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

Enero 2020

Versión 1

Corporación Autónoma Regional del Guavio - CORPOGUAVIO
Dirección: Carrera 7 No. 1A-52 Gachalá - Cundinamarca
(+57) 314 395 7802 (031)8538500
atencionalusuario@corpoguavio.gov.co

INTRODUCCIÓN

El plan de tratamiento de riesgos de seguridad y privacidad de la información tiene como fin generar una cultura de prevención contra los riesgos informáticos inmersos en una revolución digital, en los cuales su disponibilidad, integridad y confidencialidad se podrían verse afectados poniendo en riesgo los activos de información de la Corporación Autónoma Regional del Guavio, CORPOGUAVIO. Basados en un enfoque de planeación de gestión del riesgo se pretende realizar una estrategia que permita diagnosticar, evaluar, implementar y desarrollar la Seguridad de la Información enfocados en la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten la memoria historia de la entidad, a través de la implementación de medidas de control de seguridad de la información que permitan gestionar y reducir los riesgos e impactos a que está expuesta de acuerdo a la modificación de la política de administración de riesgos aprobada por la entidad de acuerdo al acto administrativo No. 725 del 25 de julio 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.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

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.
- Ley 1712 de 2014 - Ley de Transparencia y acceso a la información pública

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

1. Establecimiento del Contexto

A continuación, se visualizan los riesgos de Seguridad de la Información

Proceso	#Riesgo	Clase de Riesgo	Causas				Riesgo	Consecuencia
			Establecimiento de contexto interno		Establecimiento de contexto externo			
			factor	Definición de la Causa	factor	Definición de la Causa		
Tecnología de la Información y [illegible]	#R3	Seguridad Digital	Tecnología	-Saturación de la red -Limitante de equipos (servidores, PC, Almacenamiento, procesamiento, Elementos de Comunicación) -Sobrecarga de equipos (servidores, PC, Almacenamiento, procesamiento, Elementos de Comunicación)	Tecnología	- software malicioso	Falta de capacidad Instalada	Atraso tecnológico, incompatibilidad con otros sistemas, incapacidad de soportar la operación de la corporación

	#R4	Seguridad Digital	Tecnología	- pérdida de información - Daño de Equipos - Manipulación del usuario - Extravío del dispositivo de almacenamiento			Perdida de información - integridad	'Pérdida total o parcial de la información
	#R5	Seguridad Digital	Tecnología	-Rotación de personal, -Acceso no autorizado -manejo de contraseñas			Fuga de información por confidencialidad	Mal manejo de la información, perdidas e inexactitud en la respuesta a usuarios, , uso ineficiente de hardware y software

2. Identificación del Riesgo

#Riesgo	Riesgo	Descripción	Activo de Información	Amenaza	Tipo de Vulnerabilidad	Vulnerabilidad
#R3	Falta de capacidad Instalada	¿Qué pude suceder? No accesibilidad a los sistemas de información que posee la entidad ¿Cómo Puede Suceder? Por malos procedimientos o manipulaciones, por sobrecargas de información y/o procesamiento, por saturación de equipos, por falta de mantenimiento ¿Cuándo puede suceder? En cualquier momento ¿Qué Consecuencias tendría su materialización? la no disponibilidad de los servicios tecnológicos con los que cuenta la entidad	SIDCOR, PCT Integrado, SIG, PAGINA WEB, SAE, APP, OBSERVAROTIO AMBIENTAL	Mal funcionamiento del equipo	HARDWARE	Ausencia de esquemas de reemplazo periódico

#R4	Perdida de información - integridad	¿Qué pude suceder? Perdida de información ¿Cómo Puede Suceder? Daño de equipo por manipulación o fenómenos naturales, mal manejo de las plataformas, falta de conocimiento de las políticas de seguridad de la información ¿Cuándo puede suceder? en cualquier momento ¿Qué Consecuencias tendría su materialización? perdida de información, alteración de la información, daño de equipos, desconfiguración	SIDCOR, PCT Integrado, SIG, PAGINA WEB, SAE, APP, OBSERVAROTIO AMBIENTAL	Mal funcionamiento del software	SOFTWARE	Ausencia de documentación
#R5	Fuga de información por confidencialidad	¿Qué pude suceder? Acceso no autorizados a sistemas de información, reprocesos divulgación de información confidencial ¿Cómo Puede Suceder? Por mal uso de las contraseñas, no atender las recomendaciones de seguridad de las plataformas ¿Cuándo puede suceder? en cualquier momento ¿Qué Consecuencias tendría su materialización? perdida de la confidencialidad de la información que reposa en los sistemas de información de la entidad	SIDCOR, PCT Integrado, SIG, PAGINA WEB, SAE, APP, OBSERVAROTIO AMBIENTAL	Uso no autorizado del equipo	SOFTWARE	Contraseñas sin protección

3. ANALISIS DEL RIESGO

CRITERIOS PARA CALIFICAR EL IMPACTO LOS RIESGOS DE SEGURIDAD DIGITAL

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
INSIGNIFICANTE	1	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
MENOR	2	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X días de recuperación.	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad.
MODERADO	3	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X semanas de recuperación.	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MAYOR	4	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación importante del medio ambiente que requiere de ≥X meses de recuperación.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
CATASTRÓFICO	5	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación muy grave del medio ambiente que requiere de ≥X años de recuperación.	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

CORPORACIÓN AUTONOMA REGIONAL DEL GUAVIO - CORPOGUAVIO

Corporación Autónoma Regional del Guavio - Corpoguavio

APLICATIVO PARA EL LEVANTAMIENTO DEL MAPA DE RIESGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL

FASE:	**CALIFICACION Y EVALUACION**
FECHA:	**0/01/1900**

NOMBRE DEL PROCESO	OBJETIVO DEL PROCESO
Tecnología de la Información y las Comunicaciones TICs	Integrar y coordinar los servicios informáticos estratégicamente de manera que se apoye a los diferentes procesos de la Corporación en términos de disponibilidad, integridad y confidencialidad, promoviendo así la investigación de nuevas y mejores tecnologías y el desarrollo de las mismas al interior de la Entidad.

No. DEL RIESGO	NOMBRE DEL RIESGO	CALIFICACION		ZONA RIESGO	MEDIDA DE CONTROL ESTABLECIDA
		PROBABILIDAD (1-5)	IMPACTO (1-5)		
R1	Posible incumplimiento de normas	3	3	ALTA	Revisión semestral de normas Asistencia a Capacitaciones de las diferentes entidades a nivel nacional
R2	Desactualización y obsolescencia de equipos y programas	3	3	ALTA	Revisión en el mercado de nuevas tecnologías. Gestionar recursos para la renovación de los elementos Obsoletos
R3	Falta de capacidad Instalada	3	4	EXTREMA	Seguimiento al formato Hoja de vida de los equipos
R4	Perdida de información - integridad	4	3	ALTA	1. Formulario de capacitación 2. Formato Copias de Seguridad de la información
R5	Fuga de información por confidencialidad	3	3	ALTA	Formato inducción de personal Capacitación sobre sistemas de información y uso de equipos
R6	Utilizar información privilegiada para favorecer a un tercero a cambio de un beneficio particular.	3	4	EXTREMA	Evaluación y verificación de las políticas de seguridad de la información.

Tabla 2. Criterios parar calificar la probabilidad

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

4. CONTROLES

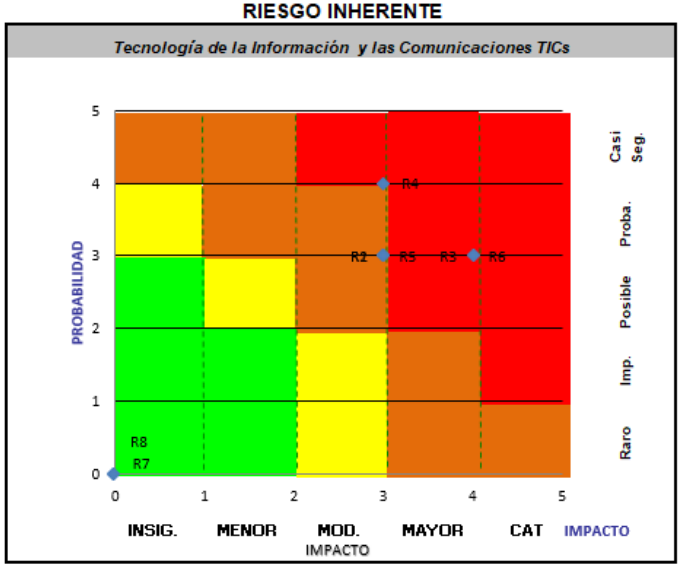
#Riesgo	Riesgo	Descripción del Control
#R3	Falta de capacidad Instalada	La oficina TIC realizará seguimiento al formato Hoja de vida de los equipos para asegurar que estos estén en perfectas condiciones para el su uso diario. Asegurar que las plataformas tendrán Soporte activo a los diferentes aplicativos
#R4	Perdida de información - integridad	la oficina TIC realizará inducción y/o capacitación al personal nuevo y antiguo y se hará seguimiento con el Formulario de inducción de personal. Se realizará las Copias de Seguridad de la información de acuerdo a la política de seguridad de la información Se tendrá en cuenta el plan de contingencia de servicios informáticos de CORPOGUAVIO
#R5	Fuga de información por confidencialidad	La oficina TIC realizara seguimiento de los accesos de acuerdo al formato centralizado de cuentas de usuarios y realizara reinducción sobre sistemas de información y uso de equipos cuando estos sean requeridos

5. Valoración del Riesgo

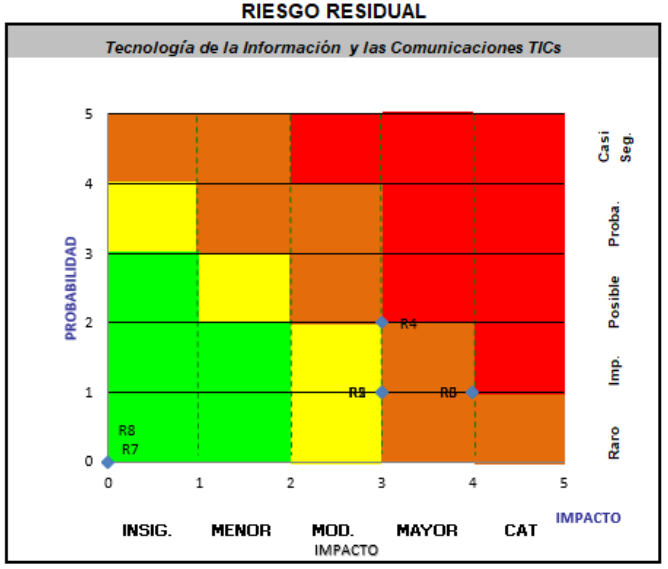
#Riesgo	Riesgo	Tratamiento Elegido	Actividades de control	Responsabilidad de implementar la acción	indicador	Unidad de medida
#R3	Falta de capacidad Instalada	REDUCIR EL RIESGO	revisar el cronograma de mantenimientos de la hoja de vida de los equipos de computo	líder del proceso	# de equipos con mantenimiento realizado / # de equipos programados	porcentaje
#R4	Perdida de información	**REDUCIR EL RIESGO**	realizar copias de seguridad de los activos de información	líder del proceso	# de copias de seguridad realizadas/ # de copias de seguridad programadas	porcentaje
#R5	Fuga de información por	**REDUCIR EL RIESGO**	Revisar el estado de autorizaciones de acceso a las diferentes plataformas de la entidad enviar por medio de las plataformas de comunicación internas tips de seguridad y confidencialidad a todos los funcionarios y contratistas de la entidad	líder del proceso	# de piezas de comunicación enviadas/# de piezas de comunicación planeadas	porcentaje

6. Mapa de Riegos

RIESGO INHERENTE



RIESGO RESIDUAL



	ZONA RIESGO EXTREMA
	ZONA RIESGO ALTA
	ZONA RIESGO MODERADA
	ZONA RIESGO BAJA

7. 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.