribuido de manera directa o indirecta a la comisión de delitos en el marco del conflicto, y se acojan o soliciten acogerse a la Jurisdicción Especial para la Paz⁶.
- f) Comparecientes protesta social: Son titulares de derechos en la Jurisdicción Especial para la Paz y se refiere a las personas que han comparecido a la Jurisdicción Especial para la Paz por conductas de protesta social⁷.
- g) Comunidad internacional: Son los Estados, organismos internacionales y multilaterales y agencias de cooperación⁸.
- h) Confidencialidad: Propiedad de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados⁹.
- i) Control: Medios de gestión de riesgos, incluye políticas, procedimientos, directrices, prácticas o estructuras organizativas que pueden ser de naturaleza administrativa, técnica o legal¹⁰.
- j) Contratista: Para la Jurisdicción Especial para la Paz pueden ser internos (personas naturales) y externos (personas jurídicas) y se refiere al que toma a su cargo, la ejecución de alguna actividad.
- k) Disponibilidad: Propiedad de ser accesible y utilizable ha pedido por una entidad autorizada¹¹.

² NTC- ISO-IEC 27001:2013.

³ Acuerdo 017 del 12 de marzo de 2019.

⁴ Acuerdo 017 del 12 de marzo de 2019.

⁵ Acuerdo 017 del 12 de marzo de 2019.

⁶ Acuerdo 017 del 12 de marzo de 2019.

⁷ Acuerdo 017 del 12 de marzo de 2019.

⁸ Acuerdo 017 del 12 de marzo de 2019.

⁹ NTC- ISO-IEC 27001:2013.

¹⁰ NTC-ISO-IEC 27001:2013.

¹¹ NTC-ISO-IEC 27001:2013.

- l) Entidades concernidas: Entidades públicas del SIVJNR (Sistema Integral de Verdad, Justicia, Reparación y No Repetición, del SNARIV (Sistema Nacional de Atención y Reparación Integral a las Víctimas) y otras entidades que se vinculan en el cumplimiento de las funciones de la Jurisdicción Especial para la Paz¹².
- m) Evento de Seguridad de la Información: Ocurrencia identificada de un sistema, servicio o estado de la red que indica un posible incumplimiento de la política de seguridad de la información o el incumplimiento de las salvaguardas, o una situación desconocida que puede ser relevante para la seguridad¹³.
- n) Incidente de Seguridad de la Información: Uno o una serie de eventos de Seguridad de la Información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la Seguridad de la Información¹⁴.
- o) Información: Datos relacionados que tienen significado para la entidad. La información es un activo esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada¹⁵.
- p) Información pública: En los términos de la Ley 1712 de 2014 y aquella que la modifique, complemente, suprima o sustituya, toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.
- q) Información pública clasificada: En los términos de la Ley 1712 de 2014 y aquella que la modifique, complemente, suprima o sustituya, es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 del 2014.
- r) Información pública reservada: En los términos de la Ley 1712 de 2014 y aquella que la modifique, complemente, suprima o sustituya, es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo de esta ley.
- s) Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos¹⁶.
- t) Manual del Sistema de Seguridad y Privacidad de la Información: Documento definido por el Comité de Seguridad de la Información el cual reúne en forma general todos los elementos requeridos y su interacción para la implementación del SGSPI, con base en la Norma ISO 27001:2013.
- u) Partes interesadas: Personas u organizaciones que están involucradas con el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), para la Jurisdicción Especial para la Paz corresponden a los mismos grupos de interés.
- v) Público general: Grupo de interés al que corresponde la sociedad colombiana¹⁷.
- w) Riesgo: Efecto de la incertidumbre sobre los objetivos¹⁸.
- x) Riesgo residual: Riesgo restante después del tratamiento de riesgo¹⁹.
- y) Seguridad de la información: Preservación de confidencialidad, integridad y disponibilidad de la información²⁰.
- z) Servidores públicos: Persona con una vinculación laboral al Estado, que ejerce funciones públicas que están al servicio del Estado y de la comunidad²¹.
- aa) Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI): Consiste en políticas, procedimientos, pautas, recursos y actividades administrados colectivamente por la Jurisdicción Especial para la Paz, en la búsqueda de proteger sus activos de información²².
- bb) Víctimas: Son titulares de derechos en la Jurisdicción Especial para la Paz y se refiere a aquellos que, individual o colectivamente, sufrieron daños como consecuencia de las acciones u omisiones presentadas en el marco del conflicto armado.

¹² Acuerdo 017 del 12 de marzo de 2019.

¹³ NTC-ISO-IEC 27001:2013.

¹⁴ NTC-ISO-IEC 27001-1:2013.

¹⁵ Modelo de Seguridad y Privacidad de la Información.

¹⁶ NTC-ISO-IEC 27001:2013.

¹⁷ Acuerdo 017 del 12 de marzo de 2019.

¹⁸ ISO 31000.

¹⁹ ISO 31000.

²⁰ NTC-ISO-IEC 27001:2013.

²¹ Departamento Administrativo de la Función Pública. Glosario. En: <https://www.fimcionpublica.gov.co/>

²² NTC-ISO-IEC 27001:2013.

Artículo 4°. *Alcance del SGSPI*. El alcance del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), son los activos de información requeridos para el adecuado funcionamiento de todos los procesos de la Jurisdicción Especial para la Paz, en la sede central, grupos territoriales y en las demás que en el futuro se establezcan.

Artículo 5°. *Principios*. El cumplimiento de la Política de Seguridad y Privacidad de la Información se regirá conforme a los siguientes principios:

- 5.1. Principio de confidencialidad: La Jurisdicción Especial para la Paz asegurará la confidencialidad de la información generada, procesada y resguardada en el ejercicio de la información gestionada por la Jurisdicción Especial para la Paz.
- 5.2. Principio de integridad: La Jurisdicción Especial para la Paz protegerá la integridad de la información creada, procesada, transmitida y resguardada, en el ejercicio de las funciones realizadas en la Jurisdicción Especial para la Paz.
- 5.3. Principio de disponibilidad: La Jurisdicción Especial para la Paz propenderá por la disponibilidad de la información gestionada.
- 5.4. Principio de la continuidad de la información: La Jurisdicción Especial para la Paz propenderá por la continuidad de los servicios de procesamiento de información, infraestructura tecnológica, instalaciones físicas, bienes y personal requerido, con el fin de asegurar la continuidad de la operación.

CAPÍTULO SEGUNDO

Disposiciones específicas

Artículo 6°. *Política de Seguridad y Privacidad de la Información*. La Jurisdicción Especial para la Paz se compromete a preservar la confidencialidad, integridad y disponibilidad de su información, mediante la formulación de objetivos, definición de lineamientos, procedimientos, protocolos y controles con el propósito de gestionar de manera efectiva los activos de información y los riesgos de estos en el marco de su misión institucional. Igualmente, fomentará la formación de una cultura de seguridad y privacidad de la información, el cumplimiento del marco normativo vigente en esta materia y velará por la asignación de los recursos necesarios para la implementación de la política y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI).

Artículo 7°. *Alcance del SGSPI*. El alcance del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), son los activos de información requeridos para el adecuado funcionamiento de todos los procesos de la Jurisdicción Especial para la Paz, en la sede central, grupos territoriales y en las demás que en el futuro se establezcan.

Artículo 8°. *Objetivos de Seguridad de la Información*. Son objetivos de la Política de Seguridad y Privacidad de la Información los siguientes:

- 8.1. Asegurar la confidencialidad, integridad, disponibilidad y continuidad de los activos de información, mediante la gestión de los Riesgos de Seguridad de la Información.
- 8.2. Promover una cultura de Seguridad de la Información en los funcionarios, contratistas y demás personas vinculadas a la Jurisdicción Especial para la Paz, a través de la implementación de programas de capacitación y sensibilización.
- 8.3. Asegurar el mejoramiento continuo del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) mediante la implementación de acciones correctivas, de mejora y planes de acción.
- 8.4. Mitigar el impacto de la materialización de los incidentes y riesgos de Seguridad de la Información.

Artículo 9°. *Políticas complementarias*. La Secretaría Ejecutiva de la Jurisdicción Especial para la Paz adoptará el Manual del Sistema de Seguridad y Privacidad de la Información (SGSPI), el cual contendrá las Políticas Complementarias incorporadas dentro la norma Norma NTC-ISO-IEC 27001:2013 y los lineamientos de Gobierno Digital, a saber:

- 9.1. Política para dispositivos móviles: Conjunto de controles y medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
- 9.2. Política de teletrabajo: Conjunto de controles y medidas de seguridad de soporte, para proteger la información a la cual se accede, se procesa o almacenada en los lugares en los que se realiza el teletrabajo.
- 9.3. Política de control de acceso: Conjunto de controles y medidas de seguridad de acceso físico y lógico a la información de la Jurisdicción Especial para la Paz.
- 9.4. Política sobre el uso de controles criptográficos: Conjunto de controles y medidas sobre el uso de controles criptográficos para la protección de la información, a través del cifrado de mensajes.
- 9.5. Política de gestión de llaves criptográficas: Conjunto de controles y medidas de seguridad sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.

- 9.6. Política de escritorio limpio y pantalla limpia: Conjunto de controles y medidas para proteger la información dispuesta en el escritorio físico y lógico y medios de almacenamiento removibles en las instalaciones de procesamiento de información.
- 9.7. Política de respaldo de información: Conjunto de controles y medidas sobre copias de respaldo de la información, software e imágenes de los sistemas, y sobre las pruebas de las copias de respaldo.
- 9.8. Políticas y procedimientos de transferencia de información: Conjunto de controles y medidas de seguridad de transferencia formales de información.
- 9.9. Política de desarrollo seguro: Conjunto de controles y medidas de seguridad para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
- 9.10. Política de Seguridad de la Información para las relaciones con proveedores: Conjunto de controles y medidas de seguridad para mitigar los riesgos asociados con el acceso de proveedores a los activos de la Entidad.
- 9.11. Política de no repudio: Conjunto de controles y medidas para evitar el no repudio de las partes interesadas con acceso a la información.
- 9.12. Política de gestión de incidentes de Seguridad de la Información: Conjunto de controles y medidas sobre la gestión de eventos, incidentes y vulnerabilidades de Seguridad de la Información.
- 9.13. Política de gestión de activos de información: Conjunto de controles y medidas que sobre identificación, clasificación, etiquetado, tratamiento, devolución, y eliminación segura de los activos de información de cada proceso de la Jurisdicción Especial para la Paz.
- 9.14. Política de capacitación y sensibilización en Seguridad de la Información: Conjunto de controles y medidas sobre la formación y concienciación del personal en temas relacionados con la Seguridad de la Información.

Artículo 10. *Roles y Responsabilidades del Sistema de Gestión de Seguridad y Privacidad de Información (SGSPI)*. Los siguientes roles y responsabilidades de Seguridad de la Información deben ser inherentes a los cargos desempeñados por los servidores y las actividades realizadas por los contratistas y se deben relacionar con las funciones esenciales descritas en el Manual Específico de Funciones y Competencias Laborales de la Jurisdicción Especial para la Paz.

- 10.1. Órgano de Gobierno. Para el Sistema de Gestión de Seguridad y Privacidad de Información (SGSPI), es el encargado de la aprobación de la Política General de Seguridad de la Información.
- 10.2. Secretaría Ejecutiva. Es la encargada de la formulación y presentación para aprobación por parte del Órgano de Gobierno, de la Política General de Seguridad de la Información.
- 10.3. Comité de Seguridad de la Información de la JEP. Es el responsable del seguimiento de la aplicación de la Política de Seguridad de la Información para el SGSPI, dentro del Comité de Gestión para la Administración de Justicia de la JEP.
- 10.4. Dirección de Tecnologías de la Información. A cargo de la planeación, coordinación y administración del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI).
- 10.5. Oficial de Seguridad de la Información. Le corresponde apoyar las responsabilidades de la Dirección de TI en esta materia y hará las veces de secretario del Comité de Seguridad de la Información en la Entidad.
- 10.6. Comité de Seguridad Informática de la Jurisdicción Especial para la Paz. Este comité estará integrado por los miembros del Comité de Seguridad Informática y este mismo aprobará el Manual de SGSPI en el cual se definirán los roles y responsabilidades de los funcionarios y contratistas en Seguridad de la Información para el SGSPI.
- 10.7. El Oficial de Seguridad de la Información. El Oficial de Seguridad de la Información, deberá realizar la planeación, coordinación y administración del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) además hará las veces de Secretariado del Comité de Seguridad de la Información en la Entidad:
 - a) Asegurar que el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) opere de conformidad con el Modelo de Seguridad y Privacidad de la Información (MSPI).
 - b) Identificar la brecha entre el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) y la situación de la Entidad a través de la herramienta establecida por el Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC.
 - c) Liderar la implementación y mantenimiento del Sistema de Gestión de Seguridad y Privacidad de Información (SGSPI), asegurando el cumplimiento de las políticas generales y específicas de Seguridad de la Información aprobadas por la Entidad.

- d) Asegurar la ejecución de los planes del Sistema de Gestión de Seguridad y Privacidad de Información (SGSPI) y el logro de los objetivos de Seguridad de la Información. Realizar actualizaciones metodológicas y de lineamientos del Sistema de Gestión de Seguridad y Privacidad de Información (SGSPI) de acuerdo con la normatividad vigente y aplicable.
- e) Administrar, monitorear y coordinar permanentemente la Seguridad de la Información en la Entidad.
- f) Apoyar la definición e implementación de controles para el tratamiento de riesgos de Seguridad de la Información para cada proceso.
- g) Apoyar la definición de acciones que permitan identificar las vulnerabilidades en la infraestructura tecnológica de la Entidad.
- h) Atender las auditorías internas, externas y revisiones de entes de control, proporcionando la información correspondiente a Seguridad de la Información.
- i) Asegurar la adecuada gestión de los incidentes de Seguridad de la Información en la Entidad.
- j) Promover la divulgación de las responsabilidades de Seguridad de la Información de los funcionarios, contratistas y demás personas vinculadas a la Jurisdicción Especial para la Paz.
- k) Promover programas, campañas y actividades de sensibilización del Sistema de Gestión de Seguridad y Privacidad de Información (SGSPI) al interior de la Entidad.
- l) Gestionar la actualización del Sistema de Gestión de Seguridad y Privacidad de Información (SGSPI).
- m) Documentar el seguimiento, medición, análisis y evaluación del desempeño de la Seguridad de la Información y la eficacia del Sistema de Gestión de Seguridad y Privacidad de Información (SGSPI).
- n) Actuar como enlace con las autoridades y grupos de interés relacionados con la Seguridad de la Información.
- o) Convocar al Comité de Seguridad de la Información y proponer la agenda a tratar.
- p) Informar a intervalos planificados al Comité de Seguridad de la Información sobre el desempeño del Sistema de Gestión de Seguridad y Privacidad de Información (SGSPI) en la Entidad.

CAPÍTULO TERCERO

Disposiciones finales

Artículo 11. *Publicidad*. La presente Política de Seguridad y Privacidad de la Información y su anexo técnico estará disponible para su consulta en la página web.

Artículo 12. *Vigencia*. La presente Política de Seguridad y Privacidad de la Información rige a partir de la fecha de su expedición.

(C. F.).

ACUERDO AOG NÚMERO 046 DE 2019

(septiembre 10)

por la cual se adopta la Política de Prevención de Consumo de Alcohol, Tabaco y otras Sustancias Psicoactivas en la Jurisdicción Especial para la Paz (JEP).

El Órgano de Gobierno de la Jurisdicción Especial para la Paz (JEP), en ejercicio de las facultades constitucionales y legales, en especial las conferidas por el parágrafo 2° del artículo transitorio 5° del Acto Legislativo 01 de 2017, precisado en sus alcances por la Corte Constitucional en Sentencia C-674 de 2011, el artículo 10 de la Ley 1957 de 2019 y el artículo 12 del Reglamento General de la Jurisdicción Especial para la Paz, y

CONSIDERANDO:

Que el artículo 49 de la Constitución Política, modificado por el Acto Legislativo 2 de 2009, establece entre otros, que la atención de la salud y el saneamiento ambiental son servicios públicos a cargo del Estado, garantizando a todas las personas el acceso a los servicios de promoción, protección y recuperación de la salud.

Que el literal f) del artículo 3° de la Resolución 2400 de 1979 del Ministerio del Trabajo y Seguridad Social “por la cual se establecen algunas disposiciones sobre vivienda, higiene y seguridad en los establecimientos de trabajo”, determina:

“Artículo 3°. Son obligaciones de los trabajadores:

(...)

f) No introducir bebidas u otras sustancias no autorizadas en los lugares o centros de trabajo ni presentarse en los mismos bajo los efectos de sustancias embriagantes, estupefacientes o alucinógenas; y comportarse en forma responsable y seria en la ejecución de sus labores”.

Que el artículo 1° de la Resolución 1075 de 1992, del Ministerio del Trabajo y Seguridad Social “por la cual se reglamentan actividades en materia de Salud Ocupacional” fija: