PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y PLAN DE CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO

Versión 0

Información segura... ¡es cultura!

Corpoboyacá
Región estratégica para la sostenibilidad

INTRODUCCIÓN

Con el fin de garantizar el manejo eficaz de la información con la cual trabaja la CORPOBOYACÁ por medio de los equipos, aplicaciones informáticas y demás medios con los cuales interactúan diariamente los funcionarios y usuarios en general, se hace necesario identificar y gestionar las actividades que se relacionan con la Seguridad de la Información.

Esto se logra por medio de un Sistema de Gestión de Seguridad de la Información acorde con referentes nacionales e internacionales como la norma ISO 27001:2013, que permite la evaluación de riesgos, el establecimiento de controles, la evaluación de la conformidad de las partes interesadas, tanto internas como externas y contribuye en la ejecución de un plan de continuidad de negocio, de tratamiento de incidentes y de contingencia que son vitales para la institución, como medida preventiva ante cualquier eventualidad a la cual se pueda ver expuesta. Este Sistema de Gestión de Seguridad de la Información además permite el fortalecimiento de los procesos por medio del diseño, implementación y revaluación de la seguridad, lo cual arroja como resultado el mejoramiento continuo gracias a la adopción del modelo PHVA (Planear-Hacer-Verificar-Actuar).

Para la Corporación como entidad de carácter público, del orden nacional, cuyo objetivo principal es la administración de los recursos naturales renovables, propendiendo por el desarrollo sostenible de conformidad con las disposiciones normativas y legales, es importante y requerido para su operación el contar con un estándar de Seguridad de la Información acorde a las certificaciones ya obtenidas, estándar que ayudará a mantener un sistema coherente con los procesos de la entidad en beneficio de la comunidad.

Para lograr este objetivo, las políticas aquí definidas brindan las herramientas necesarias para que los funcionarios, contratistas y terceros que hacen parte del Sistema de Gestión de Seguridad de la Información (SGSI en adelante) de la Corporación, puedan adoptar los controles requeridos para asegurar la información, gestionar con eficiencia los riesgos de seguridad y mejorar continuamente el SGSI, ello solo es posible a través de la integración de políticas, procedimientos, sistemas de información y controles con un fin común: gestionar de manera pertinente y eficaz los riesgos, de tal forma que las partes interesadas obtengan un alto nivel de seguridad y confianza.

Se entiende, por lo tanto, que las políticas deben ser plenamente conocidas y cumplidas por los funcionarios, contratistas y terceras partes que tienen acceso a los activos de información y a los sistemas de procesamiento de información de la Corporación. En este sentido, es indispensable que sus esfuerzos y capacidades se concentren en lograr los fines primordiales de las políticas, como son: generar controles para proteger los activos de información; crear conciencia en los usuarios acerca del uso responsable de las tecnologías de la información y comunicaciones y realizar una gestión de riesgos adecuada que permita minimizar el impacto frente a un eventual caso de materialización.

OBJETIVO GENERAL

Planificar, orientar y desarrollar los mecanismos necesarios para dotar de disponibilidad, confidencialidad e integridad al conjunto de datos y activos de información de la Entidad.

OBJETIVOS ESPECÍFICOS

- Formular el esquema de seguridad de la información de acuerdo a las necesidades del Sistema de Información Corporativo.
- Instaurar medidas de control de acceso a los activos de información de la Corporación.
- Alinear a la normatividad vigente a nivel Nacional las políticas de gestión y administración de activos de información de la Corporación.
- Establecer las acciones, documentos, procedimientos y responsabilidades frente a la garantía de la seguridad de la información en la Corporación.
- Proyectar la implementación del presente plan junto con sus actividades y documentos relacionados.
- Fortalecer la seguridad de la información, además de promover y mantener la confianza de los funcionarios, contratistas y terceros, mediante el desarrollo, implementación y cumplimiento de las políticas y procedimientos establecidos dentro del SGSI.
- Cumplir con los principios de confidencialidad, disponibilidad e integridad de la información, garantizando la protección de los activos de información de la Corporación.
- Apoyar el cumplimiento de los principios de la función administrativa correspondientes a la legalidad, economía, eficacia, contradicción y publicidad, a través de los lineamientos establecidos por el SGSI.
- Incentivar la cultura de la Seguridad y Privacidad de la Información fortaleciendo las buenas prácticas y la conciencia de los funcionarios, contratistas y terceros.
- Gestionar los riesgos de seguridad de la información con el fin de evitar el impacto en los objetivos estratégicos de la Corporación, en especial, en aquellos que afecten los procesos misionales.
- Garantizar la continuidad del negocio mediante la implementación de planes y controles que sea necesario desarrollar frente a la existencia de incidentes de seguridad de la información.
- Apoyar las innovaciones y proyectos tecnológicos que garanticen los niveles de seguridad de la información previstos por la Entidad.

JUSTIFICACIÓN

En la actualidad, la seguridad en la información es una de las preocupaciones más grandes que puede llegar a tener una compañía, ya que se refiere a garantizar la calidad, disponibilidad, veracidad y confidencialidad de su activo más preciado: la información.

La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades.

Hoy en día las empresas que manejen sistemas de información han generado la necesidad del aseguramiento de la información, generando políticas y controles, buscando garantizar la estabilidad y confiabilidad de la información, proyectándose ser reconocidas a nivel nacional como internacional, teniendo buena credibilidad y ubicándose siempre en los primeros lugares.

Teniendo en cuenta la obligatoriedad de cumplimiento de lo definido en la estrategia de Gobierno en Línea, y el conjunto de normativas que rigen al respecto, además de la situación actual del sistema de información y los servicios tecnológicos de CORPOBOYACÁ, se hace necesario levantar una línea de base sobre la cual se articulen diferentes esfuerzos encaminados a ofrecer la seguridad en la información, teniendo en cuenta las distintas amenazas y vulnerabilidades que pueden comprometer la integridad de los datos, en las redes, en los servicios y demás herramientas tecnológicas dispuestas para tal fin.

Es importante aclarar que este proyecto se encamina a formar las bases para una declaratoria de lineamientos progresivamente aplicables que vayan dando forma al Plan de Seguridad Informática partiendo desde las copias de seguridad, su protección, integralidad, restricción de acceso y demás elementos a tener en cuenta.

Los principales beneficiarios son en primera medida la Alta Dirección, ya que se ofrecerá disponibilidad y veracidad en la información que se usa para la toma de decisiones. Por otra parte, los usuarios finales del sistema de información que alimentan y requieren de agilidad y seguridad al momento de ingresar información que puede o no ser pública, a través de los servicios tecnológicos de la Corporación.

ALCANCE Y DELIMITACIÓN DEL PLAN

El objetivo que se busca con la implementación de su SGSI es mejorar los niveles de seguridad de la información y la protección de los activos de información, para lograrlo sabe que es indispensable implementar los controles según lo señalado por el estándar ISO 27001:2013 y la normatividad vigente aplicable.

Por tal razón, los funcionarios, contratistas y terceros que interactúen con los activos de información de la Corporación, como ya se ha mencionado, deberán conocer y cumplir las políticas, procesos y procedimientos que hacen parte del SGSI, salvaguardando ante todo los principios de confidencialidad, integridad y disponibilidad que los protegen frente a cualquier tipo de tratamiento.

MARCO DE REFERENCIA

ANTECEDENTES

En los últimos años, las entidades públicas tienden a mejorar la eficiencia, efectividad y eficacia de su gestión a partir de la reducción de costos por diferentes medios y buscando siempre la mejora del aprovechamiento de sus recursos, para lo cual buscan: optimizar sus procesos misionales, revisar y actualizar políticas de adquisición en la entidad, automatizar los procesos manuales, dinamizar la integración de los procedimientos de su sistema integrado de gestión, entre otros.

Esto se realiza a partir de los lineamientos de la Política Gobierno en Línea, en la cual se describen las características sobre las cuales debe enmarcarse la ejecución de todos estos objetivos.

Para la optimización de estos procesos se hace necesario utilizar las tecnologías de información de acuerdo a las necesidades de la entidad, teniendo en cuenta la visión, misión y estrategias que la alta dirección quiere implementar en la Entidad.

El Plan Estratégico de Tecnología de Información y comunicación (PETIC) es un conjunto de políticas tecnológicas e iniciativas de la Oficina de Sistemas que deben soportar la visión, misión y estrategias que la Corporación tiene, teniendo en cuenta que la razón de ser de las tecnologías de información son las áreas misionales de la Corporación y por ende ambas perspectivas (misión y tecnología) deben estar alineadas y contar con mecanismos para facilitar éste alineamiento.

De su mano, el Plan de Seguridad Informática debe constituirse como una línea de mando sobre la cual se establezcan los parámetros a seguir para garantizar su principal objetivo. A este se relacionan a su vez varios procedimientos, enfocándonos en el procedimiento de Copias de Seguridad.

En el año 2016 se documentaron las Politicas de Seguridad de la Información, sin embargo, posteriormente tras los requerimientos y análisis realizados por diferentes instancias internas y externas, se determinó que se requería la realización de un Plan que recogiera la actualización de las necesidades y normativas que circundan la seguridad de la información en las instituciones públicas y principalmente en las Corporaciones Autónomas Regionales.

DEFINICIONES

- Activo: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.
- Amenaza: causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.
- Amenaza informática: la aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado (Ministerio de Defensa de Colombia).
- Análisis de riesgos: proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.
- Anonimización del dato: eliminar o sustituir algunos nombres de personas (físicas o jurídicas); direcciones y demás información de contacto, como números identificativos, apodos o cargo.
- Autenticación: provisión de una garantía de que una característica afirmada por una entidad es correcta.
- Autenticidad: propiedad de que una entidad es lo que afirma ser. (ISO 27000.es, 2012).
- Ciberseguridad: capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
- Ciberespacio: ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701).
- Confidencialidad: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- Control: comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.
- Custodio de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la Corporación, que tiene la responsabilidad de administrar y hacer efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad.
- Datos abiertos: son datos primarios o sin procesar puestos a disposición de cualquier ciudadano, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.
- Datos biométricos: parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (huella digital o voz).
- 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.

- Dato privado: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
- Dato público: es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.
- Dato semiprivado: es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.
- Disco duro: disco de metal cubierto con una superficie de grabación ferro magnético. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y re-grabados como una cinta de audio.
- Disponibilidad: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- DVD: Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad.
- Evento de seguridad de la información: ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.
- Gestión de claves: son controles que realizan mediante la gestión de claves criptográficas.
- 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.
- Gestión de riesgos: actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
- Habeas data: derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.
- Impacto: el coste para la empresa de un incidente “de la escala que sea”, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.
- Incidente de seguridad de la información: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- Información: La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente.

La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

- Integridad: la propiedad de salvaguardar la exactitud y complejidad de la información.
- Inventario de activos: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es,2012).
- No repudio: servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2).
- Parte interesada (Stakeholder): persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- Plan de continuidad del negocio: plan orientado a permitir la continuidad 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.
- Proceso: conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas. (ISO 27000.es, 2012).
- Propietario de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.
- 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 consideraciones. (ISO Guía 73:2002).
- Responsable del tratamiento: 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.
- Segregación de tareas: reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.
- Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información.
- Sistema de Gestión de Seguridad de la Información (SGSI): conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.
- Titular de la información: es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.

- Trazabilidad: cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociada de modo inequívoco a un individuo o entidad.
- Vulnerabilidad: debilidad de un activo o control que pueda ser explotado por una o más amenazas. (ISO 27000.es, 2012).

NORMATIVIDAD

El Sistema de Gestión de Seguridad de la Información de la Corporación se ciñe a la normatividad legal vigente colombiana, tal como se describe enseguida:

LEGISLACIÓN	TEMA	REFERENCIA
Ley 527/99	Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos	El mensaje de datos es "*La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos, Internet, el correo electrónico, el telegrama, el télex o el telefax*".
Ley 594/00	Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones	La presente ley "tiene por objeto establecer las reglas y principios generales que regulan la función archivística del Estado". Y "comprende a la administración pública en sus diferentes niveles, las entidades privadas que cumplen funciones públicas y los demás organismos regulados por la presente ley".
La Ley 850/03 establece en su artículo 9º	Principio de Transparencia	"A fin de garantizar el ejercicio de los derechos, deberes, instrumentos y procedimientos consagrados en esta ley, la gestión del Estado y de las veedurías deberán asegurar el libre acceso de todas las personas a la información y documentación relativa a las actividades de interés colectivo de conformidad con lo dispuesto en esta ley y en las normas vigentes sobre la materia".
Ley 1266/08	Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información	Se regula el manejo de la información para "*todos los datos de información personal registrados en un banco de datos, sean estos administrados por*

	contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.	*entidades de naturaleza pública o privada*".
Ley 1221 de 2008	Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones	La presente ley tiene por objeto promover y regular el Teletrabajo como un instrumento de generación de empleo y autoempleo mediante la utilización de tecnologías de la información y las telecomunicaciones (TIC).
Ley 1273/09	Por medio de la cual 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.	"*De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos*".
CONPES 3701 de 2011	Lineamientos de política para ciberseguridad y Ciberdefensa	Busca generar lineamientos de política en ciberseguridad y ciberdefensa encaminados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.
Resolución 2886 de 2012	Por la cual se definen las entidades que harán parte de la Red Nacional de Fomento al Teletrabajo y se dictan otras disposiciones.	Resolución del Ministerio de Trabajo define "*las entidades que harán parte de la Red Nacional de Fomento al Teletrabajo, las actividades que compete desarrollar y su funcionamiento*".
Ley 1581/12	Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales	Hace referencia, en particular, al artículo 15 de la Constitución Nacional, según el cual "*todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido*

		sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución…". La ley tiene por objeto "desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma".
Decreto 884 de 2012	Por medio del cual se reglamenta la Ley 1221 de 2008 y se dictan otras disposiciones.	El propósito de la Ley 1221 de 2008 es promover y regular el teletrabajo como un instrumento de generación de empleo y autoempleo mediante la utilización de tecnologías de la información y las telecomunicaciones.
Decreto 2609 de 2012 (hoy incorporado al Decreto Único 1080 de 2015	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.	Sobre la Gestión de Documentos indica que las normas del decreto se aplicarán a cualquier tipo de información producida y/o recibida por las entidades públicas, sus dependencias y servidores públicos, y en general por cualquier persona que desarrolle actividades inherentes a la función de dicha entidad o que hayan sido delegados por esta, independientemente del soporte y medio de registro (análogo o digital) en que se produzcan, y que se conservan en: a) Documentos de Archivo (físicos y electrónicos). b) Archivos institucionales (físicos y electrónicos). c) Sistemas de Información Corporativos. d) Sistemas de Trabajo Colaborativo. e) Sistemas de

		Administración de documentos. f) Sistemas de Mensajería Electrónica. g) Portales, Intranet y Extranet. h) Sistemas de Bases de Datos. i) Disco duros, servidores, discos o medios portables, cintas o medios de video y audio (análogo o digital), etc. j) Cintas y medios de soporte (back up o contingencia). k) Uso de tecnologías en la nube.
Decreto 886 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, en lo relativo al Registro Nacional de bases de datos.	Serán objeto de inscripción en el Registro Nacional de Bases de Datos, "las bases de datos que contengan datos personales cuyo Tratamiento automatizado o manual se realice por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano o fuera de él, en este último caso, siempre que al Responsable del Tratamiento o al Encargado del Tratamiento le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales. Lo anterior sin perjuicio de las excepciones previstas en el artículo 2° de la Ley 1581 de 2012".
En el Decreto Nacional 2573 de 2014	Estrategia de Gobierno en Línea de la República de Colombia	El Decreto establece los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones
LEY 1712 DE 2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública	Hace referencia, principalmente, al artículo 74 de la Constitución Nacional en el cual se establece que "Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley". El objeto de la ley es "regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las

		excepciones a la publicidad de información”.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones	El decreto tiene por objeto regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información, y constituye el marco general de la protección del ejercicio del derecho de acceso a la información pública en Colombia.

PLAN GENERAL DE SEGURIDAD DE LA INFORMACIÓN

El Plan de seguridad es un documento de alto nivel que denota el compromiso de CORPOBOYACÁ con la seguridad de la información. Este Plan contribuye a minimizar los riesgos asociados a daños, proyecta la eficiencia administrativa y asegura el cumplimiento de las funciones misionales de la entidad apoyadas en el uso adecuado de TICs.

DETALLE

La Corporación Autónoma Regional de Boyacá . CORPOBOYACÁ debe salvaguardar las características de integridad, disponibilidad y confidencialidad de la seguridad de la información, mediante la adopción de políticas y procedimientos institucionales orientadas al logro de sus objetivos estratégicos, en estricto cumplimiento de las normas vigentes. De este modo, la Corporación velará por la adecuada gestión de los riesgos, la adopción de buenas prácticas en el uso de los activos de información y la mejora continua de las competencias del talento humano.

La eficiencia de la política de seguridad de la información se construye a través del liderazgo y compromiso de la Alta Dirección y la participación activa de los funcionarios, contratistas y terceros, quienes mancomunadamente deberán alcanzar el nivel de cumplimiento según los lineamientos y requisitos de seguridad de la información determinados aquí, así como el desarrollo de estrategias de mejora continua y gestión oportuna frente a incidentes o eventos de seguridad de la información.

METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL PROYECTO

El modelo a implementar es el ciclo Deming ó ciclo PHVA, como metodología para la mejora continua.

Además, se debe verificar la existencia de los siguientes lineamientos:

ACTIVIDADES SEGÚN LINEAMIENTOS PARA LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN.

Una vez la entidad ha logrado alinearse con el SGSI entra en el ciclo **PHVA**	**LINEAMIENTO 1. IDENTIFICAR EL NIVEL DE MADUREZ EN S.I**
	FASE 1. Preparación
	- Plan de capacitación - Conformación Equipo de Gestión del Proyecto
	FASE 2. Análisis situación actual y definición de brechas.
	- **Diseñar y aplicar encuesta de seguridad.** - **Definir nivel de madurez**: Realizar autoevaluación con respecto a los niveles de seguridad. - **Definición de brechas**: Revisión de estructura organizacional. Revisión por niveles de madurez de acuerdo a los requisitos del manual de GEL. Revisión de controles de SI (Existentes y ausentes). Definir el estado actual de SI de la entidad. Definición del plan o cronograma a seguir para disminuir la brecha y alinearse con el nivel de madurez adecuado.
	FASE 3. Alineación con el Sistema de Gestión de Seguridad de la Información SGSI.
	- Ejecución del Programa para la reducción de la brecha.
PLANEAR	**LINEAMIENTO 2. LLEVAR A LA ENTIDAD A UN NIVEL DE MADUREZ INICIAL EN SEGURIDAD.**
	FASE 1. Actividades Lineamientos Nivel Inicial
	- **Obtener soporte de la Dirección de la entidad.** - **Identificar legislación y normatividad aplicable.** - **Definir el alcance del SGSI "SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN"** - **Definir la Política de la Seguridad de la información.** - **Realizar el análisis de riesgo:** Definir la aproximación para la Gestión del Riesgo. Realizar la identificación de Activos. Identificar los riesgos Analizar el riesgo en contexto de los objetivos de la entidad y partes interesadas. - **Selección de Controles.**

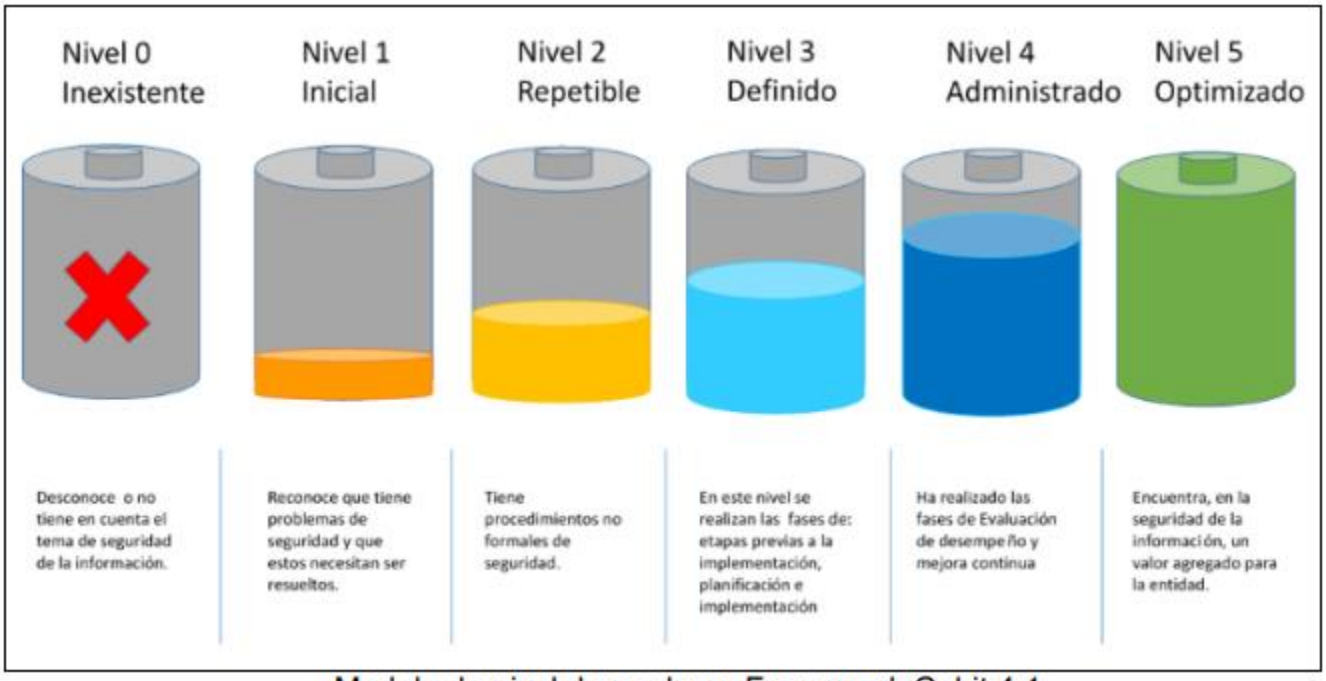
	- **Plan de Tratamiento del riesgo.** - **Generar el DDA - Declaración de aplicabilidad.**
HACER	**LINEAMIENTO 3. LLEVAR A LA ENTIDAD A UN NIVEL DE MADUREZ BÁSICO EN SEGURIDAD.**
	FASE 1. Actividades Lineamientos Nivel Avanzado.
	- Implementar el plan de tratamiento del riesgo. **- Documentar los controles del SGSI:** Definir métricas y medidas para medir el desempeño del SGSI. **- Implementar políticas y controles de seguridad de la fase de planeación.** **- Implementar los planes de concientización y entrenamiento.** **- Establecer y gestionar la operación del SGSI y sus recursos.** **- Implementar la infraestructura de respuesta a incidentes.**
VERIFICAR	**LINEAMIENTO 4. LLEVAR A LA ENTIDAD A UN NIVEL DE MADUREZ AVANZADO EN SEGURIDAD.**
	FASE 1. Actividades Lineamientos Nivel Avanzado.
	- Ejecutar plan operacional. **- Revisiones regulares de eficacia:** Monitorear y revisar políticas, estándares, procedimientos y prácticas. Revisar la eficacia de las operaciones de seguridad usando métricas y mediciones. **- Revisar el nivel del riesgo residual.** **- Realizar Auditorías internas.** **- Realizar Auditorías externas.** **- Revisión de la dirección del SGSI.** **- Registro del impacto en el SGSI.**
ACTUAR	**LINEAMIENTO 5. LLEVAR A LA ENTIDAD A UN NIVEL DE MADUREZ DE MEJORAMIENTO PERMANENTE EN SEGURIDAD.**
	FASE 1. Actividades Lineamientos Nivel Mejoramiento Permanente.
	- Implementar las mejoras identificadas y aprobadas al SGSI en un nuevo ciclo. **- Tomar medidas preventivas y correctivas.** **- Aplicar las lecciones aprendidas.** **- Comunicar los resultados.** **- Proceso continuo y Gestión auto sostenible del modelo de las entidades:** Revisión de Política de Seguridad. Verificación del alcance del conjunto de políticas en la entidad. Revisión de los activos de información de la entidad. Revisión del riesgo residual. Recopilación y análisis de los indicadores del modelo. Análisis de estadísticas de incidentes de seguridad de la información en entidades del Estado. Implementación de los ajustes.

Posterior a la revisión de cumplimiento de los lineamientos, se debe verificar el nivel de madurez del CGSI "Componente de Gestión de Seguridad de la Información", de acuerdo a como se describe a continuación:

MODELO DE MADUREZ

NIVEL	DESCRIPCIÓN
INEXISTENTE	- Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo, no están alineados a un Modelo de Seguridad. - No se reconoce la información como un activo importante para su misión y objetivos estratégicos. - No se tiene conciencia de la importancia de la seguridad de la información en las entidades
INICIAL	- Se han identificado las debilidades en la seguridad de la información. - Los incidentes de seguridad de la información se tratan de forma reactiva. - Se tiene la necesidad de implementar el MSPI "MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN", para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Entidad.
REPETIBLE	- Se identifican en forma general los activos de información. - Se clasifican los activos de información. - Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información. - Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión.
ADMINISTRADO	- La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información. - La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información. - La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas. - La Entidad tiene procedimientos formales de seguridad de la Información. - La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información. - La Entidad ha realizado un inventario de activos de información aplicando una metodología. - La Entidad trata riesgos de seguridad de la información a través de una metodología. - Se implementa el plan de tratamiento de riesgos.

OPTIMIZADO	- En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización. - Se utilizan indicadores de efectividad para establecer si la entidad encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales.



Modelo de nivel de madurez Framework Cobit 4.1

HERRAMIENTAS PARA LA EJECUCIÓN DEL PROYECTO

Finalmente, a continuación se lleva a cabo una reseña de las principales características de la norma ISO/IEC 27001:2013, la cual se ha seleccionado como estándar para la implementación y mantenimiento del CGSI dentro de CORPOBOYACÁ.

Objetivos de control.

- Políticas de seguridad de la Información:
  Establece la necesidad de definir un conjunto de políticas aplicadas a todas las actividades relacionadas con la gestión de la seguridad de la información dentro de la Organización, con el propósito de proteger la misma contra las amenazas presentes en el entorno.

- Organización de la seguridad de la información:
  Sugiere diseñar una estructura para la gestión de la seguridad de la información dentro la Organización que establezca los roles y responsabilidades con la seguridad de la información a lo largo de la misma.

- Seguridad del Recurso Humano:
  Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y confidencialidad de la información que manejan.

  También determina cómo incide el papel que desempeñan los empleados como coresponsables de la seguridad de la información.

- Gestión de Activos:
  Detalla los elementos de la Organización (servidores, PCs, medios magnéticos, información impresa, documentos, etc.), que deben ser considerados para establecer un mecanismo de seguridad que permita garantizar un nivel adecuado de protección.

- Control de acceso:
  Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para protegerlos contra los abusos internos e intrusos externos. Asimismo, establece los diferentes tipos de accesos o privilegios a los recursos informáticos (sistema operativo, aplicaciones, correo electrónico, Internet, comunicaciones, conexiones remotas, etc.) que requiere cada empleado de la Organización y el personal externo que brinda servicios, en concordancia con sus responsabilidades.

  Esto permitirá identificar y evitar acciones o actividades no autorizadas, garantizando los servicios informáticos.

- Cifrado:
  Garantiza el uso adecuado y eficaz del cifrado para proteger la confidencialidad, autenticidad y/o integridad de la información.

- Seguridad física y ambiental:
  Responde a la necesidad de proteger las áreas, los equipos y los controles generales. El objetivo principal es la prevención de accesos no autorizados a las instalaciones de la Organización, con especial atención a todos los sitios en los cuales se procesa información (centros de cómputo, PC de usuarios críticos, equipos de los proveedores de servicios, etc.), y áreas en las cuales se recibe o se almacena información (magnética o impresa) sensitiva (fax, áreas de envío y recepción de documentos, archivadores, etc.), minimizando riesgos por pérdidas de información, hurto, daño de equipos y evitando la interrupción de las actividades productivas.

  - Seguridad de las operaciones:
  Define las políticas, procedimientos y responsabilidades para asegurar la correcta operación de las instalaciones de procesamiento de información.

- Seguridad de las comunicaciones:
Define las políticas y procedimientos para asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información.

- Adquisición, desarrollo y mantenimiento de los sistemas de información:
Establece la necesidad de implantar medidas de seguridad y aplicación de controles de seguridad en todas las etapas del proceso de desarrollo y mantenimiento de los sistemas de información. Además, considera los mecanismos de seguridad que deben implantarse en el proceso de adquisición de todos los sistemas o aplicaciones de la Organización, para prevenir pérdidas, modificaciones, o eliminación de los datos, asegurando así la confidencialidad e integridad de la información.

- Relación con proveedores:
Permite asegurar la protección de los activos de información que son accedidos por proveedores.

- Gestión de Incidentes de Seguridad:
Establece la necesidad de desarrollar una metodología eficiente para la generación, monitoreo y seguimiento de eventos e incidentes de seguridad.

- Aspectos de seguridad de la información en la gestión de la continuidad del negocio:
Considera el análisis de todos los procesos y recursos críticos del negocio, y define las acciones y procedimientos a seguir en casos de fallas o interrupción de los mismos, evitando la pérdida de información y la no disponibilidad de los procesos productivos de la Organización, lo que podría provocar un deterioro de la imagen de la Organización, una posible pérdida de clientes o incluso una dificultad severa que impida continuar operando.

- Cumplimiento:
Imparte instrucciones a las organizaciones para que verifiquen si el cumplimiento con la norma técnica ISO/IEC 27002:2013, concuerda con otras leyes, reglamentos, normatividad y obligaciones contractuales o cualquier requerimiento de seguridad, tales como propiedad intelectual, auditorías, contrato de servicios, entre otros. Esta sección también requiere una revisión a las políticas de seguridad, al cumplimiento y las consideraciones técnicas; asimismo, busca garantizar que las políticas de seguridad y privacidad de la información sean acordes a la infraestructura tecnológica de la Organización.

CONTROL DE CAMBIOS

FECHA	VERSIÓN	CAMBIOS
Julio 30 2018	0	Documento inicial