PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SERVICIUDAD E.S.P

DOSQUEBRADAS, AÑO 2021

TABLA DE CONTENIDO

PRESENTACIÓN

La política de Gobierno Digital busca desarrollar un enfoque integral que permita añadir tanto valor público como social a través del uso y aprovechamiento de las Tecnologías de la Información, mediante la articulación de las Entidades con los ciudadanos generando escenarios de innovación, competitividad y proactividad. Por tal motivo, El plan de Seguridad y Privacidad de la Información de SERVICIUDAD E.S.P como componente principal de la etapa de planificación del Modelo de Seguridad y Privacidad de la Información, busca brindar directrices y herramientas bajo buenas prácticas para la preservación de la disponibilidad, integridad y confidencialidad de los activos de información al interior de la Entidad.

1. OBJETIVO

Diseñar el Plan de Seguridad y Privacidad de la Información como herramienta integral del Modelo de Seguridad y Privacidad de la Información bajo buenas prácticas para la preservación de la disponibilidad, integridad y confidencialidad de los activos de información de SERVICIUDAD E.S.P

1.1. OBJETIVOS ESPECIFICOS

- Establecer y adoptar planes, programas, políticas y procedimientos bajo buenas prácticas para la gestión de riesgos en materia de seguridad de la información al interior de la Entidad.
- Diseñar las herramientas y directrices que forman parte de la etapa de Planificación del Modelo de Seguridad y Privacidad de la Información de la Entidad

2. ALCANCE

El Plan de Seguridad y Privacidad de la Información contiene los componentes que integran la fase de Planificación del MSPI, lo cual incluye la documentación y adopción de la Política de Seguridad y Privacidad de la Información, el procedimiento para la identificación y clasificación de los activos de información e infraestructura crítica, el plan de tratamiento de riesgos y controles, la declaración de aplicabilidad de controles bajo el estándar del Anexo A de la ISO 27001:2013, los roles y responsabilidades de Seguridad de la Información y el Plan de capacitación, sensibilización y comunicación de seguridad de la Información.

3. DEFINICIONES

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
- **Activos de Información y recursos:** se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 20116).
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
- **Control:** 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.
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Información Pública Clasificada:** 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 de 2014. (Ley 1712 de 2014, art 6)
- **Información Pública Reservada:** 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 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Riesgo:** 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. (ISO/IEC 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad. (ISO/IEC 27000).
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

4. MARCO LEGAL

El marco normativo aplicable para la elaboración del Plan de Seguridad y Privacidad de la Información es el siguiente:

- **Ley 1581 de 2012**: Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Decreto 2609 de 2012:** Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- **Decreto 1377 de 2013:** Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- **Decreto 886 de 2014:** Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- **Ley 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.
- **Decreto 103 de 2015:** Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **Decreto 1074 de 2015**: Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- **Decreto 1078 de 2015:** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Decreto 612 de 2018:** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- **Decreto 1008 de 2018:** 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.
- **Resolución 500 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.

5. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para el desarrollo del Plan de Seguridad y Privacidad de la Información se tuvieron presente los resultados obtenidos de la fase de diagnóstico del Modelo de Seguridad y privacidad de la Información bajo las directrices establecidas por MinTIC. A su vez, El Plan de Seguridad y Privacidad de la información se encuentra integrado como plan institucional y estratégico desde el ámbito de aplicación del Modelo Integrado de Planeación y Gestión.

De acuerdo a lo anterior, el Plan de Seguridad y Privacidad de la Información de SERVICIUDAD E.S.P se compone de los siguientes elementos:

5.1. Contexto de la Entidad

En la gestión de la estrategia desde todos los niveles de la estructura organizacional de la Entidad, continuamente se está procesando, almacenando, gestionando, custodiando y transfiriendo información, cuanto mayor es el valor de esta información mayores son los riesgos asociados a su pérdida por manipulación indebida o malintencionada. Por tal motivo, el Plan de Seguridad de la Información se encuentra alineado con el Plan Estratégico de la Entidad, apalancando la estrategia de seguridad digital para la preservación de los activos y continuidad en la operación del negocio, cumpliendo objetivos de seguridad. Así mismo, la seguridad de la información realmente debe propenderse como cultura estratégica de la Entidad, en la cual se involucren todas las partes interesadas de la misma.

5.*2.* Partes Interesadas Seguridad y Privacidad de la Información

La Entidad tiene una visión holística de los riesgos que puede afectar la seguridad y privacidad de la información donde se puede establecer controles y medidas transversales viables y efectivas, con el propósito de brindar garantías de disponibilidad, integridad y confidencialidad de la información de la Entidad y bases de datos de las partes interesadas. Por tal motivo, las partes interesadas de Seguridad y Privacidad de la Información están alineadas con los Stakeholder del Plan Estratégico de la Entidad.

IMAGEN Nª1. PARTES INTERESADAS

Fuente: Elaboración Propia

5.*3.* Alcance del MSPI

El Modelo de Seguridad y Privacidad de la Información permite definir los limites sobre los cuales se implementará la seguridad y privacidad en SERVICIUDAD E.S.P mediante un enfoque de procesos y riesgos en todos los procesos de la Entidad, teniendo en cuenta los Planes, programas, políticas y procedimientos documentados en las fases del ciclo de vida del MSPI.

5.4. Liderazgo y Compromiso

La Entidad cuenta con acto administrativo que debe adoptar mediante resolución, el cual contiene la conformación del Comité de Seguridad y Privacidad de la Información, señalando los roles y responsabilidades de éstos, el cual se puede visualizar en el documento ***"Comité de Seguridad y Privacidad de la Información"***

5.5. Política de Seguridad y Privacidad de la Información

La Entidad tiene definida y documentada la Política de Seguridad y Privacidad de la Información, mediante la cual se establecen los parámetros de riesgos y controles para proteger de posibles riesgos de daño, pérdida y uso indebido de la información, los equipos y demás recursos informáticos de SERVICIUDAD E.S.P, los cuales

están en constante cambio y evolución de acuerdo con el avance de la tecnología y los requerimientos de la Entidad. Esta política se puede visualizar en el documento **"Política de Seguridad y Privacidad de la Información"**

5.6. Roles y responsabilidades

La Entidad definió los roles y responsabilidades de la seguridad de la Información al Interior de la misma de acuerdo a los niveles estratégico, táctico y operativo, en el nivel estratégico se encuentra el Comité de Seguridad de la Información, en el nivel táctico el responsable de la Seguridad de la Información y en el nivel operativo los líderes de procesos y responsable del tratamiento de datos personales. De esta manera, las funciones en dichos niveles se encuentran documentadas en el "***"Comité de Seguridad y Privacidad de la Información"***

5.7. Procedimiento de Identificación y clasificación de activos

La Entidad cuenta con el siguiente procedimiento para la identificación y clasificación de activos e infraestructura crítica, el cual contiene la metodología para la tipificación y valoración de activos al interior de la misma.

ALCANCE

El procedimiento de inventario y clasificación de los activos de información e infraestructura crítica, abarca la metodología con las pautas requeridas para un adecuado proceso de clasificación y valoración de los activos de información de la Entidad.

RESPONSABLE

Los responsables del procedimiento de inventario y clasificación de los activos de información e infraestructura crítica de acuerdo a las siguientes actividades son:

TABLA Nª1. RESPONSABLES

ACTIVIDAD	RESPONSABLE
Suministrar la Información de los activos para la documentación y actualización de la matriz de activos de Información.	• Propietario de los activos al interior de cada proceso.
Validar y actualizar la matriz de activos de Información de acuerdo a la frecuencia establecida desde el índice	• El responsable designado por el Comité Institucional de Gestión y Desempeño.

de Transparencia y acceso a la Información pública.	
Aprobar la Matriz de Activos de Información	• Comité Institucional de Gestión y Desempeño.
Publicar la Matriz de Activos de Información	• El responsable designado por el Comité Institucional de Gestión y Desempeño.

Fuente: Elaboración Propia.

FASES DEL PROCEDIMIENTO

La identificación y clasificación de los activos es una de las actividades principales e importantes del Modelo de Seguridad y Privacidad de la Información y se conforma por las siguientes fases:

FASE 1: IDENTIFICACIÓN Y TIPIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

En esta fase la dependencia propietaria y custodia de la información, identifica y clasifica la información producida de acuerdo con el tipo de activo: Información, Hardware, Software, Servicios, Recurso Humano, Instalaciones e Infraestructura Crítica Cibernética Nacional.

FASE 2: CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN:

En esta fase la dependencia propietaria y custodia de la información clasifica los activos en información pública, clasificada o reservada de acuerdo con lo establecido en el artículo 6 de la ley 1712 de 2014 “Ley de Transparencia y Acceso a la Información Pública”.

FASE 3: REVISIÓN Y APROBACIÓN:

En esta etapa se valida la clasificación y valoración dada a los activos de información, la cual debe ser aprobada por el Comité Institucional de Gestión y Desempeño para su publicación.

FASE 4: PUBLICACIÓN DE LOS ACTIVOS DE INFORMACIÓN:

Después de aprobar el inventario de activos de información, éste se publica en la página web de la Entidad en el botón de transparencia y acceso a la información pública.

METODOLOGIA DE INVENTARIO Y CLASIFICACIÓN DE LA INFORMACIÓN E INFRAESTRUCTURA CRÍTICA:

La metodología para la identificación, clasificación y construcción de la matriz de activos de información e infraestructura critica se compone de los siguientes pasos:

1. **Identificador:** Relacionar el número consecutivo único que identifica el activo en el inventario.
2. **Proceso:** Relacionar el nombre del Proceso al que pertenece el activo.
3. **Nombre del Activo:** Nombre de identificación del activo dentro del proceso al que pertenece.
4. **Descripción:** Describir el activo de manera que sea claramente identificable por todos los miembros del proceso.
5. **Idioma:** Relacionar el idioma en que se encuentra documentado el activo
6. **Ubicación:** Describe la ubicación tanto física como electrónica del activo de información.
7. **Medio de Conservación/ Soporte:** Describe el repositorio donde se conserva la información, puede ser un sistema de información, un servidor, una carpeta pública, un computador, entre otros.
8. **Fecha de Generación de la Información:** Describe la fecha en que se creó el documento.
9. **Formato:** Relacionar el formato en que se encuentra el documento puede ser Word, pdf, Excel, JPG, entre otros.
10. **Tipificación del Activo:** Define el tipo al cual pertenece el activo, los activos se pueden clasificar en:
    - **Información:** Corresponden a este tipo datos e información almacenada o procesada electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, proyectos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.
    - **Hardware:** Se consideran los medios materiales físicos destinados a soportar directa o indirectamente los servicios que presta la Entidad. Ejemplo: Servidores, routers, módems Computadores (portátiles, escritorio), impresoras, Celulares, Tablet, Teléfonos IP
    - **Software:** Se refiere a los programas, aplicativos, sistemas de información que soportan las actividades de la Entidad y la prestación de los servicios. Ejemplo: Software de aplicación, correo electrónico, sistema operativo, etc.
    - **Servicios:** Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.

- **Recurso Humano:** Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información
- **Instalaciones:** Los lugares donde se almacenan o resguardan los sistemas de información y comunicaciones**.**
- **Infraestructura crítica cibernética nacional:** Se entiende por aquella infraestructura soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública**.**

11. Clasificación de los Activos de Información:

La clasificación de activos de información tiene como objetivo asegurar que la información recibe los niveles de protección adecuados, de acuerdo con sus características particulares. El sistema de clasificación definido se basa en los principios de la ISO 27001 Correspondientes a: Confidencialidad, Integridad y la Disponibilidad de cada activo

- **Confidencialidad:** se refiere a que la información no esté disponible ni sea revelada a individuos, Entidades o procesos no autorizados, se definieron tres (3) niveles alineados con los tipos de información declarados en la ley 1712 del 2014:

TABLA Nª2. CLASIFICACIÓN DE ACUERDO A CONFIDENCIALIDAD

INFORMACIÓN PÚBLICA RESERVADA	Información disponible sólo para un proceso de la Entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.

INFORMACIÓN PÚBLICA CLASIFICADA	Información disponible para todos los procesos de la Entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la Entidad o de terceros y puede ser utilizada por todos los funcionarios de la Entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACION PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la Entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la Entidad.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PUBLICA RESERVADA.

Fuente: Anexo 1. Modelo de Seguridad y Privacidad de la Información.

- **Integridad:**

La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.

TABLA Nª3. CLASIFICACIÓN DE ACUERDO A INTEGRIDAD

A (ALTA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la Entidad.
M (MEDIA)	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la Entidad.
B (BAJA)	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la Entidad o entes externos.

NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

Fuente: Anexo 1. Modelo de Seguridad y Privacidad de la Información.

- **Disponibilidad:** La disponibilidad es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona, Entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso.

TABLA Nª4. CLASIFICACIÓN DE ACUERDO A DISPONIBILIDAD

1 (ALTA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2 (MEDIA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la Entidad.
3 (BAJA)	La no disponibilidad de la información puede afectar la operación normal de la Entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

Fuente: Anexo 1. Modelo de Seguridad y Privacidad de la Información.

12. **Clasificación del impacto del activo:** Se deben relacionar los propietarios, custodios y Usuarios.

- **Propietario:** Es una parte designada de la Entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente.
- **Custodio:** Es una parte designada de la Entidad, un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario.

- **Usuario:** Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.

13. Control, seguimiento y publicación:

- **Área responsable de suministrar la información:** Corresponde al mismo propietario de la Información.
- **Periodicidad de Actualización:** Corresponde a la frecuencia con que se deben actualizar los activos, estos se deben actualizar teniendo presente los siguientes aspectos:
  - Actualizaciones al proceso al que pertenece el activo.
  - Adición de actividades al proceso.
  - Inclusión de nuevos registros de calidad, nuevos registros de referencia o procesos y procedimientos.
  - Inclusión de un nuevo activo.
  - Desaparición de un área, proceso o cargo en la Entidad que tenía asignado el rol de propietario o custodio.
  - Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados.
  - Cambios físicos de la ubicación de activos de información.
- **Área responsable de Publicar la información:** Corresponde al área o dependencia encargada de publicar la información, una vez haya sido revisada y aprobada.
- **Observaciones:** Describir las observaciones del seguimiento en caso de ser necesario.

Con base al procedimiento de inventario y clasificación de los activos e infraestructura crítica la Entidad tiene documentada la Matriz de Activos de Información, la cual reposa en el botón de transparencia del sitio web de acuerdo a los lineamientos del Índice de Transparencia y Acceso a La Información Pública y se puede visualizar en el documento **"Matriz de Activos de Información"**

5.8. Valoración de riesgos de seguridad de la Información

La Entidad tiene identificados y definidos los riesgos de seguridad y privacidad de la información de acuerdo a los lineamientos establecidos por MinTIC para la gestión del riesgo, los cuales se puede visualizar en el documento de la Entidad de "**Matriz de Riesgos Seguridad de la Información".** A su vez, cuenta. Con los procedimientos de gestión de seguridad de la información, los cuales le brindan las directrices para la valoración de riesgos al interior de la misma, dichos

procedimiento se pueden visualizar en el archivo de **"Procedimientos de Seguridad de la información"**

5.9. Plan de tratamiento de riesgos

De acuerdo a los riesgos identificados y documentados de Seguridad y Privacidad de la Información, la Entidad cuenta con el plan de tratamiento de riesgos con los controles para mitigar la materialización de éstos y brindar garantías de continuidad en la operación del servicio a través del tratamiento de la información, el plan de acción para tratar los riesgos de la Entidad se encuentra documentado en el **"Plan de Tratamiento de Riesgos"**

5.10. Declaración de Aplicabilidad

La Declaración de Aplicabilidad, por sus siglas en ingles Statement of Applicability (SoA), es un elemento fundamental para la implementación del Modelo de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información. En esta SERVICIUDAD E.SP. indica los objetivos de control y controles seleccionados e implementados al interior de la Entidad, con su respectiva justificación, tomando como marco de referencia el Anexo A del estándar ISO/IEC 27001:2013. De esta manera, la declaración de aplicabilidad es la siguiente:

TABLA Nª5. DECLARACIÓN DE APLICABILIDAD SERVICIUDAD E.S.P

Declaración de Aplicabilidad							
Dominio	Numeral	Nombre	Descripción	Objetivo de Control o Control Seleccionado	Razón de la Selección	Objetivo de Control o Control Implementado	Justificación de Exclusión
	A.5	**Políticas de seguridad de la información**					
Objetivo de	A.5.1	Directrices establecidas por la dirección	Lineamiento: Brindar orientación y apoyo por	SI	Si, Porque la Entidad debe	NO	N/A

Control		para la seguridad de la información	parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes		alinear la Seguridad y Privacidad y de la Información con la protección de datos personales y transparencia en el acceso de la Información Pública		
Control	A.5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.	SI	Si, Porque la Entidad por marco normativo debe adoptar y adaptar la Política de Seguridad de la Información para brindar herramientas como garantía de seguridad hacia el uso y	SI	N/A

					apropiación de los servicios de TI		
Control	A.5.1.2	Revisión de las políticas para seguridad de la información	Control: Las políticas para seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	SI	Si, Porque la Entidad debe mantener y actualizar la Política de Seguridad y Privacidad de la Información de acuerdo a marco normativo vigente	NO	N/A
	A.6	**Organización de la seguridad de la información**					
Control	A.6.1.1	Roles y responsabilidades para la seguridad de información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	SI	Porque la Entidad por marco normativo debe adoptar y adaptar el Comité de Seguridad de la Información, el cual debe cumplir actividade	SI	N/A

					s propias del Modelo de Seguridad y Privacidad de la Información, en la que los roles y responsabilidades brindan garantías para este cumplimiento requerido.		
Control	A.6.1.4	Contacto con grupos de interés especial	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	SI	Si, porque la Entidad debe definir los grupos de interés y Entes de control que regulan y estan relacionados con la seguridad y privacidad de la información	NO	N/A

Control	A.6.1.5	Seguridad de la información en la gestión de proyectos	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	SI	Si, porque la Entidad debe brindar garantias sobre la seguridad y privacidad en la información registrada en la gestión de proyectos	NO	N/A
Objetivo de Control	A.6.2	Dispositivos móviles y teletrabajo	Lineamiento: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.	SI	Si, porque se van a implementar los controles del objetivo de control	NO	N/A
Control	A.6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	SI	Si, porque la Entidad debe adoptar medidas de seguridad sobre los riesgos que se pueden llegar a materializar en el uso de los dispositiv	NO	N/A

					os móviles		
	A.7	**Seguridad de los recursos humanos**					
Objetivo de Control	A.7.1	Antes de asumir el empleo	Lineamiento: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	SI	Si, porque se van a implementar los controles del objetivo de control	SI	N/A
Control	A.7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionale	SI	Si, porque la selección de personal en la Entidad se realiza con base al Manual de Contratación establecido mediante	SI	N/A

			s a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.		el acuerdo Nª11 del 29 de diciembre de 2016		
Control	A.7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información	SI	Si, Porque la Entidad tiene establecidas políticas y roles definidos en seguridad y privacidad de la información que deben conocer y cumplir los empleados y contratistas al momento de ingresar a ésta	SI	N/A

Objetivo de Control	A.7.2	Durante la ejecución del empleo	Lineamiento: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan	SI	Si, porque se van a implementar los controles del objetivo de control. Cabe resaltar que el control de toma de concienciа, educación y formación se encuentra inmerso dentro de la responsabilidad de la Dirección con ejecución de cronograma de Socialización y sensibilización	NO	N/A

Control	A.7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	SI	Si, porque la Alta Dirección debe comprometerse para el funcionamiento de cualquier actividad estratégica dentro de la Entidad, promoviendo desde éstas el uso y apropiación de la seguridad de la información por parte de los colaboradores	NO	N/A
Control	A.7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones	SI	Si, porque se deben aplicar las sanciones pertinentes a los colaboradores que infrinjan las directrices	NO	N/A

			contra empleados que hayan cometido una violación a la seguridad de la información		estipuladas en las políticas de TI		
Objetivo de Control	A.7.3	Terminación o cambio de empleo	Lineamiento: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.	SI	Si, porque se va a implementar el control del objetivo de control	NO	N/A
Control	A.7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deben definir, comunicar al empleado o contratista y se deberían hacer cumplir	SI	Si, porque dentro de la Política de Acceso a Tecnologías de Información se contempla la revocación de privilegios por terminación laboral	NO	N/A
	A.8	**Gestión de activos**					

Objetivo de Control	A.8.1	Responsabilidad por los activos	Lineamiento: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas	SI	Si, porque la Entidad debe documentar el inventario de activos, promoviendo la integridad, disponibilidad y confidencialidad de éstos	NO	N/A
Control	A.8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.	SI	Si, porque la Entidad debe identificar, clasificar y documentar la Matriz de inventario de Activos, dando cumplimiento a los lineamientos del índice de Transparencia y Acceso a la Información pública	NO	N/A

					y el Modelo de Seguridad y Privacidad de la Información		
Control	A.8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	SI	Si, porque la Entidad debe definir el uso y apropiación de las Tecnologías de Información	SI	N/A
Control	A.8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al	SI	Si, porque dentro de la Política de Acceso a Tecnologías de Información se contempla la revocación de privilegios	NO	N/A

			terminar su empleo, contrato o acuerdo		y devolución de activos acorde a la naturaleza requerida		
	A.9	**Control de acceso**					
Objetivo de Control	A.9.1	Requisitos del negocio para control de acceso	Lineamiento: Limitar el acceso a información y a instalaciones de procesamiento de información.	SI	Si, porque se van a implementar los controles del objetivo de control	NO	N/A
Control	A.9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	SI	Si, porque la Entidad debe documentar, socializar y sensibilizar la Política de Acceso a las Tecnologías de la Información	NO	N/A
Control	A.9.1.2	Política sobre el uso de los servicios de red	Control: Solo se debe permitir acceso de los	SI	Si, porque la Entidad debe document	NO	N/A

			usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.		ar, socializar y sensibilizar la Política de Uso de las facilidades por parte de los usuarios		
Objetivo de Control	A.9.2	Gestión de acceso de usuarios	Lineamiento: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.	SI	Si, porque se van a implementar los controles del objetivo de control	NO	N/A
Control	A.9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	SI	Si, porque la Entidad tiene inmerso el registro y cancelación de usuarios en la Política de Acceso a las Tecnologías de la Información	NO	N/A

Control	A.9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	SI	Si, porque la Entidad tiene inmerso el suministro de acceso de usuarios en la Política de Acceso a las Tecnologías de la Información	NO	N/A
Control	A.9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	SI	Si, porque la Entidad tiene inmersa la gestión de derechos de acceso privilegiado en la Política de Acceso a las Tecnologías de la Información	NO	N/A
Control	A.9.2.4	Gestión de información de autenticación secreta	Control: La asignación de la información secreta se debe	SI	Si, porque la Entidad tiene inmerso la Gestión	NO	N/A

		de usuarios	controlar por medio de un proceso de gestión formal.		de información de autenticación secreta de usuarios en la Política de Acceso a las Tecnologías de la Información		
Control	A.9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	SI	Si, porque la Entidad tiene inmersa la revisión de los derechos de acceso a los usuarios en la Política de Acceso a las Tecnologías de la Información	NO	N/A

Control	A.9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.	SI	Si, porque la Entidad tiene inmerso el retiro o ajuste de los derechos de acceso en la Política de Acceso a las Tecnologías de la Información	NO	N/A
Objetivo de Control	A.9.3	Responsabilidades de los usuarios	Lineamiento: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.	SI	Si, porque se va a implementar el control del objetivo de control y en la política de uso de las facilidades por parte de los usuarios	NO	N/A

					se encuentran descritas las responsabilidades por parte de éstos		
Control	A.9.3.1	Uso de la información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	SI	Si, porque la Entidad debe documentar, socializar y sensibilizar la Política de Uso de las facilidades por parte de los usuarios	NO	N/A
Objetivo de Control	A.9.4	Control de acceso a sistemas y aplicaciones	Lineamiento: Evitar el acceso no autorizado a sistemas y aplicaciones.	SI	Si, porque se van a implementar los controles del objetivo de control	NO	N/A

Control	A.9.4.1	Restricción de acceso Información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	SI	Si, porque la Entidad tiene inmerso la restricción de acceso a la información en la Política de Acceso a las Tecnologías de la Información	NO	N/A
Control	A.9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	SI	Si, porque la Entidad tiene descritas las directrices de ingreso seguro en la Política de Acceso a las Tecnologías de la Información	NO	N/A
Control	A.9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y	SI	Si, porque la Entidad tiene inmerso el sistema de	NO	N/A

			deben asegurar la calidad de las contraseñas.		gestión de contraseñas en la Política de Acceso a las Tecnologías de la Información		
Control	A.9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	SI	Si, porque la Entidad tiene descritas las restricciones de uso en la Política de Acceso a las Tecnologías de la Información	NO	N/A
Control	A.9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	SI	Si, porque la Entidad tiene descritos los controles de acceso a códigos fuente de programas en la Política de	NO	N/A

					Acceso a las Tecnologías de la Información		
	A.10	**Criptografía**					
	A.11	**Seguridad física y del entorno**					
Objetivo de Control	A.11.1	Áreas seguras	Lineamiento: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	SI	Si, porque se van a implementar los controles del objetivo de control	NO	N/A
Control	A.11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.	SI	Si, porque la Entidad debe documentar, socializar y sensibilizar el procedimiento de Seguridad Física y del Entorno	NO	N/A

					que incluya los perímetros de seguridad física al interior de la Entidad		
Control	A.11.1.2	Controles físicos de entrada	Control: Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	SI	Si, porque la Entidad debe documentar, socializar y sensibilizar el procedimiento de Seguridad Física y del Entorno que incluya los controles físicos de Entrada	NO	N/A
Control	A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Control: Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	SI	Si, porque la Entidad debe documentar, socializar y sensibilizar el procedimiento de	NO	N/A

					Seguridad Física y del Entorno que incluya la seguridad de oficinas, recintos e instalaciones		
Control	A.11.1.4	Protección contra amenazas externas y ambientales	Control: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	SI	Si, porque la Entidad debe documentar, socializar y sensibilizar el procedimiento de Seguridad Física y del Entorno que incluya la protección contra amenazas externas y ambientales	NO	N/A

Control	A.11.1.5	Trabajo en áreas seguras	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	SI	Si, porque la Entidad debe documentar, socializar y sensibilizar el procedimiento de Seguridad Física y del Entorno que incluya el trabajo en áreas seguras	NO	N/A
Control	A.11.1.6	Áreas de despacho y carga	Control: Se deben controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información	SI	Si, porque la Entidad debe documentar, socializar y sensibilizar el procedimiento de Seguridad Física y del Entorno que incluya los puntos de acceso a áreas de	NO	N/A

			para evitar el acceso no autorizado.		despacho y carga		
Objetivo de Control	A.11.2	Equipos	Lineamiento: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	SI	Si, porque se van a implementar los controles del objetivo de control	NO	N/A
Control	A.11.2.1	Ubicación y protección de los equipos	Control: Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	SI	Si, porque la Entidad debe definir un procedimiento de mantenimiento de Equipos que incluya la Ubicación y Protección de los equipos para disminuir riesgos	NO	N/A

Control	A.11.2.2	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	SI	Si, porque la Entidad debe definir un procedimiento de mantenimiento de Equipos que incluya la protección contra fallas de energía y otras interrupciones	NO	N/A
Control	A.11.2.3	Seguridad del cableado	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debe estar protegido contra interceptación, interferencia o daño.	SI	Si, porque la Entidad debe definir un procedimiento de mantenimiento de Equipos que incluya la seguridad del cableado	NO	N/A
Control	A.11.2.4	Mantenimiento de equipos	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad	SI	Si, porque la Entidad debe definir un procedimiento de mantenimiento de	NO	N/A

			e integridad continua.		Equipos que incluya los mecanismos de disponibilidad e integridad		
Control	A.11.2.5	Retiro de activos	Control: Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	SI	Si, porque la Entidad debe definir un procedimiento de mantenimiento de Equipos que incluya el retiro de activos	NO	N/A
Control	A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	SI	Si, porque la Entidad debe definir un procedimiento de mantenimiento de Equipos que incluya la seguridad de los equipos y activos fuera de las instalaciones	NO	N/A

Control	A.11.2.7	Disposición segura o reutilización de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.	SI	Si, porque la Entidad debe documentar, socializar y sensibilizar el procedimiento de disposición de residuos tecnológicos	NO	N/A
Control	A.11.2.8	Equipos de usuario desatendidos	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les dé protección apropiada.	SI	Si, porque la Entidad debe definir un procedimiento de mantenimiento de Equipos que incluya el inventario de activos informáticos de la Entidad	NO	N/A

Control	A.11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	SI	Si, porque la Entidad incluye en la Política de Uso de las facilidades por parte de los usuarios directrices sobre el cuidado de los recursos	NO	N/A
	A.12	**Seguridad de las operaciones**					
Objetivo de Control	A.12.1	Procedimientos operacionales y responsabilidades	Lineamiento: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	SI	Si, porque se van a implementar los controles del objetivo de control	NO	N/A
Control	A.12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los	SI	Si, porque el proceso de infraestructura y operación del servicio debe	NO	N/A

			usuarios que los necesiten.		prestar Lon insumos y recursos para la disponibilidad en la prestación del servicio al usuario		
Control	A.12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	SI	Si, porque el proceso de infraestructura y operación del servicio debe prestar los mecanismos de control de cambios sobre la operación de los servicios de TI que afecten la seguridad de la Información	NO	N/A

Control	A.12.1.3	Gestión de capacidad	Control: Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	SI	Si, porque el proceso de infraestructura y operación del servicio debe brindar garantias en la capacidad y el uso de los recursos	NO	N/A
Control	A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	SI	Si, Porque la Dirección de la Oficina de TI de la Entidad debe brindar garantias en escenarios de prueba idénticos a los de operación y así asegurar una operación	NO	N/A

					de servicio funcional en un estado deseado		
Objetivo de Control	A.12.2	Protección contra códigos maliciosos	Lineamiento: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.	SI	Si, porque se va implementar el Control del Objetivo de Control	NO	N/A
Control	A.12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	SI	Si, porque en los Acuerdos de Nivel de Servicio la Entidad debe exigir los filtros de control a código malicioso tanto a proveedores de desarrollo como de servicio	NO	N/A

Objetivo de Control	A.12.3	Copias de respaldo	Lineamiento: Proteger contra la pérdida de datos.	SI	Si, porque se va implementar el Control del Objetivo de Control	SI	N/A
Control	A.12.3.1	Respaldo de información	Control: Se deben hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	SI	Si, porque la Entidad debe tener un procedimiento de copias de respaldo para la protección de los activos de información	SI	N/A
Objetivo de Control	A.12.4	Registro y seguimiento	Lineamiento: Registrar eventos y generar evidencia.	SI	Si, porque se va implementar el Control del Objetivo de Control	SI	N/A

Control	A.12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	SI	Si, porque la Entidad debe hacer seguimiento y control en la herramienta HESK sobre las incidencias y requerimientos que tienen los colaboradores al interior de sus procesos	SI	N/A
Control	A.12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deberían proteger y revisar con regularidad.	SI	Si, porque la Entidad cuenta con Matriz CRUD como registro de los roles que tiene cada colaborador dentro de los sistemas de información	NO	N/A

Control	A.12.4.4	sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	SI	Si, porque todos los sistemas de información de la Entidad estan sincronizados con el reloj del servidor de dominio, el cual se actualiza por medio de internet	SI	N/A
Objetivo de Control	A.12.5	Control de software operacional	Lineamiento: Asegurar la integridad de los sistemas operacionales.	SI	Si, porque se debe implementar el Control del Objetivo de Control	SI	N/A
Control	A.12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	SI	Si, porque en la Política de Seguridad de la Información, la Entidad tiene descritas las directrices	NO	N/A

					en relación con la instalación por parte de los usuarios del software en sistemas operativos ajeno a la Entidad		
Objetivo de Control	A.12.6	Gestión de la vulnerabilidad técnica	Lineamiento: Prevenir el aprovechamiento de las vulnerabilidades técnicas.	SI	Si, porque se van a implementar los controles del Objetivo de Control	NO	N/A
Control	A.12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidad	SI	Si porque la Entidad debe implementar los controles del Plan de tratamiento de riesgos, gestionando y reduciendo la materialización de	NO	N/A

			es, y tomar las medidas apropiadas para tratar el riesgo asociado.		éstos al interior de la misma		
Control	A.12.6.2	Restricciones sobre la instalación de software	Control: Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	SI	Si, porque en la Política de Seguridad de la Información, la Entidad tiene descritas las directrices en relación con la instalación por parte de los usuarios del software en sistemas operativos ajeno a la Entidad	NO	N/A

Objetivo de Control	A.12.7	Consideraciones sobre auditorias de sistemas de información	Lineamiento: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.	SI	Si, porque se debe implementar el Control del Objetivo de Control	NO	N/A
Control	A.12.7.1	Información controles de auditoría de sistemas	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	SI	Si, porque la Entidad debe diseñar e implementar el Plan de Auditorias del Modelo de Seguridad y Privacidad de la Información, el cual incluye auditorias sobre los sistemas de información	NO	N/A
	A.13	**Seguridad de las comunicaciones**					
Objetivo de Control	A.13.1	Gestión de la seguridad de las redes	Lineamiento: Asegurar la protección de la información	SI	Si, porque se deben implementar los Controles	NO	N/A

			en las redes, y sus instalaciones de procesamiento de información de soporte.		del Objetivo de Control		
Control	A.13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	SI	Si, porque la Entidad debe separar los segmentos de red para brindar garantias de disponibilidad, continuidad y contingencia de la Informaci ón	NO	N/A
Control	A.13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos	SI	Si, porque la Entidad de acuerdo a los roles de la segmentación de redes debe ofrecer unas capas de seguridad	NO	N/A

			de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.		sobre los servicios de red		
Control	A.13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	SI	Si, porque de acuerdo a la funcionalidad requerida por los usuarios se deben prestar segmentos operativos que brinden capacidad, disponibilidad y seguridad de la información	NO	N/A
Objetivo de Control	A.13.2	Transferencia de información	Lineamiento: Mantener la seguridad de la información transferida dentro de una organización	SI	Si, porque se deben implementar los Controles del Objetivo	NO	N/A

			y con cualquier Entidad externa.		de Control		
Control	A.13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.	SI	Si, porque la Entidad cuenta con Política de Gestión de la Información y formato de transferencia de conocimientos	NO	N/A
Control	A.13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	SI	Si, porque la Entidad cuenta con Política de Gestión de la Información y formato de transferencia de	NO	N/A

					conocimientos		
Control	A.13.2.3	Mensajería electrónica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	SI	Si, porque la Entidad dentro de la Política de Uso de las facilidades por parte de los usuarios contiene descritas las directrices sobre el uso de correo electrónico	NO	N/A
Control	A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización	SI	Si, porque la Entidad cuenta con Política de Gestión de la Información	NO	N/A

			para la protección de la información.				
	A.14	**Adquisición, desarrollo y mantenimientos de sistemas**					
Objetivo de Control	A.14.1.1	Requisitos de seguridad de los sistemas de información	Lineamiento: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.	SI	Si, porque se deben implementar los Controles del Objetivo de Control	NO	N/A
Control	A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos	SI	Si, porque la Entidad cuenta con la Política de Adquirió tecnológica que incluye	NO	N/A

			sistemas de información o para mejoras a los sistemas de información existentes.		los requisitos para nuevos sistemas de información o para mejora de los sistemas de información existentes		
Control	A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	SI	Si, porque la Entidad cuenta con la Política de Desarrollo e Implantación de los Sistemas de Información	NO	N/A

Control	A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	SI	Si, porque la Entidad cuenta con la Política de Adquirió tecnológica que incluye la protección de la información involucrada en las transacciones de los servicios de las aplicaciones	NO	N/A
Objetivo de Control	A.14.2	Seguridad en los procesos de desarrollo y soporte	Lineamiento: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los	SI	Si, porque se deben implementar los Controles del Objetivo de Control	NO	N/A

			sistemas de información.				
Control	A.14.2.1	Política de desarrollo seguro	Control: Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	SI	Si, porque la Entidad cuenta con la Política de Desarrollo e Implantación de los Sistemas de Información	NO	N/A
Control	A.14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	SI	Si, porque la Entidad tiene un procedimiento formal de Control de Cambios para las etapas de diseño y transición de los proyectos que incluye los elemento	NO	N/A

					s de cambios		
Control	A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	SI	Si, porque la Entidad debe instaurar escenarios de pruebas funcionales de acuerdo al Plan de Seguridad de pruebas de la Información	NO	N/A
Control	A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se	SI	Si, porque el software estándar en la Entidad no se debe convertir en software personalizados que	NO	N/A

			deberían controlar estrictamente.		alteren el funcionamiento, dificultando la transferencia de conocimiento e información		
Control	A.14.2.5	Principios de construcción de sistemas seguros	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	SI	Si, porque la Entidad cuenta con la Política de Desarrollo e Implantación de los Sistemas de Información que incluye la implementación de sistemas seguros al interior de la misma	NO	N/A
Control	A.14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de	SI	Si, porque la Entidad cuenta con la Política de Desarrollo e	NO	N/A

			desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.		Implantación de los Sistemas de Información que incluye ambientes de desarrollo seguro		
Control	A.14.2.7	Desarrollo contratado externamente	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	SI	Si, porque la Entidad cuenta con la Política de Adquirió tecnológica que incluye la supervisión y seguimiento de los desarrollos de sistemas contratados externamente	NO	N/A
Control	A.14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	SI	Si, porque la Entidad debe instaurar escenarios de pruebas funcionales de	NO	N/A

					acuerdo al Plan de Seguridad de pruebas de la Informaci ón		
Con trol	A.14 .2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizacion es y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	SI	Si, porque la Entidad debe instaurar escenario s de pruebas funcionale s de acuerdo al Plan de Seguridad de pruebas de la Informaci ón	NO	N/A
Obj etiv o de Con trol	A.14 .3	Datos de prueba	Lineamiento: Asegurar la protección de los datos usados para pruebas.	SI	Si, porque se debe implemen tar el Control del Objetivo de Control	NO	N/A
Con trol	A.14 .3.1	Protección de datos de prueba	Control Los datos de ensayo se deben seleccionar, proteger y controlar	SI	Si, porque la Entidad debe brindar garantias de informaci	NO	N/A

			cuidadosamente.		ón de prueba que no impacten en la operación del servicio		
	A.15	**Relación con los proveedores**					
Objetivo de Control	A.15.1	Seguridad de la información en las relaciones con los proveedores	Lineamiento: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.	SI	Si, porque se deben implementar los Control del Objetivo de Control	NO	N/A
Control	A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deberían documentar.	SI	Si, porque en la Política de Seguridad de la Información, se tienen relacionadas las directrices con base el recurso humano: Proveedores	NO	N/A

Control	A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	SI	Si, porque en los Acuerdos de Nivel de Servicio la Entidad debe exigir los requisitos de seguridad por parte de cada proveedor que da soporte a la Infraestructura de TI	NO	N/A
Control	A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y	SI	Si, porque en los Acuerdos de Nivel de Servicio la Entidad debe incluir requisitos para tratar los riesgos de seguridad en la	NO	N/A

			comunicación.		cadena de suministros de productos y servicios de tecnología de Información y Comunicación		
Objetivo de Control	A.15.2	Gestión de la prestación de servicios con los proveedores	Lineamiento: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.	SI	Si, porque se van a implementar los controles del objetivo de control	NO	N/A
Control	A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	SI	Si, porque en los Acuerdos de Nivel de Servicio la Entidad debe incluir auditorias para validar el cumplimiento de los	NO	N/A

					acuerdos en la prestación de servicios de los proveedores		
Control	A.15.2.2	Gestión de cambios en los servicios de proveedores	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.	SI	Si, porque en la Política de Desarrollo e Implantación de los sistemas de información, se contempla la norma de desarrollo externo del proveedor que contiene lo siguiente: III. Garantías de la calidad y precisión del trabajo llevado a cabo por el	NO	N/A

					proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos.		
	A.16	**Gestión de incidentes de seguridad de la información**					
Objetivo de Control	A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	Lineamiento: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.	SI	Si, porque se van a implementar los controles del Objetivo de control	NO	N/A

Control	A.16.1.1	Responsabilidad y procedimientos	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	SI	Si, porque la Entidad debe brindar herramientas de gestión sobre las incidencias de la seguridad de la información, que indiquen un desarrollo de actividades y unos roles de responsabilidad	NO	N/A
Control	A.16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	SI	Si, porque la Entidad debe hacer seguimiento y control en la herramienta HESK sobre las incidencias y requerimientos que tienen los colaboradores al	SI	N/A

					interior de sus procesos		
Control	A.16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	SI	Si, porque la Entidad debe hacer seguimiento y control en la herramienta HESK sobre las incidencias y requerimientos que tienen los colaboradores al interior de sus procesos	SI	N/A
Control	A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deben evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de	SI	Si, porque la Entidad debe hacer seguimiento y control en la herramienta HESK sobre las incidencias y requerimi	SI	N/A

			la información.		entos que tienen los colaboradores al interior de sus procesos		
Control	A.16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	SI	Si, porque la Entidad debe dar respuesta en la herramienta HESK sobre las incidencias y requerimientos que tienen los colaboradores al interior de sus procesos	SI	N/A
Control	A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	SI	Si, porque la Entidad debe hacer establecer planes preventivos sobre los incidentes recurrentes con el fin de evitar la materialización de	SI	N/A

					riesgos en la misma		
Control	A.16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	SI	Si, porque la Entidad debe hacer seguimiento y control en la herramienta HESK sobre las incidencias y requerimientos para el mejoramiento continuo y la toma de decisiones	SI	N/A
	A.17	**Aspectos de seguridad de la información de la gestión de continuidad de negocio**					
Objetivo de Control	A.17.1	Continuidad de seguridad de la información	Lineamiento: La continuidad de seguridad de la información se debe incluir en los	SI	Si, porque se van a implementar los controles del Objetivo de control	NO	N/A

			sistemas de gestión de la continuidad de negocio de la organización.				
Control	A.17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	SI	Si, porque la Entidad debe documentar el Plan de Continuidad del negocio con los requisitos para brindar garantías en la continuidad en la prestación de los servicios	NO	N/A
Control	A.17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de	SI	Si, porque la Entidad debe documentar el Plan de Continuidad del negocio con los requisitos para brindar garantías	NO	N/A

			continuidad requerido para la seguridad de la información durante una situación adversa.		en la continuidad en la prestación de los servicios		
Control	A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	SI	Si, porque la Entidad debe documentar el Plan de Continuidad del negocio con los requisitos para brindar garantías en la continuidad en la prestación de los servicios	NO	N/A
Objetivo de Control	A.17.2	Redundancias	Lineamiento: Asegurar la disponibilidad de instalaciones de procesamiento de información.	SI	Si, porque la Entidad debe documentar el Plan de Continuidad del negocio con los requisitos para	NO	N/A

					brindar garantias en la continuidad en la prestación de los servicios		
Control	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Control: Las instalaciones de procesamiento de información se debe implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	SI	Si, porque la Entidad debe documentar el Plan de Continuidad del negocio con los requisitos para brindar garantías en la continuidad en la prestación de los servicios	NO	N/A
	A.18	**Cumplimiento**					
Objetivo de Control	A.18.1	Cumplimiento de requisitos legales y contractuales	Lineamiento: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas	SI	Si, porque se van a implementar los controles del Objetivo de Control	NO	N/A

			con seguridad de la información, y de cualquier requisito de seguridad.				
Control	A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	SI	Si, porque los requisitos legales y contractuales de la Entidad se deben cumplir con base al Manual de Contratación establecido mediante el acuerdo Nª11 del 29 de diciembre de 2016	SI	N/A

Control	A.18.1.2	Derechos de propiedad intelectual	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de softwares patentados.	SI	Si, porque la Entidad cuenta con la Política de Adquirió tecnológica que contempla los derechos de propiedad intelectual	NO	N/A
Control	A.18.1.3	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de	SI	Si, porque la Entidad cuenta con el programa de Gestión documental de acuerdo al Archivo General de la Nación para la protecció	NO	N/A

			reglamentación, contractuales y de negocio.		n de registros		
Control	A.18.1.4	Privacidad y protección de datos personales	Control: Cuando sea aplicable, se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.	SI	Si, porque la Entidad cuenta con la Política de Protección de datos personales	NO	N/A
Objetivo de Control	A.18.2	Revisiones de seguridad de la información	Lineamiento: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.	SI	Si, porque se van a implementar los controles del objetivo de control	NO	N/A

Control	A.18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	SI	Si, porque en la Política de Seguridad de la Información, se tienen relacionadas los controles para la seguridad	NO	N/A
Control	A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y	SI	Si, porque la Entidad desde la Alta Dirección debe propender por el cumplimiento de las	NO	N/A

			procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.		políticas y normas de seguridad		
Control	A.18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	SI	Si, porque se deben realizar auditorías constantes a los sistemas de información para revisar el cumplimiento de las políticas y normas de seguridad	NO	N/A

Fuente: Elaboración propia

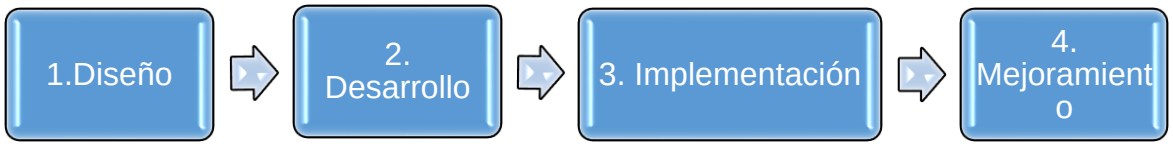
5.11. Competencia, toma de conciencia y comunicación

La Entidad tiene definido el plan de capacitación, sensibilización y comunicación del Modelo de Seguridad y Privacidad de la Información, el cual incluye el Plan de Seguridad y Privacidad de la Información y se relaciona a continuación:

DESCRIPCIÓN DEL PLAN DE SENSIBILIZACIÓN, CAPACITACIÓN Y COMUNICACIÓN

Este plan pretende sensibilizar, capacitar y comunicar las reglas de comportamiento adecuadas para el uso seguro de los servicios de TI plasmados en el portafolio de servicios, políticas y procedimientos de seguridad de la información que la Entidad, requiere que sean adoptados y adaptados por parte de todos los usuarios del sistema. Teniendo en cuenta lo anterior, este plan de capacitación, sensibilización y comunicación adecuado, debe llevarse a cabo con base a las siguientes fases:

IMAGEN Nª2 FASES PLAN DE SENSIBILIZACIÓN, CAPACITACIÓN Y COMUNICACIÓN SERVICIUDAD E.S.P



Fuente: Elaboración propia

1. **DISEÑO:** En esta fase se Identifican las actividades necesarias para cumplir con el Plan de acuerdo a la matriz de interesados de la Entidad.

TABLA Nª6. MATRIZ DE INTERESADOS DEL PLAN

INTERESADO	EXPECTATIVA/ NECESIDAD
Gerencia/ Comité Directivo	Deben conocer y entender las leyes y directivas que forman la base del Modelo de Seguridad y Privacidad de la Entidad. A su vez, deben comprender el liderazgo que su rol tiene y que son el ejemplo a seguir de todas las demás Dependencias.
Comité de Seguridad de la Información	Deben velar por la actualización y cumplimiento de las políticas y gestionar de manera oportuna las incidencias y requerimientos presentados en materia de Seguridad y Privacidad de la Información al interior de la Entidad.
Director Oficina de TI	Debe velar por la gestión de los controles de seguridad en los sistemas de información, con el fin de brindar

	continuidad y disponibilidad en la prestación de los servicios de TI.
Proveedores de Servicios de TI	Deben proporcionar Acuerdos de Nivel de Servicio que contengan mecanismos de continuidad y disponibilidad en la prestación de los servicios de TI
Usuarios Finales	Colaboradores, contratistas, pasantes universitarios y SENA, personal temporal y otras personas relacionadas a terceras partes, que deben conocer los aspectos relacionados con el Modelo de Seguridad y Privacidad de la Información.

Fuente: Elaboración propia

2. DESARROLLO:

La información resultante y documentada del Plan de Sensibilización, capacitación y comunicación debe conservarse en un repositorio de fácil acceso para su consulta y guía, para tal efecto SERVICIUDAD E.S.P dispone de la siguiente ruta: _ Sistema de gestión de Calidad y Documentación (serviciudad.gov.co) como fuente de almacenamiento y consulta.

3. IMPLEMENTACIÓN:

El material dispuesto como consulta y guía del Plan de Sensibilización, Capacitación y Comunicación de Seguridad de la Información, puede visualizarse en documentación ofimática y audiovisual para su mejor entendimiento y comprensión.

4. MEJORAMIENTO:

La información inherente del plan debe ser validada y actualizada por el Comité de Seguridad de la Información con periodicidad de revisión cuatrimestral y de acuerdo a los requerimientos exigidos por MinTIC. Cabe resaltar que, este Comité tiene dentro de sus funciones realizar monitoreos constantes de la efectividad del plan y de esta forma realizar acciones de mejora con base a los hallazgos identificados.

ROLES RESPONSABLES DE LOS TEMAS A COMUNICAR EN EL PLAN

TABLA Nª8. TEMAS A COMUNIAR POR RESPONSABLE

RESPONSABLE/ÁREA	TEMA	FUNCIONARIO
	Seguimiento y Control Sobre los Planes de Auditoria de Seguridad de la Información	

RESPONSABLE/ÁREA	TEMA	FUNCIONARIO
Control interno	Revisión independiente de la seguridad de la información	Profesional Especializada de Control Interno
	Velar por el cumplimiento de las políticas y normas de seguridad de la información	
	Auditorías Internas e identificación de hallazgos sobre la seguridad de la Información	
	Documentación de Planes de mejoramiento sobre los hallazgos encontrados en Seguridad de la información	
	Aplicación de las sanciones correspondientes de acuerdo a las faltas en materia de seguridad de la Información	
Gestión Humana	Selección e investigación de antecedentes del Colaborador	Profesional Especializado en Talento Humano
	Términos y condiciones del empleo	
Responsable de compras y adquisiciones	Relación con los Proveedores	Subgerente Financiera y Administrativa /Secretario General
	Seguridad de la información en las relaciones con los proveedores	
	Gestión de la prestación de servicios de proveedores	
Responsable de la continuidad	Gestión sobre los aspectos de seguridad de la información para la continuidad del negocio	Director Oficina de TI
	Continuidad de la seguridad de la información	
	Planificación de la continuidad de la seguridad de la información	

RESPONSABLE/ÁREA	TEMA	FUNCIONARIO
	Implementación de la continuidad de la seguridad de la información	
	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	
	Disponibilidad de sistemas de Información para la continuidad de la Información	
Responsable de la seguridad física	Seguridad Física y del Entorno	Comité de Seguridad de la Información
	Áreas seguras	
	Perímetro de seguridad física	
	Controles de Acceso al cuarto de Servidores	
	Seguridad Física y del Entorno	
Responsable de Seguridad de la Información	Políticas de Seguridad de la Información	Comité de Seguridad de la Información
	Organización de la Seguridad de la Información	
	Seguridad del Talento Humano	
	Gestión de los activos de Información	
	Modelo de Seguridad y Privacidad de la Información	
	Política de Acceso a las Tecnologías de la información	
	Cumplimiento de requisitos legales y contractuales	
	Criptografía	
	Proyectos de Seguridad de la Información	
	Metodologías de Seguridad de la información	
	Procedimientos de operación documentados y responsables	

RESPONSABLE/ÁREA	TEMA	FUNCIONARIO
	Protección Contra códigos maliciosos	
	Copias de respaldo	
	Gestión de Vulnerabilidades	
	Registros de eventos	
	Adquisición, desarrollo y mantenimiento de los sistemas de Información	
	Transferencia de Información	
	Controles sobre auditorías de sistemas de información	
	Requisitos de seguridad de los sistemas de información	
	Identificación y valoración de riesgos	
	Tratamiento de riesgos de seguridad de la información	
	Sensibilización y socialización sobre los temas de la seguridad de la información	
	Planificación y control operacional	
	Implementación del plan de tratamiento de riesgos	
	Indicadores de gestión del MSPI	
	Plan de seguimiento, evaluación y análisis del MSPI	
	Evaluación del plan de tratamiento de riesgos	
	Plan de seguimiento, evaluación y análisis del MSPI	
	Tratamiento de temas de seguridad y privacidad de la información en los comités del modelo integrado de gestión, o en los comités directivos	

RESPONSABLE/ÁREA	TEMA	FUNCIONARIO
	interdisciplinarios de la Entidad	
	Inventario de Activos de Información.	
	Gestión de riesgos que incluya riesgos de ciberseguridad	
	Respuesta a incidentes de ciberseguridad, planes de recuperación y restauración	
Responsable de Tics	Teletrabajo	Director Oficina de TI
	Manejo de medios	
	Derechos de propiedad intelectual.	
	Control de Acceso	
	Seguridad de la Operaciones	
	Procedimientos Operacionales y de respaldo	
	Copias de Seguridad	
	Políticas de TI	
	Adquisición, desarrollo y mantenimiento de los sistemas de Información	
	Gestión de la Seguridad de las Redes	
	Gestión de Incidentes de Seguridad de la Información	
	Plan y Estrategia de transición de IPv4 a IPv6	
	Implementación del plan de estrategia de transición de IPv4 a IPv6	
	Indicadores de TI	

RESPONSABLE/ÁREA	TEMA	FUNCIONARIO
Calidad	Procedimientos de control documental del MSPI	Profesional Especializada de Calidad

Fuente: Elaboración propia

AUDIENCIA OBJETIVO

La audiencia objetivo que debe ser sensibilizada, capacitada y entrenada son los usuarios de lectura, consulta y ejecución de tareas en los servicios de TI.

FRECUENCIA DE CAPACITACIÓN Y ENTRENAMIENTO DEL PLAN

La frecuencia de las inducciones, reinducciones y capacitaciones se da de acuerdo a los requerimientos de las subgerencias en materia de ingresos de personal nuevo, traslados y acciones de mejora al interior de la Entidad, validada por la Oficina de Control Interno.

ANEXOS

- Política de Seguridad y Privacidad de la Información
- Procedimientos de Seguridad de la Información
- Comité de Seguridad de la Información
- Matriz de Activos de Información
- Matriz de riesgos y Plan de tratamiento de riesgos del MSPI
- Plan de Comunicación y Sensibilización del MSPI
- Estrategia de Planificación y Control Operacional del MSPI
- Procedimiento de inventario y clasificación de activos e infraestructura critica
- Declaración de Aplicabilidad de los Controles del MSPI

BIBLIOGRAFÍA

Ministerio de Tecnologías de la Información y las Comunicaciones. Anexo 1. Modelo de Seguridad y Privacidad de la Información. [en línea], [revisado el 05 de Abril de 2021]. Disponible en internet: Anexo1 Pyr Seg DigitalMSPI_Limpio_05.02.2021.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. Resolución 00500 de marzo de 2021. [en línea], [revisado el 08 de Abril de 2021]. Disponible en internet: Resolución número 00500 de 2021.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones.Guías MSPI. [en línea], [revisado el 20 de abril de 2021]. Disponible en internet: MSPI (mintic.gov.co)