TABLA DE CONTENIDO

1. INTRODUCCIÓN.

El Manual de la política de Gobierno Digital expedido por el Ministerio de Tecnologías de información y de las Comunicaciones establece que la política tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

Por lo tanto, las entidades públicas deben implementar lineamientos de seguridad de la información en todos sus procesos, tramites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

La adopción, implementación y evaluación del modelo mencionado, es una actividad obligatoria según lo expresado en el artículo 2.2.9.1.3.2., en el numeral 2, en los literales A, B y C, el cual debe ser planificado en atención a lo establecido en el decreto 612 de 2018, que en el artículo 1, señala la importancia de la integración de los planes institucionales y estratégicos al Plan de Acción institucional, en el ámbito de aplicación del modelo integrado de

planeación y gestión.

Así mismo, la resolución 0500 de marzo 10 del 2021 expedida por el Ministerio de Tecnologías de Información y de las Comunicaciones, que tiene como objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información, la guía de gestión de riesgos de Seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y establecer los lineamientos y estándares para la estrategia de seguridad digital. La resolución en mención precisa la necesidad de que los sujetos obligados deban adoptar las medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al Plan de Seguridad y Privacidad de la Información y así mitigar los riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital. Es precisamente a través del artículo 5 de la resolución 0500 que se precisa la necesidad de adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital, e incluirla en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos del artículo 2.22.22.3.14 del capítulo 3 del título 22 de la parte 2 del libro 2 del decreto 1083 de 2015. En atención a lo anterior, se presenta el plan de seguridad y privacidad de la información enfocado en la seguridad informática frente a ciberamenazas de activos de tecnologías de información de la entidad.

2. OBJETIVO GENERAL

Establecer el marco de acción para la implementación del Modelo de seguridad y privacidad de la información, enfocado en la seguridad informática sobre los activos de tecnología que soportan los servicios digitales **del Hospital San Vicente de Paúl de Santa Rosa de Cabal Risaralda**, de acuerdo al contexto de la Empresa, las capacidades y recursos disponibles, para fortalecer la confianza de los ciudadanos, grupos de valor y demás partes interesadas.

3. ALCANCE

La presente planeación se define para las vigencias 2022 a 2025 y sus acciones estarán enfocadas en los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, orientados a la seguridad informática de la plataforma tecnológica y la información del Hospital San Vicente de Paúl de Santa Rosa de Cabal, Risaralda y debe ser cumplido e implementado por todos los procesos, por los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con el Hospital, para conseguir un adecuado nivel de protección de las características de privacidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad del Modelo y del presente Plan.

4. GLOSARIO

- **Acceso a la Información Pública**: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Activo de la información:** activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede
- entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).
- **Amenaza:** 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 riesgo.
- **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).
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **Ciberseguridad**: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Ciberespacio**: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **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 Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias
- personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).
- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (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)
- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.
- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.
- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.
- **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.
- **Privacidad:** Derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades.
- **Registro Nacional de Bases de Datos**: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25).
- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).
- **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.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información.
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).
- **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.

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.
- **Partes interesadas:** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Certificado digital:** O Firma Digital es un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje.

5. NORMATIVIDAD RELACIONADA

TIPO DE NORMA	FECHA	NORMA	DESCRIPCIÓN
Ley	1982	23	Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.
Constitución Política	Actualizada	1991	Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data
Ley	1999	527	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Ley	2009	1341	"Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
Ley	2009	1273	"Por la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones."
Decreto	2011	4632	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
Ley	2011	1474	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley	2012	1581	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto	2013	1377	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.
NTC - ISO/IEC	2013	27001	Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa
Decreto	2014	2573	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.
Ley	2014	1712	Para la Implementación de la Estrategia de Gobierno en Línea, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno en Línea

TIPO DE NORMA	FECHA	NORMA	DESCRIPCIÓN
Decreto	2015	1494	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
CONPES	2016	3854	"Política Nacional de Seguridad Digital"
Decreto	2018	1008	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
Ley	2019	1978	"Por la cual se moderniza el sector de las tecnologías de la información y las comunicaciones -TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones"
Ley	2019	1955	"Por la cual se expide el Plan Nacional de Desarrollo, en los artículos 147 y 148 se establece lo referente a la Transformación Digital Pública y Gobierno Digital como política de gestión y desempeño Institucional"
Resolución	2021	0500	"Por la cual se establece los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital"

6. OBJETIVO DE LA POLÍTICA DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN.

Generar una adecuada seguridad y protección de la información de los procesos del Hospital a través de pautas, directrices y reglas, estableciendo dentro del Plan Estratégico de Tecnologías de la Información, su liderazgo y desarrollo y renovar la gestión de la Entidad, entendiendo la importancia de una adecuada gestión de la información, y la implementación de un Sistema de Gestión de Seguridad de la Información buscando establecer un marco de confianza en el ejercicio de sus deberes como entidad pública y los usuarios. Para el Hospital, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad, acorde con las necesidades de los diferentes grupos de interés identificados. De acuerdo con lo anterior, esta política aplica al Hospital, teniendo en cuenta sus funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con el Hospital y los Usuarios en general. En cumplimiento de sus Valores Corporativos.

7. COMPROMISO DE LA ALTA DIRECCIÓN.

La Alta Dirección del Hospital San Vicente de Paúl de Santa Rosa de Cabal Risaralda E.S.E. se compromete con la implementación y mantenimiento del Plan de Gestión de Seguridad y Privacidad de la Información, definiendo la política de seguridad y privacidad de la información, el gobierno digital y la asignación de los recursos necesarios para llevar a dar cumplimiento las actividades programadas.

8. PLAN DE IMPLEMENTACIÓN.

ISO 27001:2013	ACTIVIDADES	RESPONSABLES	CRONOGRAMA	
A5 Políticas de Tecnología de la Información.	Actualizar, las políticas TIC.	Sistemas, Planeación y Sistemas de Información		
	Consolidar las políticas TIC en acto administrativo.	Planeación y Sistemas de Información		
	Presentar para aprobación.	Planeación y Sistemas de Información		
	Socialización de la política.	Sistemas, Planeación y Sistemas de Información		
	Implementación de los lineamientos de las política TI.	Sistemas, Planeación y Sistemas de Información		
A6 Organización de la seguridad y privacidad de la información.	Realizar la evaluación al modelo de seguridad y privacidad de la información en la herramienta y el instrumento de evaluación del MSPI.	Sistemas, Planeación y Sistemas de Información		
	Revisar y actualizar el plan de seguridad y privacidad de la información.	Sistemas, Planeación y Sistemas de Información		
	Implementar la evaluación de riesgos, centrada en la seguridad y privacidad de la información, al comienzo de cualquier proyecto para identificar amenazas.	Sistemas, Planeación y Sistemas de Información		
	Disponibilidad de personal suficiente que garantice la operación de las TI.	Planeación y Sistemas de Información		
	Definir y comunicar las responsabilidades de cada empleado o puesto de trabajo en relación a la Seguridad y privacidad de la información.	Planeación y Sistemas de Información		
	Asignar y separar las funciones de los distintos perfiles o áreas de responsabilidad.	Planeación y Sistemas de Información Gestión Humana		
	Revisar, actualizar y completar prácticas de seguridad a usuarios externos, proveedores, etc.	Sistemas, Planeación y Sistemas de Información		
	Revisar, actualizar y complementar la definición de lineamientos de dispositivos móviles con el fin de mitigar los riesgos de la seguridad y privacidad de la información en el uso de estas en la ESE.	Sistemas, Planeación y Sistemas de Información		
	Establecer el Plan de trabajo para la adopción de IPv6 en toda la organización.	Sistemas		
A7 Seguridad de los recursos humanos.	Realizar sensibilización en seguridad y privacidad de la información para el personal.	Sistemas		
	Inclusión de los temas de seguridad y privacidad de la información en el proceso de selección, inducción y reinducción.	Planeación y Sistemas de Información Gestión Humana		
	Inclusión de los temas de seguridad y privacidad de la información en el proceso de ingreso de contratistas y personal de planta.	Planeación y Sistemas de Información Gestión Humana		
	Implementación del proceso control interno disciplinario.	Planeación y Sistemas de Información Control Interno		
A8. Gestión de activos.	Elaborar y validar el inventario de activos de información de servicios tecnológicos de la entidad y su interrelación entre ellos, identificando claramente cuáles elementos (equipos y software) soportan IPv6. Como inicio al proceso de transición de IPv4 a IPv6.	Sistemas		
	Realizar la entrega formal de los activos a cada uno de los colaboradores que tiene responsabilidades sobre el activo.	Planeación y Sistemas de Información		
	Realizar la publicación de los instrumentos de la ley 1712 en la página web del Hospital.	Planeación y Sistemas de Información Comunicaciones		

ISO 27001:2013	ACTIVIDADES	RESPONSABLES	CRONOGRAMA	
	Revisar, actualizar el plan de tratamiento de riesgos de seguridad y privacidad de la información.	Sistemas, Planeación y Sistemas de Información		
	Identificar los riesgos de seguridad y privacidad de la información.	Sistemas, Planeación y Sistemas de Información		
	Implementar los controles establecidos para cada uno de los riesgos identificados.	Sistemas, Planeación y Sistemas de Información		
	Establecer lineamientos de protección de la información almacenada con copias de seguridad en soportes independientes.	Sistemas		
	Revisar, actualizar y completar lineamientos para controlar la transferencia de información hacia medios extraíbles.	Sistemas, Planeación y Sistemas de Información		
	Establecer y aplicar lineamientos para la devolución de activos.	Planeación y Sistemas de Información Sistemas		
	Gestionar la información y los datos a través del tablero único de indicadores que permita la disponibilidad de la información oportuna, veraz y estandarizada para la toma de decisiones estratégicas y administrativas.	Estadística		
	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos.	Estadística Líderes de Proceso		
	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información.	Estadística Líderes de Proceso		
A9 Control de acceso.	Revisar y si aplica, actualizar el manual de Administración de usuarios garantizando una la seguridad en el manejo del acceso a la información, de acuerdo a su clasificación.	Planeación y Sistemas de Información		
	Realizar la centralización de autenticación de usuarios y la integración de las aplicaciones que lo permitan. Establecer lineamientos para el control de acceso a la información, sistemas y aplicaciones.	Sistemas, Planeación y Sistemas de Información		
A10 Criptografía.	Realizar el proceso de aseguramiento de los sitios que requieran autenticación a través de certificados digitales.	Sistemas, Planeación y Sistemas de Información		
	Realizar el proceso para la adquisición de los certificados y firmas digitales que se requieran para la operación.	Planeación y Sistemas de Información		
	Seguimiento a la aplicación de controles criptográficos para la protección de la información.	Sistemas		
	Definir lineamientos de seguridad para el uso de los certificados y firmas digitales.	Sistemas, Planeación y Sistemas de Información		
A11 Seguridad física y del entorno.	Identificar y/o establecer los controles de acceso y protección contra amenazas en: • Datacenter y centros de cableado. • Áreas con servidores, ya sean de procesamiento o dispositivos de comunicación. • Áreas donde se encuentren concentrados dispositivos de información. • Áreas donde se almacenen y guarden elementos de respaldo datos (CD, Discos, Cintas etc.).	Sistemas, Mantenimiento		
	Monitoreo de los controles de accesos biométricos.	Sistemas, Mantenimiento		
	Cumplimiento de normas de seguridad física.	Seguridad y Salud en el Trabajo		
	Adecuación y mantenimiento del Centro de Datos y centro de cableado.	Sistemas		
	Planear y ejecutar el Mantenimiento de planta eléctrica, física, UPS, software y hardware.	Sistemas, Mantenimiento		
	Asignar el software y hardware a los servicios teniendo en cuenta la políticas de seguridad y privacidad de la información.	Sistemas		
	Implementar el procedimiento de gestión de incidentes.	Sistemas		
	Realizar el monitoreo y análisis de Vulnerabilidades.	Sistemas		

ISO 27001:2013	ACTIVIDADES	RESPONSABLES	CRONOGRAMA	
	Revisar, actualizar y complementar el sistema para la gestión de Backups.	Sistemas		
	Realizar la administración de herramientas de seguridad de manera centralizada como Antivirus Firewall, etc.	Sistemas		
	Ejecutar la separación de ambientes (físicos y lógicos).	Sistemas		
	Realizar la revisión de código malicioso.	Sistemas		
	Establecer y ejecutar el plan de continuidad del negocio y recuperación de desastres.	Sistemas, Planeación y Sistemas de Información		
	Disponer del soporte necesario para mantener operativas las instalaciones y los equipos.	Sistemas, Mantenimiento		
	Operar el procedimiento de control de cambios.	Sistemas		
A12 Seguridad de las operaciones.	Documentar los procedimientos que abarquen aquellas actividades que afectarán al procesamiento de la información y aquellas que la protegen.	Planeación y Sistemas de Información Calidad		
	Incluir en el plan de formación y capacitación los procedimientos sobre el tratamiento de la información y su seguridad.	Planeación y Sistemas de Información Desarrollo Humano		
	Revisar, actualizar y establecer los controles necesarios para asegurar que la información y las instalaciones de procesamiento de información se encuentren protegidos contra el código malicioso.	Sistemas		
	Establecer sistemas de monitoreo de software y los datos de la red.	Sistemas		
	Incluir en plan de capacitación institucional actualización de las nuevas amenazas y de cómo responder a ellas.			
	Revisar, actualizar y complementar lineamientos para copias de seguridad que permita asegurar la disponibilidad e integridad de la información ante incidentes.	Sistemas		
	Mantener en estado de funcionamiento los medios que permitirán la restauración de las copias cuando las necesitemos.	Sistemas		
	Definir e implementar la monitorización de cada sistema de información.	Sistemas, Planeación y Sistemas de Información		
	Llevar registro histórico de los incidentes. (Intentos de acceso exitosos y fallidos, Desconexiones del sistema Acciones ejecutadas, Alertas por fallos en el sistema Fecha y hora en que se producen los eventos, Tiempos de detención).	Sistemas		
	Establecer en el plan de continuidad del negocio el tiempo requerido para realizar restauraciones completas del sistema.	Sistemas		
	Definir lineamientos o procedimientos para cubrir las instalaciones de Software en cualquier dispositivo dentro de una organización.	Sistemas		
	Realizar el monitoreo y análisis de Vulnerabilidades.	Sistemas		
A13 Seguridad de las Comunicaciones.	Analizar, diseñar, desarrollar y afinar el plan de diagnóstico de IPv6 en la red de la ESE, con base en lo establecido en el inventario de activos de información.	Sistemas, Planeación y Sistemas de Información		
	Establecer e implementar lineamientos respecto a la protección, contra intercepción, copia, modificación, dirección incorrecta o destrucción de la información.	Sistemas, Planeación y Sistemas de Información		
	Establecer e implementar lineamientos de protección de la información en redes y la protección de la infraestructura de soporte.	Sistemas		
	Establecer e implementar lineamientos seguridad de la información cuando se intercambian datos dentro de la ESE y con cualquier otra entidad.	Sistemas		

ISO 27001:2013	ACTIVIDADES	RESPONSABLES	CRONOGRAMA	
A14 Adquisición, desarrollo y Mantenimiento de sistemas.	Establecer e implementar requisitos para la seguridad de la información: Análisis y especificación de los requisitos de seguridad. Aseguramiento de los servicios de aplicación en las redes públicas. Transacciones en línea.	Sistemas		
	Establecer controles para garantizar que se tienen en cuenta las necesidades de la seguridad de la información en los entornos de desarrollo de sistemas de información y en todo el ciclo de vida del mismo. Lineamientos de desarrollo seguro. Procedimiento de control de cambio del sistema. Revisión técnica de aplicaciones después de cambios de las plataformas operativas. Restricciones a los cambios en los paquetes de software. Principios de la ingeniería de sistemas seguros.	Sistemas		
	Condicionar la aceptación de la incorporación de nuevas aplicaciones actualizaciones o nuevas versiones de software un proceso de aceptación donde se le realicen las pruebas funcionales y de seguridad planificadas.	Sistemas		
	Establecer controles para seleccionar los datos para los sistemas de prueba o entornos de desarrollo.	Sistemas		
	Conocer la seguridad y funcionalidad requeridas por una aplicación o sistema antes de su fase de adquisición.	Sistemas		
	Establecer una fuente única de información.			
	Implementar controles de código fuente, gestión de requerimientos y gestión de pruebas.	Sistemas		
	Implementar controles para la revisión de código seguro.	Sistemas		
	Realizar pruebas de vulnerabilidad.	Sistemas		
A15 Relaciones con los proveedores.	Incluir en la política de seguridad y privacidad de la información lineamientos para proveedores y terceros.	Sistemas, Planeación y Sistemas de Información		
	Monitoreo al cumplimiento de procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, los incidentes de seguridad de la información y la revaloración de los riesgos.	Sistemas, Planeación y Sistemas de Información		
	Establecer de modo formal las condiciones para el uso de dichos activos y supervisar el cumplimiento de dichas condiciones.	Sistemas, Planeación y Sistemas de Información		
A16 Gestión de incidentes de seguridad de la información.	Documentar e implementar el procedimiento de Gestión de Incidentes, asignando responsabilidades para todo el ciclo de gestión de estos.	Planeación y Sistemas de Información Calidad		
	Capacitaciones en el procedimiento de gestión de incidentes.	Planeación y Sistemas de Información Desarrollo Humano		
	Definir las guías e instrumentos de atención para los incidentes comúnmente presentados, que permitan: Detectar, Responder, Reportar, Aprender.	Planeación y Sistemas de Información Calidad		
	Realizar la medición del procedimiento a través de los indicadores definidos.	Planeación y Sistemas de Información Estadística		
	Definir el alcance de los incidentes y gestionar su materialización.	Planeación y Sistemas de Información Estadística		
	Definir e implementar controles para gestionar los incidentes en la seguridad de la información.	Sistemas, Planeación y Sistemas de Información		
	Definir actividades tendientes a fortalecer el reporte de incidentes y las posibles debilidades por parte de todos los colaboradores.	Planeación y Sistemas de Información		
	Realizar los procesos de retroalimentación adecuados para asegurar que las personas que reportan eventos de seguridad de la información sean notificadas de los resultados después de su tratamiento.	Sistemas, Planeación y Sistemas de Información		

ISO 27001:2013	ACTIVIDADES	RESPONSABLES	CRONOGRAMA	
A17 Aspectos de seguridad de la información de la gestión de continuidad del negocio.	Revisión y actualización del Planes de Continuidad del Negocio (BCP).	Sistemas		
	Actualización Planes de recuperación ante desastres (DRP).	Sistemas		
	Revisión de Sistemas de alta disponibilidad para los procesos críticos.	Sistemas		
	Revisión de la seguridad para la estrategia de contingencia definida.	Sistemas		
A18 Cumplimiento.	Crear la Matriz de verificación de Requisitos Legales de Seguridad de la Información.	Sistemas, Planeación y Sistemas de Información		
	Monitoreo del cumplimiento de la instalación de software.	Sistemas		
	Monitoreo al inventario de software instalado y se compara con el número de licencias adquiridas para asegurar que no se incumplen los derechos de propiedad intelectual.	Sistemas		
	Atención de las auditorias de Seguridad de la información programadas por Control Interno.	Planeación y Sistemas de Información Control Interno		
	Revisar y alinear la documentación de la Entidad al Modelo de seguridad y privacidad de la información, contenido en el PETI, tener en cuenta la normatividad vigente.	Sistemas, Planeación y Sistemas de Información		
	Aplicar el Instrumento de identificación de la línea base de seguridad administrativa y técnica suministrada por MINTIC.	Sistemas, Planeación y Sistemas de Información		
	Hacer seguimiento a los hallazgos, acciones correctivas y oportunidades de mejora de las evaluaciones de seguridad realizadas.	Sistemas, Planeación y Sistemas de Información		
A18.1.4 Protección de los datos y privacidad de la información personal.	Definir e implementar controles para dar cumplimiento a la Ley de Protección de Datos Personales o Ley 1581 de 2012 y el decreto 1377 de 2013.	Sistemas, Planeación y Sistemas de Información		
	Realizar revisión independiente al cumplimiento de la seguridad y privacidad de la información.	Control interno		
	Establecer e implementar la evaluación de los sistemas de información de manera periódica, para asegurar que se encuentran configurados correctamente.	Sistemas, Planeación y Sistemas de Información		
	Identificar fallos en las actualizaciones de los sistemas, Establecer medidas correctivas antes de que estos fallos puedan suponer una amenaza real para el sistema.	Sistemas		

9. SEGUIMIENTO.

Evaluar el desempeño y la eficacia, a través del seguimiento a las actividades propuestas, dentro del ciclo de auditorías internas y el seguimiento a los riesgos identificados y a los indicadores de gestión, de manera permita determinar la efectividad de la implantación del presente Plan de Seguridad y Privacidad de la Información.

10. MEJORA CONTINUA.

Teniendo en cuenta los resultados obtenidos en el componente de seguimiento, establecer e implementar el mejoramiento continuo de seguridad y privacidad de la información, a través de acciones correctivas y oportunidades de mejora identificadas.

11. INDICADORES DE GESTIÓN.

Fuente: Guía de Indicadores de Gestión para la Seguridad de la Información. Guía No. 9. MINTIC.

INDICADOR 01- ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN.					
IDENTIFICADOR					
DEFINICIÓN					
El indicador permite determinar y hacer seguimiento, al compromiso de la dirección, en cuanto aseguridad de la información, en lo relacionado con la asignación de personas y responsabilidades relacionadas a la seguridad de la información al interior de la entidad					
OBJETIVO					
Hacer un seguimiento a la asignación de recursos y responsabilidades en gestión de seguridad dela información, por parte de la alta dirección.					
TIPO DE INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		**FORMULA**		**FUENTE DE INFORMACIÓN**	
1. Número de personas con su respectivo rol definió según el modelo de operación.		(1/2)*100		Manual de funciones y competencias. Contratos de prestación de servicio.	
2: Número de personas con surespectivo rol definió después de un año				Actas de posesión. Contratos de prestación de servicio firmados. personal.	
METAS					
MÍNIMA	**75-80%**	**SATISFACTORIA**	80- 90%	**SOBRESALIENTE**	100%
OBSERVACIONES					
De acuerdo a lo establecido en el capítulo 2 de la guía del modelo de operación del marco deseguridad y privacidad de la información, es necesario crear nuevos cargos y asignar responsabilidades en los actuales, por lo tanto, el indicador está enfocado, no solo a lacontratación de nuevas personas, sí no a la asignación de responsabilidades.					

INDICADOR 02 - CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN.					
TIPO DE INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		**FORMULA**		**FUENTE DE INFORMACIÓN**	
1. Número de activos críticos de información incluidos en el alcance de implementación del modelo, incluidos en la zona de riesgo inaceptable y la implementación del control no requiereadquisición de elementos de hardware o software.		(1/2)*100		Alcance del SGSI, Inventariode Activos de información,plan de tratamiento, matrizde riesgos	
2. Número de activos críticos deinformación incluidos en el alcance de implementación del modelo; activosincluidos en la zona de riesgo inaceptable.				Inventario de Activos deinformación, nuevos	
METAS					
MÍNIMA	75-80%	**SATISFACTORIA**	80-90%	**SOBRESALIENTE**	100%
OBSERVACIONES					
El indicador de cada proceso debe ser recolectado y promediado para construir un indicador querefleje el estado a nivel empresa. El terminó “incluir un activo” debe ser entendido como realizar la correcta clasificación del activo,tratamiento, evaluación de riesgos sobre el mismo y determinación de controles para minimizar elriesgo calculado. Para este indicador, solo se tienen en cuenta los controles que no implican adquisición de hardware o software.					

INDICADOR 03 - TRATAMIENTOS DE EVENTOS RELACIONADOS EN MARCO DE SEGURIDAD PRIVACIDAD DE LA INFORMACIÓN					
IDENTIFICADOR					
DEFINICIÓN					
El indicador permite determinar la eficiencia en el tratamiento de eventos relacionados la seguridad de la información. Los eventos serán reportados por los usuarios o determinadas en las auditorías planeadas para el sistema.					
OBJETIVO					
El objetivo del indicador es reflejar la gestión y evolución del modelo de seguridad y privacidad de la información al interior de una entidad					
TIPO DE INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES			**FORMULA**	**FUENTE DE INFORMACIÓN**	
1: Número de anomalías cerradas.			(1/V2)*100	Auditorías internas, herramientas de monitoreo	
2: Número total de anomalías encontradas.				Auditorías internas, herramientas de monitoreo	
METAS					
MÍNIMA	75-80%	**SATISFACTORIA**	80- 90%	**SOBRESALIENTE**	100%
OBSERVACIONES:					

INDICADOR 04 – PLAN DE SENSIBILIZACIÓN					
IDENTIFICADOR					
DEFINICIÓN					
El indicador permite medir la aplicación de los temas sensibilizados en seguridad de la informaciónpor parte de los usuarios finales. Estas mediciones se podrán realizar por medio de auditorías especializadas en el tema o de forma aislada por parte de los responsables de la capacitación y sensibilización.					
OBJETIVO					
El objetivo del indicador es establecer la efectividad de un plan de capacitación y sensibilizaciónpreviamente definido como medio para el control de incidentes de seguridad.					
TIPO INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES			**FORMULA**	**FUENTE DE INFORMACIÓN**	
1: Número de fallas o no cumplimientos encontrados en las sensibilizaciones programadas o eventos realizados para evaluar el tema.			(1/2)*100	Oficial de Seguridad de la Información, auditorías internas, atención al usuario, listas de asistencia	
2: Total de personal a capacitar.				Total de funcionarios de laentidad.	
METAS					
MÍNIMA	75-80%	**SATISFACTORIA**	80- 90%	**SOBRESALIENTE**	100%
OBSERVACIONES					
Para el levantamiento de la información que permita obtener datos para la medición el responsabledebe idear planes, laboratorios o actividades periódicas que permitan medir lo capacitado o divulgado.					

INDICADOR 05 – CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA ENTIDAD				
IDENTIFICADOR				
DEFINICIÓN				
Cumplimiento de políticas de seguridad de la información en la entidad.				
OBJETIVO				
Busca identificar el nivel de estructuración de los procesos de la entidad orientados a la seguridad de la información.				
TIPO INDICADOR				
Indicador de Cumplimiento				
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**	
1: ¿La entidad ha definido una política general de seguridad de la información?		1 (se evidencia) 0 (no se evidencia)	Documento política de la seguridad y privacidad de la información aprobada mediante acto administrativo.	
2: ¿La entidad ha definido una organización interna en términos de personas y responsabilidades con el fin de cumplir las políticas de seguridad de la información y documenta estas actividades?			Organigrama de TI.	
2: ¿La entidad cumple con los requisitos legales, reglamentarios y contractuales con respecto al manejo de la información?			Matriz de requisitos legales TI. Contratos con cláusula de privacidad y seguridad de la información.	
METAS				
CUMPLE	1		**NO CUMPLE**	0
OBSERVACIONES				

INDICADOR No 6– IDENTIFICACIÓN DE LINEAMIENTOS DE SEGURIDAD DE LA ENTIDAD			
IDENTIFICADOR			
DEFINICIÓN			
Grado de la seguridad de la información y los equipos de cómputo.			
OBJETIVO			
Busca medir el nivel de preparación del recurso humano y su apropiación en cuanto a la seguridadde la información y los equipos de cómputo.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
1: ¿La entidad ha definido lineamientos de trabajo a través del comité o responsable de seguridad para que sus funcionarios cumplan las políticas de seguridad y evalúa periódicamente su pertinencia?		1 = 1 (Sí se evidencia) 0= 0 (NO se evidencia)	Usuarios Internos.
2: ¿La entidad ha definido lineamientos en cuanto a la protección de las instalacionesfísicas, equipos de cómputo y su entorno paraevitar accesos no autorizados y minimizar riesgos de la información de la entidad?			Usuarios Internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR No 7 – VERIFICACIÓN DEL CONTROL DE ACCESO			
IDENTIFICADOR			
DEFINICIÓN			
Grado control de acceso en la entidad.			
OBJETIVO			
INDICADOR – VERIFICACIÓN DEL CONTROL DE ACCESO			
Busca identificar la existencia de lineamientos, normas o estándares en cuanto al control deacceso en la entidad.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
1: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el acceso de los usuarios a sus servicios de Gobierno en línea y a sus redes de comunicaciones?		1 = 1 (SÍ se evidencia) 0 = 0 (NO se evidencia)	Usuarios Internos.
2: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar el uso yel acceso a los sistemas de información, las aplicaciones y los depósitos de información con las que cuenta la entidad?			Usuarios Internos.
3: ¿La entidad ha definido lineamientos, normas y/o estándares para controlar las terminales móviles y accesos remotos a los recursos de la entidad?			
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR No 08– ASEGURAMIENTO EN LA ADQUISICIÓN Y MANTENIMIENTO DE SOFTWARE			
IDENTIFICADOR			
DEFINICIÓN			
Grado de protección de los servicios de la entidad.			
OBJETIVO			
Busca identificar la existencia de lineamientos, normas o estándares en cuanto a la adquisición odesarrollo de aplicaciones.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
1: ¿La entidad ha definido lineamientos,normas y/o estándares para el desarrollo o, adquisición de software sistemas yaplicaciones?		1= 1 (SÍ se evidencia) 0= 0 (NO se evidencia)	Usuarios Internos.
2: ¿La entidad ha definido lineamientos, normas y/o estándares para la gestión deincidentes relacionados con el servicio?			Usuarios Internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR No 09 – IMPLEMENTACIÓN DE LOS PROCESOS DE REGISTRO Y AUDITORÍA			
IDENTIFICADOR			
DEFINICIÓN			
Grado de existencia de lineamientos, normas o estándares en cuanto registro y auditoría para laseguridad de la información.			
OBJETIVO			
Busca identificar la existencia de lineamientos, normas o estándares en cuanto registro y auditoríapara la seguridad de la información.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
1: ¿La entidad ha definido lineamientos,normas y/o estándares para el registro y control de eventos que sucedan sobre sus sistemas, redes y servicios?		1 = 1 (SÍ se evidencia)	Usuarios Internos.
2: ¿La entidad verifica de manera interna y/o a través de terceros, periódicamente sus procesos de seguridad de la información y sistemas para asegurar el cumplimiento del modelo?		0 = 0 (NO se evidencia)	Usuarios Internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR No 10– IMPLEMENTACIÓN DE LOS PROCESOS DE REGISTRO Y AUDITORÍA			
IDENTIFICADOR			
DEFINICIÓN			
Grado de implementación de los mecanismos encaminados a la detección de anomalías eirregularidades.			
OBJETIVO			
Busca medir el nivel de mecanismos encaminados a la detección de anomalías e irregularidades			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
VSI21: VAPRSG005: ¿La entidad ha implementado mecanismos para detectar periódicamente vulnerabilidades de seguridad en el funcionamiento de: a) su infraestructura, b) redes, c) sistemas de información, d) aplicaciones y/o e) uso de los servicios?		1 = 1 (SÍ se evidencia) 0 = 0 (NO se evidencia)	Usuarios internos. No conformidades.
METAS			
CUMPLE			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR No 11 – POLÍTICAS DE PRIVACIDAD Y CONFIDENCIALIDAD			
IDENTIFICADOR			
DEFINICIÓN			
Grado de implementación de políticas privacidad y confidencialidad de la entidad.			
OBJETIVO			
Busca identificar el nivel de implementación de políticas privacidad y confidencialidad de laentidad.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
1: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información personal y privada delos ciudadanos que utilicen sus servicios?		1= 1 (SÍ se evidencia) 0 = 0 (NO se evidencia)	Usuarios Internos.
2: ¿La entidad ha implementado lineamientos, normas y/o estándares para proteger la información privada de las entidades que utilicen sus servicios?			Usuarios Internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR No 12– VERIFICACIÓN DE LAS POLÍTICAS DE INTEGRIDAD DE LA INFORMACIÓN			
IDENTIFICADOR			
DEFINICIÓN			
Grado de implementación de mecanismos para la integridad de la información de la entidad.			
OBJETIVO			
Busca identificar el nivel de implementación de políticas privacidad y confidencialidad de laentidad.			
TIPO INDICADOR			
Indicador de Cumplimiento			
DESCRIPCIÓN DE VARIABLES		**FORMULA**	**FUENTE DE INFORMACIÓN**
1: ¿La entidad ha implementado lineamientos contra modificación o pérdidaaccidental de información?		1 = 1 (SÍ se evidencia) 0 = 0 (NO se evidencia)	Usuarios Internos.
2: ¿La entidad ha implementado lineamientos, normas y/o estándares para recuperar información en caso de modificación o pérdida intencional o accidental?			Usuarios Internos.
METAS			
CUMPLE	1	**NO CUMPLE**	0
OBSERVACIONES			

INDICADOR No 13 – POLÍTICAS DE DISPONIBILIDAD DEL SERVICIO Y LA INFORMACIÓN	
IDENTIFICADOR	
DEFINICIÓN	

Grado de cumplimiento de las políticas de disponibilidad del servicio y la información.		
OBJETIVO		
Busca identificar el nivel de implementación de políticas de disponibilidad del servicio y lainformación.		
TIPO INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTE DE INFORMACIÓN**
1: ¿La entidad verifica que los lineamientos, normas y/o estándares orientados a la continuidad en la prestación delos servicios se cumplan?	1 = 1 (SÍ se evidencia)	Usuarios Internos.
2: ¿La entidad ha implementado mecanismos para que los servicios de Gobierno en línea tengan altos índices dedisponibilidad?	0 = 0 (NO se evidencia)	Usuarios Internos.
METAS		
CUMPLE 1	**NO CUMPLE**	0
OBSERVACIONES		

INDICADOR No 14 – ATAQUES INFORMÁTICOS A LA ENTIDAD.		
IDENTIFICADOR		
DEFINICIÓN		
Porcentaje de ataques informáticos recibidos en la entidad que impidieron la prestación de algunode sus servicios.		
OBJETIVO		
Busca conocer el número de ataques informáticos que recibe la entidad		
TIPO INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTE DE INFORMACIÓN**
1: ¿Cuántos ataques informáticos recibióla entidad en el último año?	1 = 1 (SÍ se evidencia)	Herramientas de Monitoreo/Usuarios Internos.
2: ¿Cuántos ataques recibió la entidad en el último año que impidieron la prestación de algunos de los servicios que la entidad ofrece a los ciudadanos y empresas?	1 = 0 (NO se evidencia)	Herramientas de Monitoreo/Usuarios Internos.
METAS		
CUMPLE 1	**NO CUMPLE**	0
OBSERVACIONES		

INDICADOR No 15– PORCENTAJE DE DISPONIBILIDAD DE LOS SERVICIO DE GOBIERNO EN LÍNEA QUE PRESTA LA ENTIDAD	
IDENTIFICADOR	
DEFINICIÓN	
Porcentaje de disponibilidad de los servicios que presta la entidad	

OBJETIVO		
Busca identificar el nivel de disponibilidad del servicio y la información.		
TIPO INDICADOR		
Indicador de Cumplimiento		
DESCRIPCIÓN DE VARIABLES	**FORMULA**	**FUENTE DE INFORMACIÓN**
1: La entidad tiene definidos ANS paralos servicios de Gobierno en Línea que presta	1 = 1 (SÍ se evidencia) 0 = 0 (NO se evidencia)	Usuarios Internos.
2: Porcentaje de disponibilidad de losservicio de Gobierno en línea que presta la entidad en base a los ANS del punto anterior.		Usuarios Internos.
METAS		
CUMPLE 1	**NO CUMPLE**	0
OBSERVACIONES		

INDICADOR No 16 – PORCENTAJE DE IMPLEMENTACIÓN DE CONTROLES					
IDENTIFICADOR					
DEFINICIÓN					
Grado de avance en la implementación de controles de seguridad					
OBJETIVO					
Busca identificar el grado de avance en la implementación de controles de seguridad					
TIPO INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		**FORMULA**		**FUENTE DE INFORMACIÓN**	
1: Número de Controles Implementados		(1/2)*100		Plan de tratamiento de riesgos	
2: Número de Controles que seplanearon implementar				Plan de Tratamiento de riesgos.	
METAS					
MÍNIMA	75-80%	**SATISFACTORIA**	80- 90%	**SOBRESALIENTE**	100%
OBSERVACIONES					

NOTAS DE CAMBIO

Versión	Fecha de Actualización	Descripción del cambio
1	28-01-2022	Elaboración del Documento
2	27-01-2023	Actualización de la información de acuerdo a los cambios

CONTROL DE EMISIÓN		
Elaboró / Actualizó		Revisó / Aprobó
Nombre	Carolina Ramírez Naranjo	Javier de Jesús Cadenas Pérez
Cargo	Jefe Oficina Planeación y Sistemas de Información	Gerente
Firma		
Fecha	27-01-2023	27-01-2023