PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Enero de 2019

ANTECEDENTES

En el Plan Estratégico de TIC de CORPOGUAVIO, construido durante el año 2017 y aprobado mediante resolución 255 de 18 de abril de 2018, existe el Plan de acción con la información de cada uno de los Proyectos formulados, y allí se menciona la necesidad de diagnosticar, planear, diseñar, implementar y monitorizar el Sistema de Gestión de la Seguridad de la Información – SGSI – de acuerdo con el modelo de seguridad y privacidad de la información y las orientaciones dadas por el MINTIC.

OBJETIVO

- Definir el marco de seguridad y privacidad de la información y de los sistemas de información para la Corporación.

- Implementar acciones de mejora de acuerdo al Diagnóstico de seguridad y privacidad de la información siguiendo los lineamientos de la estrategia de Gobierno en línea (Hoy política de Gobierno Digital) del MINTIC.

- Orientar a la Alta Dirección y a la subdirección de Planeación de CORPOGUAVIO en los planes y actividades subsiguientes, con el fin de darle viabilidad económica y técnica, para que los procesos internos sean seguros y eficientes a partir de las capacidades de gestión de las tecnologías de la información.

ALCANCE

Con el presente plan se quiere dar inicio a la implementación de mejoras de las situaciones encontradas, se pretende concienciar a todos los niveles de la Corporación, en promover el uso de las mejores prácticas de seguridad de la información, con el fin de continuar la aplicación del concepto de Gobierno digital. Además. Se quiere emplear la norma ISO 27001:2013 como instrumento de identificación de la línea base de seguridad de la información. Para ello se empleó una escala con la siguiente valoración:

Tabla de Escala de Valoración de Controles ISO 27001:2013 ANEXO A		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible . La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Adicionalmente, se busca articular las acciones de CORPOGUAVIO con lo definido en la estrategia corporativa y en el plan estratégico de tecnologías de la información y comunicación:

LÍNEA ESTRATÉGICA	OBJETIVO
Sistema de Gestión de la Seguridad de la Información (SGSI)	Formular lineamientos, implementar y ejecutar los procedimientos para el manejo de los sistemas de Información y seguridad informática, garantizar la integridad, la confidencialidad y la disponibilidad de la Información establecida en la infraestructura tecnológica y de las comunicaciones para contribuir con la misión corporativa de la entidad.
Estrategia de Gobierno en Línea	Implementar la estrategia GEL en busca de la participación activa de los ciudadanos en la toma de decisiones, la creación de los mejores trámites y servicios en línea para responder a las necesidades más apremiantes de los ciudadanos, darle un uso estratégico a la tecnología para hacer más eficaz la gestión administrativa y guardar los datos de los ciudadanos como un tesoro, garantizando la seguridad de la información.

TÉRMINOS Y DEFINICIONES

Activo: 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 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.

Autenticación: provisión de una garantía de que una característica afirmada por una entidad es correcta.

Ciberseguridad: capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

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.

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 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 regrabados como una cinta de audio.

Gestión de claves: son controles que realizan mediante la gestión de claves criptográficas.

Gestión de riesgos: actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

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.

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).

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

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).

DIAGNÓSTICO

De acuerdo con la labor realizada en el 2018, las Políticas de seguridad de la información con el 33,3% y Seguridad física y del Entorno con el 36,7%, son las de mayor calificación. La evaluación de efectividad de controles, según la ISO 27001, **da como resultado general el 15,7%** según el consolidado siguiente:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	60	INICIAL
A.6	RGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓ	8	60	INICIAL
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	17	60	INICIAL
A.8	GESTIÓN DE ACTIVOS	12	60	INICIAL
A.9	CONTROL DE ACCESO	10	60	INICIAL
A.10	CRIPTOGRAFÍA	0	60	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	22	60	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	11	60	INICIAL
A.13	SEGURIDAD DE LAS COMUNICACIONES	6	60	INICIAL
A.14	JISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTE	0	60	INEXISTENTE
A.15	RELACIONES CON LOS PROVEEDORES	0	60	INEXISTENTE
A.16	IÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMA	0	60	INEXISTENTE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	10	60	INICIAL
A.18	CUMPLIMIENTO	16	60	INICIAL
PROMEDIO EVALUACIÓN DE CONTROLES		**9**	**60**	INICIAL

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

Siguiendo el precepto de los dominios de la ISO 27001 se presentan las situaciones encontradas junto con la recomendación a seguir por cada control señalado en la norma.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA EL 2019

- Realizar evaluación del cumplimiento de las políticas actuales de seguridad de la información.
- Desarrollar campañas semestrales de divulgación y sensibilización de las POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, evaluar/preguntar acerca de qué saben sobre la seguridad de la información, cuáles son sus responsabilidades y cómo aplican la seguridad de la información en su diario trabajo.
- Definir una temática para presentar los temas relevantes de procedimientos de seguridad de la información, tales como el reporte de incidentes, contraseñas, controles de software malicioso, escritorios limpios y documentos físicos, copias de seguridad.
- Continuar o actualizar el inventario de los activos de información y Asegurar que la información reciba un nivel apropiado de protección, de acuerdo con su importancia para la Corporación.

- Asegurar que todo activo de información tenga un propietario con las siguientes responsabilidades:
  a) que los activos estén inventariados;
  b) que los activos estén clasificados y protegidos apropiadamente;
  c) definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes;
  d) manejo apropiado del activo cuando es eliminado o destruido

- Definir una política o procedimiento o directriz o lineamiento que defina el uso aceptable de los activos de información, Devolución de activos, Clasificación de la información, Etiquetado de la información y Manejo de activos que sea conocida por los empleados, contratistas y usuarios de partes externas que usan activos de la Corporación o tienen acceso a ellos.

- A partir de la política de seguridad de la información, se debe definir un Procedimiento para la gestión de Derechos de propiedad intelectual, el uso de software legal y el control de licencias usadas/compradas

- Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional, considerando lo siguiente:

a. Verificar si el nivel directivo y grupo de coordinadores aseguran que todos los procedimientos de seguridad dentro de su área de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información.
b. Verificar la revisión periódica del cumplimiento del centro de cómputo con las políticas y normas de seguridad establecidas.
c. Verificar si los sistemas de información son revisados regularmente para asegurar el cumplimiento de las normas de seguridad de la información

- Evaluar durante el segundo semestre de 2019, el Procedimiento Administración de la Red Interna Corporativa y/o Procedimiento de Cuentas de Usuarios, asegurar que incluya:

a. las redes y servicios de red a los que se permite el acceso;
b. los niveles de autorización para determinar a quién se permite el acceso a qué redes y servicios de red;
c. los controles y gestión para proteger el acceso a las conexiones de red y a los servicios de red;
d. los medios usados para acceder a las redes y servicios de red (uso de VPN o redes inalámbricas, WiFi);
e. requisitos de autenticación de usuarios para acceder a diversos servicios de red;

f. seguimiento del uso de servicios de red.

- En el proceso TIC se debe definir e incorporar directrices para restringir y controlar estrictamente el uso de programas utilitarios (Antivirus, compresor de archivos, desfragmentador, diagnóstico, respaldo o recuperación) que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones de la corporación

- Evaluar la viabilidad y los riesgos para desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información confidencial de CORPOGUAVIO.

NORMATIVIDAD

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Decreto 612 de 4 de Abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.
- Decreto 1008 de 14 de Junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información

SEGUIMIENTO Y EVALUACIÓN

Se programa el monitoreo de los controles definidos en cada uno de los riesgos de seguridad y privacidad de la Información identificados de forma semestral mediante la entrega de un informe con las acciones realizadas de acuerdo a este plan