**RESOLUCION No. 0371**
(Veintiocho (28) de abril de Dos Mil Veinte (2020))

Por la cual se adoptan las Política de Gobierno Digital, y de Seguridad y Privacidad de la Información y el Modelo de Seguridad y Privacidad de la Información y se dictan otras disposiciones.

EL GERENTE DEL SANATORIO DE CONTRATACION, EMPRESA SOCIAL DEL ESTADO, en uso de sus facultades legales y en especial las conferidas por los decretos 1289 de 1994 y 139 de 1996, y

**CONSIDERANDO:**

Que mediante la ley 1273 de 2009 se creó un bien jurídico denominado de la protección de la información y de los datos, tipificando penalmente las conductas contra la confidencialidad, la integridad y la disponibilidad de los datos de los sistemas informativos.

Que el Decreto 2573 de 2014, por el cual se establecen los lineamientos generales de la estrategia de Gobierno en Línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones, en su artículo 5 ° establece los componentes que facilitan la masificación de la oferta y la demanda del Gobierno en Línea.

Que el Decreto 2573 de 2014 estableció los lineamientos generales de la Estrategia de Gobierno en línea y definió el alcance y participación de las tecnologías de la información en la gestión de datos públicos e interacción con la comunidad.

Que el gobierno nacional expidió el Decreto 1078 de 2015, "Decreto Único Reglamentario del Sector Tecnologías de la Información y las Comunicaciones".

Que el TITULO 9 del Decreto 1078 de 2015, establece las "POLÍTICAS Y LINEAMIENTOS DE TECNOLOGÍAS DE LA INFORMACIÓN".

Que el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015, reglamenta el componente de seguridad y privacidad de la información, del acceso, uso, divulgación, interrupción o destrucción no autorizada. Que en el artículo 2.2.9.1.3.2 del presente Decretó estableció los plazos para la implementación del Manual de Gobierno en Línea, por parte de las entidades del orden nacional.

Que por medio del CONPES 3701 y 3854 de 2016 se fijó los lineamientos y la política Nacional de seguridad digital, para que las entidades del Estado constituyan mecanismos para la gestión de los riesgos digitales.

Que a través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

Que el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

Que el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC recopiló en el Modelo de Seguridad y Privacidad de la Información, las mejores prácticas nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL hoy Gobierno Digital.

Que conforme con la normatividad citada surge la necesidad de adoptar una política institucional de seguridad y privacidad de la información considerando el papel estratégico de las tecnologías de la información y comunicaciones TIC frente al Modelo de Seguridad y Privacidad de la información; además de la importancia de mitigar riesgos alrededor de la información mediante la implementación de planes para el manejo de incidentes, así como las herramientas para respaldar las actividades ejecutadas en el Sanatorio de Contratación E.S.E, incentivando la cultura de seguridad de la información a los usuarios, previniendo o solucionando posibles ataques informáticos, virus, robos, uso indebido de software o perdidas de información.

Que el fundamento de una política institucional de seguridad y privacidad de la información es buscar la gestión del conocimiento como base para la mejora continua de la misma, adaptándola a la normatividad vigente en el sector, las tendencias tecnológicas y los cambios en la gestión de procesos y procedimientos tecnológicos en el Sanatorio de Contratación E.S.E.

Que el Modelo de Seguridad y Privacidad de la Información - MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos„ mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

Que el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC definió guías que apoyan la adopción de la Política General de Seguridad de la Información y otros instrumentos del Modelo de Seguridad y Privacidad de la Información.

Que se requiere adoptar las Políticas de Seguridad Digital y Gobierno Digital y definir sus elementos como parte de las estrategias en el proceso de implementación del Modelo Integrado de Planeación y Gestión adoptado por el Sanatorio de Contratación E.S.E., en cumplimiento del Decreto 1499 de 2017.

Que en mérito de lo expuesto y garantizando el ciclo de mejoramiento continuo es fundamental adoptar las Políticas de Seguridad Digital y de Seguridad y Privacidad de la Información y el Modelo de Seguridad y Privacidad de la Información -MSPI- propuestos por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC.

Que en mérito de lo anterior expuesto el Gerente del Sanatorio de Contratación, Empresa Social del Estado,

**RESUELVE**

**ARTICULO PRIMERO:** Dictar y adoptar la Política de Gobierno Digital del Sanatorio de Contratación E.S.E.

**ARTÍCULO SEGUNDO. DEFINICIÓN DE LA POLÍTICA DE GOBIERNO DIGITAL.** El Sanatorio de Contratación Empresa Social del Estado y sus colaboradores se comprometen a establecer procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información y las comunicaciones, habilitando servicios digitales de confianza y calidad, empoderando a los usuarios, funcionarios, practicantes, contratistas, proveedores y la ciudadanía en general a través de la consolidación de un entorno digital confiable, favoreciendo la toma de decisiones a partir del uso y aprovechamiento de la información que conlleven a la consolidación de una entidad competitiva, proactiva, e innovadora en un entorno de confianza digital.

**ARTICULO TERCERO. OBJETIVOS DE LA POLÍTICA DE GOBIERNO DIGITAL.** Los objetivos de la Política de Gobierno Digital del Sanatorio de Contratación E.S.E. son los siguientes:

- Habilitar y mejorar la provisión de Servicios Digitales de confianza y calidad.
- Lograr procesos internos seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información.
- Favorecer la toma de decisiones basadas en datos a partir del aumento en el uso y aprovechamiento de la información
- Empoderar a los usuarios, funcionarios, ejecutores, docentes, estudiantes, proveedores y la ciudadanía en general a través de la consolidación de un entorno digital confiable y abierto.
- Impulsar el desarrollo de territorios y ciudades inteligentes para la solución de retos y problemáticas sociales, a través del aprovechamiento de Tecnologías de la Información y las Comunicaciones.

**ARTÍCULO CUARTO.** Adoptar el Manual de Gobierno Digital para la implementación de la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones, el cual es parte integral del presente acto administrativo.

**ARTICULO QUINTO. Componentes de la Política de Gobierno Digital**:

1. **TIC para el Estado:** Tiene como objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades públicas, a través del uso de las Tecnologías de la Información y las Comunicaciones.

2. **TIC para la Sociedad:** Tiene como objetivo fortalecer la sociedad y su relación con el Estado en un entorno confiable, que permita la apertura y el aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, el diseño conjunto de servicios, la participación ciudadana en el diseño de políticas y normas, y la identificación de soluciones a problemáticas de interés común.

**ARTICULO SEXTO: Habilitadores Transversales de la Política de Gobierno Digital**: Son elementos fundamentales que permiten el desarrollo de los componentes de la Política de Gobierno Digital:

1. **Arquitectura:** busca que las entidades apliquen en su gestión un enfoque de Arquitectura Empresarial para el fortalecimiento de sus capacidades institucionales y de gestión de TI. El habilitador de Arquitectura soporta su uso e implementación en el Marco de Referencia de Arquitectura Empresarial del Estado, que es el instrumento que establece la estructura conceptual, define lineamientos, incorpora mejores prácticas y traza la ruta de implementación que una entidad pública debe realizar.

2. **Seguridad de la información**: busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos.

3. **Servicios Ciudadanos Digitales:** busca que todas las entidades públicas implementen lo dispuesto en el título 17 de la parte 2 del libro 2 del Decreto

1078 de 2015, que establece los lineamientos para la prestación de los servicios ciudadanos digitales, y para permitir el acceso a la administración pública a través de medios electrónicos. Conforme a dicha normativa, los servicios digitales se clasifican en servicios básicos: autenticación biométrica, autenticación con cédula digital, autenticación electrónica, carpeta ciudadana e interoperabilidad, los cuales son de obligatorio uso y adopción; y servicios especiales, que son adicionales a los servicios básicos, como el desarrollo de aplicaciones o soluciones informáticas para la prestación de los servicios ciudadanos digitales básicos.

**ARTÍCULO SÉPTIMO: Conformar el grupo de trabajo de Arquitectura Empresarial.** El grupo de trabajo de Arquitectura Empresarial del Sanatorio de Contratación E.S.E. estará conformado por:

- El encargado de Sistemas y Comunicaciones o quien haga sus veces
- El Jefe de Planeación
- El Jefe de Estadística
- El encargado de la Unidad de Archivo o quien haga sus veces
- El encargado de Recursos Físicos o quien haga sus veces
- El encargado de Calidad o quien haga sus veces

**PARAGRAFO 1:** A las reuniones del grupo de trabajo de Arquitectura Empresarial se podrán invitar a los servidores de las dependencias respecto de las cuales se traten temas especiales; así mismo podrán ser invitadas personas externas para apoyar técnicamente en temas específicos relacionados. Los invitados tendrán voz, pero no voto.

**PARAGRAFO 2:** Será invitado permanente el Jefe de la Oficina de Control Interno o quien haga sus veces, quien tendrá voz, pero no voto.

**ARTICULO OCTAVO: Roles y Responsabilidades de la Política de Gobierno Digital**: Se define un esquema institucional que vincula desde la alta dirección hasta las áreas específicas del Sanatorio de Contratación E.S.E. en el desarrollo de la política y el logro de sus propósitos. A continuación, se presentan las instancias y sus responsabilidades en la implementación de la política:

1. **Líder de la política de Gobierno Digital:** es el Ministerio de Tecnologías de la Información y las Comunicaciones, quién a través de la Dirección de Gobierno Digital, se encarga de emitir las normas, manuales, guías y la metodología de seguimiento y evaluación para la implementación de la política de Gobierno Digital, en las entidades públicas del orden nacional y territorial.

2. **Responsable Institucional de la Política de Gobierno Digital:** es el representante legal del Sanatorio de Contratación E.S.E., y es el responsable de coordinar, hacer seguimiento y verificación de la implementación de la Política de Gobierno Digital. El Responsable Institucional debe garantizar el desarrollo integral de la política como una herramienta transversal que apoya la gestión de la entidad y el desarrollo de las políticas de gestión y desempeño institucional del Modelo Integrado de Planeación y gestión.

3. **Responsable de orientar la implementación de la Política de Gobierno Digital**: es el Comité Institucional de Gestión y Desempeño. Esta instancia será la responsable de orientar la implementación de la política de Gobierno Digital, conforme a lo establecido en el Modelo Integrado de Planeación y Gestión. Teniendo en cuenta que la principal función de este comité es

orientar la implementación y operación de todas las políticas del Modelo Integrado de Planeación y Gestión -MIPG (entre las que se encuentra Gobierno Digital), esta instancia debe articular todos los esfuerzos institucionales, recursos, metodologías y estrategias para el desarrollo de las políticas del MIPG y en esta medida, lograr que Gobierno Digital se desarrolle articuladamente con las demás políticas en el marco del sistema de gestión de la entidad.

4. **Responsable de liderar la implementación la Política de Gobierno Digital:** es el encargado del área de Sistemas del Sanatorio de Contratación E.S.E., o quien haga sus veces en la entidad, quien hará parte del Comité Institucional de Gestión y Desempeño y responderá directamente al representante legal de la entidad, de acuerdo con lo establecido en el artículo 2.2.35.4. del Decreto Único Reglamentario de Función Pública 1083 de 2015. Teniendo en cuenta que el nuevo enfoque de Gobierno Digital es el uso de la tecnología como una herramienta que habilita la gestión de la entidad para la generación de valor público, todas las áreas o dependencias son corresponsables en su implementación.

5. **Líderes de los procesos o dependencias:** serán corresponsables de la implementación de la Política de Gobierno Digital en los temas de su competencia.

6. **Grupo de trabajo de arquitectura empresarial:** este grupo actuará como un comité técnico de arquitectura empresarial, que evalúa los impactos de cualquier decisión de inversión, adquisición o modernización de sistemas de información e infraestructura tecnológica en la entidad. Así mismo, tiene funciones de gobierno sobre la arquitectura empresarial de la entidad y debe remitirse al Comité Institucional de Gestión y Desempeño cuando se requieran tomar decisiones de alto nivel.

7. **Oficina de control interno:** De acuerdo con lo definido en la Dimensión de Control Interno del Modelo Integrado de Planeación y Gestión, las oficinas de control interno desempeñan un rol específico en materia de control y gestión del riesgo, con el fin de apoyar el desarrollo de un adecuado ambiente de control, una efectiva gestión del riesgo, la implementación de controles efectivos y un monitoreo y supervisión continua a la gestión de la entidad. En este sentido, la alta dirección, los líderes de proceso y los servidores públicos relacionados con la implementación de Gobierno Digital, deben articular con la oficina de control interno el desarrollo de acciones, métodos y procedimientos de control y de gestión del riesgo para la implementación de la política.

**ARTICULO NOVENO:** Dictar y adoptar la Política de Seguridad y Privacidad de la Información del Sanatorio de Contratación E.S.E.

**ARTÍCULO DECIMO. DEFINICIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.** El Sanatorio de Contratación E.S.E. como prestador de servicios integrales de salud a los enfermos de Hansen y a la comunidad en general, está comprometido con la preservación de la confidencialidad, disponibilidad e integridad de la información de la Institución, para lo cual da cumplimiento a los requisitos aplicables relacionados con la seguridad de la información e implementa y mejora continuamente el Modelo de Seguridad y Privacidad de la Información (MSPI), a fin de garantizar la protección de los activos de la información contra uso, modificación, acceso o destrucción no

autorizada.

**ARTICULO DECIMO PRIMERO. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DIGITAL**. Los objetivos de la Política de Seguridad y Privacidad de la Información del Sanatorio de Contratación E.S.E. son los siguientes:

- Identificar las amenazas interna y externa, deliberadas o accidentales que pueden afectar los activos de la información, evaluar y valorar los riesgos y establecer los respectivos controles.
- Realizar seguimiento a la implementación y eficacia de los controles implementados para la preservación de la confidencialidad, integridad y disponibilidad de los activos de la información.
- Cumplir la normatividad nacional vigente aplicable en materia de Seguridad y Privacidad de la Información.
- Promover la cultura de Seguridad y Privacidad de la Información en los funcionarios, contratistas y demás personas que interactúen con el Sanatorio de Contratación E.S.E.

**ARTÍCULO DECIMO PRIMERO SEGUNDO.** Adoptar el Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones, el cual es parte integral del presente acto administrativo.

**ARTÍCULO DECIMO TERCERO.** Designar como Responsable de Seguridad de la Información al Jefe de Estadística del Sanatorio de Contratación E.S.E. o quien haga sus veces.

**ARTÍCULO DECIMO CUARTO: Conformar el Comité de Seguridad de la Información.** El Comité de Seguridad de la Información del Sanatorio de Contratación E.S.E. estará conformado por:

- El Responsable de Seguridad de la Información
- El encargado de Sistemas y Comunicaciones o quien haga sus veces
- El Jefe de Planeación
- El encargado de la Unidad de Archivo o quien haga sus veces
- El encargado del SIAU o quien haga sus veces
- El encargado de Calidad o quien haga sus veces

**PARAGRAFO 1:** A las reuniones del Comité de Seguridad de la Información se podrán invitar a los servidores de las dependencias respecto de las cuales se traten temas especiales; así mismo podrán ser invitadas personas externas para apoyar técnicamente en temas específicos relacionados con la naturaleza del Comité. Los invitados tendrán voz, pero no voto.

**PARAGRAFO 2:** Será invitado permanente el Jefe de la Oficina de Control Interno o quien haga sus veces quien tendrá voz, pero no voto.

**ARTÍCULO DECIMO QUINTO:** Objetivo del Comité de Seguridad de la Información. El Comité deberá asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo, así como de la formulación y mantenimiento de la política de seguridad y privacidad

de la información a través de todo el Sanatorio de Contratación E.S.E.

**ARTÍCULO DECIMO SEXTO. Secretaria Técnica:** La Secretaría Técnica del Comité se definirá al interior del Comité y el secretario elegido será remplazado cada seis (6) meses.

**ARTÍCULO DECIMO SÉPTIMO. Funciones de la Secretaría Técnica.** Las funciones de la Secretaría Técnica serán las siguientes:

1. Elaborar las actas de las reuniones del Comité y verificar su formalización por parte de sus miembros.
2. Citar a los integrantes del Comité a las sesiones ordinarias o extraordinarias
3. Remitir oportunamente a los miembros la agenda de cada comité.
4. Llevar la custodia y archivo de las actas y demás documentos soportes.
5. Servir de interlocutor entre terceros y el Comité.
6. Realizar seguimiento a los compromisos y tareas pendientes del Comité.
7. Presentar los informes que requiera el Comité.
8. Las demás que le sean asignadas por el Comité.

**ARTÍCULO DECIMO OCTAVO. Reuniones del Comité de Seguridad de la Información.** El Comité de Seguridad de la Información – deberá reunirse cada tres (3) meses, previa convocatoria del Secretario Técnico del Comité.

**ARTÍCULO DECIMO NOVENO. Sesiones Extraordinarias.** Los miembros que conforman el Comité podrán ser citados a participar de sesiones extraordinarias de trabajo cuando sea necesario, de acuerdo a temas de riesgos, incidentes o afectaciones de continuidad dentro del Sistema de Gestión de Seguridad de la Información.

**ARTICULO VIGÉSIMO: Roles y Responsabilidades de la Política de Seguridad y Privacidad de la Información**: Se define un esquema institucional que vincula desde la alta dirección hasta las áreas específicas del Sanatorio de Contratación E.S.E. en el desarrollo de la política y el logro de sus propósitos. A continuación, se presentan las instancias y sus responsabilidades en la implementación de la política:

1. **Comité Institucional de Gestión y Desempeño:**

- Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de Seguridad y Privacidad de la información.
- Verificar el cumplimiento de la presente directiva, en particular la Difusión y adopción de las políticas, normas y estándares de Seguridad de la Información.
- Apoyar los programas de sensibilización, actualización y entrenamiento técnico del personal de las áreas de tecnología en temas relacionados con la Seguridad de la Información.
- Apoyar la mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI).
- Gestionar los recursos financieros requeridos para la apropiada protección de los activos de información y mantenimiento del Modelo de Seguridad y Privacidad de la Información (MSPI).
- Revisar el Modelo de Seguridad y Privacidad de la Información (MSPI) de

la organización a intervalos planificados, para asegurarse de su conveniencia, adecuación y eficacia continuas.

**2. Área de Sistemas:**

- Implementar, apoyar y soportar el Modelo de Seguridad y Privacidad de la Información (MSPI).
- Promover el cumplimiento por parte del personal bajo su responsabilidad de la Políticas de Seguridad de la Información.
- Administrar las herramientas tecnológicas para el cumplimiento de las políticas de seguridad de la información.
- Definir y aplicar los procedimientos para garantizar la disponibilidad y capacidad de los recursos tecnológicos a su cargo.
- Definir e implementar la estrategia de concientización y sensibilización en Seguridad de la Información para los funcionarios, contratistas y terceros.
- Custodiar la información y los medios de almacenamiento bajo su responsabilidad.
- Definir, mantener y controlar lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas; así mismo, realizar el control y verificación del cumplimiento del licenciamiento de dicho software y aplicaciones.
- Diseñar, implementar, evaluar y controlar procedimientos de Seguridad de la Información que apliquen para las plataformas de tecnologías de la información administradas.
- Diseñar, implementar, evaluar y controlar procedimientos para dar continuidad a las actividades para cada una de las plataformas tecnológicas críticas bajo su responsabilidad.

**3. Responsable de Seguridad de la Información:**

- Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades de la Institución, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo.
- Identificar la brecha entre el Modelo de seguridad de la información y la situación actual de la entidad.
- Generar el cronograma de la implementación del Modelo de Seguridad y
- privacidad de la información.
- Planear, implementar y hacer seguimiento a las tareas, fecha y plan de trabajo de los objetivos específicos del cronograma definido.
- Gestionar el equipo de trabajo requerido, definiendo roles, responsabilidades, entregables y tiempos.
- Coordinar las actividades del equipo y proporcionar apoyo administrativo.
- Encarrilar la Institución hacia el cumplimiento de la implementación del Modelo de Seguridad y privacidad de la Información para la entidad.
- Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos de seguridad de la información para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario.
- Monitorear el estado del proyecto en términos de calidad de los productos, tiempo y los costos.
- Trabajar de manera integrada con el grupo o áreas asignadas.
- Asegurar la calidad de los entregables y del Modelo de Seguridad y privacidad de la información en su totalidad.
- Velar por el mantenimiento de la documentación del Modelo de Seguridad y privacidad de la información, su custodia y protección.
- Contribuir al enriquecimiento del esquema de gestión del conocimiento

sobre el Modelo de Seguridad y privacidad de la información en cuanto a la documentación de las lecciones aprendidas.
- Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del Modelo de Seguridad y privacidad de la información.

**4. Comité de seguridad de la información:**

- Coordinar la implementación del Modelo de Seguridad y privacidad de la Información al interior de la entidad.
- Revisar los diagnósticos del estado de la seguridad de la información en el Sanatorio de Contratación E.S.E.
- Acompañar e impulsar el desarrollo de proyectos de seguridad de la información.
- Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la Institución.
- Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
- Aprobar el uso de metodologías y procesos específicos para la seguridad de la información.
- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
- Realizar revisiones periódicas del Modelo de Seguridad y privacidad de la información (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
- Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad.
- Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma.
- Las demás funciones inherentes a la naturaleza del Comité.

**5. Oficina de Talento Humano:**

- Incluir en los programas de inducción y reinducción el tema de Seguridad y Privacidad de la Información, asegurando que los funcionarios conozcan sus responsabilidades, así como las implicaciones por el uso indebido de activos de la información o de otros recursos informáticos, haciendo énfasis en las consecuencias jurídicas que se pueden acarrear como servidor público o contratista de la entidad.
- Asegurarse de las personas que realizan, bajo su control, un trabajo que afecta su desempeño de la seguridad de la información, sean competentes, basándose en la educación, formación o experiencia adecuadas.

**6. Oficina de Control Interno:**

- La oficina de control interno desempeña un rol específico en materia de control y gestión del riesgo, con el fin de apoyar el desarrollo de un adecuado ambiente de control, una efectiva gestión del riesgo, la implementación de controles efectivos y un monitoreo y supervisión continua a la gestión de la entidad. En este sentido la oficina de control interno será la encargada de realizar seguimiento a la implementación de los controles definidos para los riesgos de seguridad de la información identificados.
- Realizar auditorías internas a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de la seguridad de la

información conforme a los requisitos normativos y los propios de la organización para su sistema de gestión de la seguridad de la información.

7. **Líderes de los procesos o dependencias:** Definir, diseñar, documentar, implementar, evaluar y controlar los procedimientos relacionados con sus procesos, incluyendo aquellas actividades que sean consideradas como controles de Seguridad de la Información dentro de dichos procedimientos.

8. **Servidores públicos y contratistas:** Aplicación de la Seguridad y Privacidad de la Información de acuerdo con las políticas y procedimientos establecidos por la organización.

**ARTÍCULO VIGÉSIMO PRIMERO:** La presente resolución rige a partir de su expedición y deroga las disposiciones que les sean contrarias.

**COMUNIQUESE Y CUMPLASE**

Se expide la presente Resolución, a los veintiocho (28) días del mes de abril de dos mil veinte (2020).

**DR. FREDY EDUARDO FONSECA SUAREZ**
Gerente Sanatorio de Contratación E.S.E.

Proyectó/elaboró: Ing. Andrés Felipe Calderón Riaño/Encargado Sistemas.
Aprobó: Dr. Fredy Eduardo Fonseca Suarez: Gerente.