PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Enero de 2019

OBJETIVO

Definir y orientar los controles con los cuales se busca minimizar los riesgos de seguridad y privacidad de la información de la Corporación Autónoma Regional del Guavio – CORPOGUAVIO, con el fin de proteger y salvaguardar los activos de información, promoviendo así la disponibilidad, integridad y confidencialidad de la información que la entidad maneja.

ALCANCE

El plan de tratamiento de riesgos de la información y privacidad de la información tiene podrá ser aplicada a todos los procesos corporación, en concordancia con lo establecido en el modelo se seguridad y privacidad que la entidad viene implementado

TERMINOS Y DEFINICIONES

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.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrados.

Riesgo: Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.

Riesgo en la seguridad de la información: Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información

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

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En el Plan Estratégico detecnologias de la información y las comunicaciones PETIC 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.

Basado en esta metodología y realizando un diagnostico independiente que identifica el estado actual de CORPOGUAVIO con respecto a los requerimientos del modelo de seguridad y privacidad y teniendo en cuenta las políticas de seguridad de la información de la entidad y el plan de tratamiento y protección de datos personales se detectaron los riesgos de seguridad mas relevantes especificando sus causas tanto internas como externas, una subdirección o área responsable y estableciendo los controles necesarios para disminuir la posibilidad de materializarse estos riesgos, a raíz de estos ítem se detectaron:

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

Donde:

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.

RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A continuación se visualizan los riesgos de Seguridad de la Información

RIESGO	*CAUSA*	*DESCRIPCIÓN*	*CONSECUENCIAS*	*RESPONSABLE*	*INDICADOR /CONTROL /REGISTRO*
Falta de capacidad Instalada	Internas: -Saturación de la red -Limitante de equipos (servidores, PC, Almacenamiento, procesamiento, Elementos de Comunicación) -Sobrecarga de equipos (servidores, PC, Almacenamiento, procesamiento, Elementos de Comunicación) Externas:	Los continuos avances tecnológicos o crecimientos de las necesidades presionan a las entidades a que se actualicen, mejoren o renueven sus elementos de tecnología de la información para evitar que se afecte la Inter operatividad institucional	Atraso tecnológico, incompatibilidad con otros sistemas, incapacidad de soportar la operación de la corporación	Subdirección de Planeación – Proceso Tecnología de la Información	-Tecnologías Revisadas -DE-TIC-FT-HVE Hojas DE Vida DE Equipos -DE-TIC-FT-MHS Mantenimiento DE Hardware y Software

	Continuos cambios y avances tecnológicos (obsolescencia).	por capacidad instalada			
Perdida de información (integridad y/o disponibilidad)	Internas: - - pérdida de información - Daño de Equipos - Manipulación del usuario - Extravió del dispositivo de almacenamiento -Daños por caídas de energía - pérdida de información - Daño de Equipos - Manipulación del usuario - Extravió del dispositivo de almacenamiento	Por omisiones del personal que procesa la información o intervención externa o por situaciones externas no contraladas, se puede llegar a perder parcial o totalmente la información de la entidad.	Pérdida total o parcial de la información	Subdirección de Planeación – Proceso Tecnología de la Información	DE-TIC-FT-RCS Registro o Copias de Seguridad

	-Daños por caídas de energía Externas: - software malicioso - ataques cibernéticos				
Fuga de información por confidencialidad	Internas: -Rotación de personal, -Acceso no autorizado -manejo de contraseñas Externas: -Acceso no autorizado	La rotación de personal ocasiona una continua capacitación que implica desgaste operacional debido a que el nuevo personal deba adquirir las destrezas necesarias para operar las herramientas debidamente, así como la autorización	Mal manejo de la información, perdidas e inexactitud en la respuesta a usuarios, , uso ineficiente de hardware y software	Subdirección de Planeación – Proceso Tecnología de la Información Subdireccion Administrativa y Financiera – Talento Humano	DE-TIC-FT-RCUI Registro Centralizado de Usuarios Institucionales

		para acceder a los diferentes aplicativos, manejo de las contraseñas y concienciación de las políticas de seguridad de la información, derivando en una fuga de información			
Ejecución de actividades sin procedimientos o guías, posible duplicidad de información, o falta de información con las dependencias involucradas en los procesos y procedimientos	Falta de comunicación entre actores, Los usuarios desconocen los procedimientos, inducción deficiente	La falta de comunicación entre las dependencias involucradas en los procedimientos hace que ejecuten tareas varias veces , se consuman mas recursos o las tareas y	Duplicidad de información, reprocesos divulgación de información confidencial	Subdirección de Planeación – Proceso Tecnología de la Información	número de usuarios capacitados

		actividades no cumplan con los objetivos para las que fueron creadas			

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