

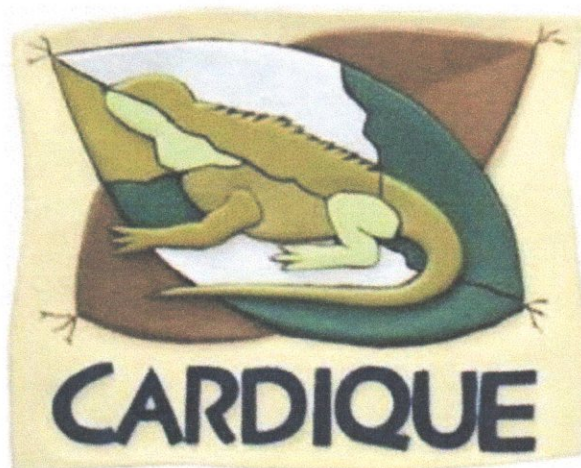
PLAN DE TRATAMIENTO DE RIESGO DE  
SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

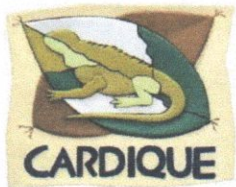
Fecha:19/12/2018

Página 1 de 13



# Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Diciembre de 2018



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

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

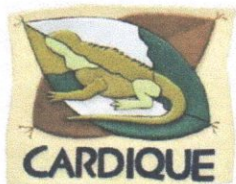
Fecha:19/12/2018

Página 2 de 13

Contenido

1. OBJETIVO .....	3
2. ALCANCE.....	3
3. ÁMBITO DE APLICACIÓN.....	3
4. REQUISITOS APLICABLES .....	3
5. TÉRMINO Y DEFINICIONES.....	4
6. METODOLOGIA PARA LA IMPLEMENTACIÓN .....	8
6.1. Riesgos de Seguridad y Privacidad de la Información. ....	8
7. MONITOREO Y REVISIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN .....	12
8. REFERENCIA Y DOCUMENTOS ASOCIADOS .....	13





## PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

### PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha: 19/12/2018

Página 3 de 13

## 1. OBJETIVO

Definir las disposiciones para la identificación de riesgos de Seguridad de la Información en los procesos de la corporación, con la finalidad de documentar los factores que puedan afectar la confidencialidad, integridad y disponibilidad de la información de CARDIQUE.

## 2. ALCANCE

Comprende las etapas para la identificación de riesgos de Seguridad de la Información, que incluyen: la identificación del riesgo, el análisis del riesgo, la evaluación de controles y los planes de tratamiento de riesgos.

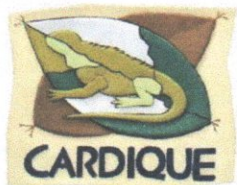
## 3. ÁMBITO DE APLICACIÓN

Aplica a los procesos estratégicos, misionales, de apoyo y de evaluación y control de la Corporación Autónoma Regional del Canal del Dique – CARDIQUE para identificar los riesgos de Seguridad de la Información mediante el cumplimiento de la Política de Administración de los Riesgos adoptado bajo la Resolución No. 1161 del 5 de septiembre del 2018 y la implementación de la Guía – diligenciamiento del Mapa de Riesgos de seguridad y privacidad de la información.

## 4. REQUISITOS APLICABLES

Da cumplimiento a los lineamientos establecidos en la Norma NTC-ISO/IEC 27001:2013, de igual forma, se tomó en cuenta la ley 1712 de 2014 y el decreto reglamentario respectivo 103 de 2015, los lineamientos descritos en la Norma Técnica Colombiana NTC-ISO/IEC 31000 y la guía para la Administración de Riesgos del Departamento Administrativo de la Función Pública (DAFP).





## PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

### PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha: 19/12/2018

Página 4 de 13

## 5. TÉRMINO Y DEFINICIONES

Los términos y definiciones aplicables para la identificación de riesgos de Seguridad de la Información se basan en la Norma NTC-ISO/IEC 27000, Norma NTC-ISO/IEC 27005, Norma NTC-ISO/IEC 31000, Guía GTC 137 (ISO Guía 73:2009 - Vocabulario de Gestión de Riesgos), GTC ISO 27035 y son aplicables al Sistema Integrado de Gestión de la Corporación:

**Aceptación de riesgo:** Decisión informada de asumir un riesgo concreto.

**Activo:** Cualquier cosa que tiene valor para la organización. La norma ISO/IEC 27000, define los siguientes tipos de activos:

- información;
- software, como programas informáticos;
- físico, como computadores;
- servicios;
- personas, y sus calificaciones, habilidades y experiencia; e
- intangibles, como reputación e imagen

**Activo de información:** Conocimiento o información que tiene valor para la organización.

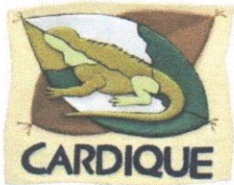
**Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

**Análisis de riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo con base en su probabilidad e impacto de ocurrencia.

**Autenticidad:** Propiedad de que una entidad es lo que afirma ser.

**Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. La información debe ser accedida sólo por aquellas personas que lo requieran como una necesidad legítima para la realización de sus funciones.





## PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha: 19/12/2018

Página 5 de 13

**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. También se puede definir como una medida que modifica el riesgo.

**Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una persona/entidad autorizada. La información debe estar en el momento y en el formato que se requiera, al igual que los recursos necesarios para su uso. La no disponibilidad de la información puede resultar en pérdidas financieras, de imagen y/o credibilidad ante los usuarios de Corporación.

**Evaluación de riesgos:** Proceso global de identificación, análisis y estimación de riesgos.

**Evento de seguridad de la información:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de Seguridad de la Información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

**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:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

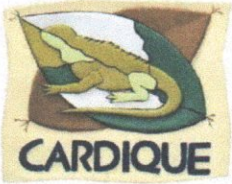
**Impacto:** El coste para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros, como pérdida de reputación o implicaciones legales.

**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.

**Incidente de seguridad de la información:** Un evento o serie de eventos de Seguridad de la Información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

**Integridad:** Propiedad de la información relativa a su exactitud y completitud. La información de la Corporación debe ser con calidad, clara y completa, y solo podrá ser modificada por el personal





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

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:19/12/2018

Página 6 de 13

expresamente autorizado para ello. La falta de integridad de la información puede exponer a la Entidad a toma de decisiones incorrectas, lo cual puede tener impacto reputacional, financiero y/o legal.

**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 información.

**Probabilidad:** Medida para estimar la ocurrencia del riesgo.

**Propietario del riesgo:** Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

**Recursos de tratamiento de la información:** Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

**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.

**Riesgo inherente:** Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

**Riesgo residual:** El riesgo que permanece tras el tratamiento del riesgo.

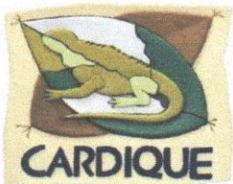
**Selección de controles:** Proceso de elección de las salvaguardas que aseguren la reducción de los riesgos a un nivel aceptable.

**Sistema de Gestión de la Seguridad de la Información:** Conjunto de elementos interrelacionados o interactuantes (estructura organizacional, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer la política y los objetivos de Seguridad de la Información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

**Seguridad de la Información:** Preservación de los principios de confidencialidad, la integridad y la disponibilidad de la información.

**Tratamiento de riesgos:** Proceso de modificar el riesgo, mediante la implementación de controles.





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

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:19/12/2018

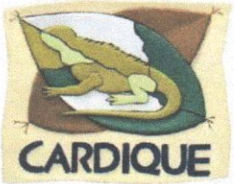
Página 7 de 13

**Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

**Valoración del riesgo:** Proceso de análisis y evaluación del riesgo.

**Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.





## PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

### PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:19/12/2018

Página 8 de 13

## 6. METODOLOGIA PARA LA IMPLEMENTACIÓN

Para la contextualización de este plan, la Corporación cuenta con la Política de Administración de Riesgos, el cual tiene como objetivo administrar los riesgos institucionales mediante la identificación, clasificación, evaluación, valoración y seguimiento de los mismos con el fin de prevenir y mitigar los eventos generados por su materialización.

Para la gestión de riesgos de Seguridad y Privacidad de la Información, CARDIQUE detallara la implementación mediante una Guía – diligenciamiento del Mapa de Riesgos de seguridad y privacidad de la información la cual se articulará con los Mapas de Riesgos existentes, complementándolos con los riesgos de Seguridad y Privacidad de la Información.

### 6.1. Riesgos de Seguridad y Privacidad de la Información.

La situación no deseada es aquella condición que en términos de gestión no queremos que se presente por ningún motivo o que conlleve impedir el logro de los objetivos en desarrollo de las funciones, planes, proyectos y/o procesos. A continuación, se presentan los siguientes ejemplos entre otros:

Las situaciones no deseadas de Seguridad de la Información, son las siguientes:

- Pérdida de Confidencialidad

Ejemplos:

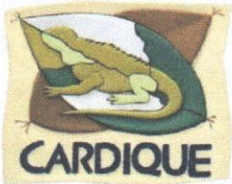
- Divulgación de información de carácter información confidencial (reservada), información confidencial (confidencial), información privada (uso interno) (Información clasificada).
- Acceso de personas no autorizadas a información (que se puede presentar por las situaciones: bloqueo de equipo en ausencia de personal, compartir contraseña, visualización de información que se encuentra en escritorio, contraseña fácil de adivinar).
- Publicación de información clasificada.
- Visualización de información clasificada en hojas dejadas en impresoras desatendidas de la Entidad.

- Pérdida de Integridad

Ejemplos:

- Visualización incompleta de la información.





**PLAN DE TRATAMIENTO DE RIESGO DE  
SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

**PROCESO DE DIRECCIÓN Y MEJORA CONTINUA**

**Versión: 1**

**Fecha: 19/12/2018**

**Página 9 de 13**

- Hurto de dispositivo móvil que contenga información de la Entidad.
- Desaparición de información.

- Pérdida de disponibilidad

Ejemplos:

- Ataque informático o Fuga de información
- Negación de acceso a la información
- Eliminación de Información de forma voluntaria e involuntaria

<b>RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CAUSA</b>	<b>CONSECUENCIA</b>
<b>Perdida Robo o Fuga de Información</b>	Fallas en el proceso de copia de respaldo o de restauración de la información, o pérdida de la misma.	Afectación parcial o total de la continuidad de las operaciones de los servicios del Incumplimiento normativo.
	Fallas en los análisis y socialización de las vulnerabilidades de la infraestructura de TI.	Vulneración de los sistemas de seguridad operando actualmente
	No contar con acuerdos de confidencialidad con los empleados y terceros.	Generación de consultas, funcionalidades o reportes con información sensible de los clientes
	Falta de autorización para la extracción de información generadas por requerimientos.	
	Ingreso a la red y acceso a los activos de TI por parte de máquinas ajenas a la entidad	
	Habilitación de puertos USB en modo lectura y escritura para medios de almacenamiento	
	Ataques cibernéticos internos o externos	
	Empleados no capacitados en los temas de riesgos informáticos.	





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

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

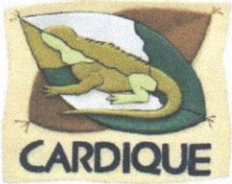
Versión: 1

Fecha:19/12/2018

Página 10 de 13

	Desconocimiento del riesgo	
	Prestar los equipos informáticos a personal no autorizado.	
	No cerrar sesión cuando se desplaza del puesto.	
	Acceso no autorizado a las dependencias.	
	Conectar dispositivos externos a los equipos.	
	Falta de implementación de la política escritorio limpio	
<b>Correos electrónicos de extraña procedencia</b>	Empleados no capacitados en los temas de riesgos informáticos	Cifrado de la información.
	Desconocimiento del riesgo	Captura de las pulsaciones del teclado.
	No generar una Cultura de Seguridad de la Información	Monitoreo de las actividades realizadas en el equipo.
	Falta de Filtros en el Servidor de Correo	Ataque remoto mediante un troyano o gusano.
	Programas de Prevención de Pérdida de Datos	Robo de contraseñas.
		Robo de documentos y/o archivos. - Sistema con mal funcionamiento
<b>Daño en los equipos tecnológicos</b>	Manejo inadecuado de los equipos	Pérdida de información
	Falta de mantenimiento o mala conexión de los mismos en las instalaciones eléctricas	Pérdidas de los equipos informáticos
	Falta de equipos de potenciación	Indisponibilidad del Servicio
	Fallas por defectos de fabrica	Traumatismos en los procesos





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

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

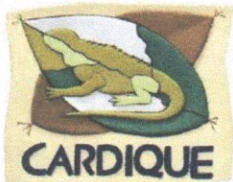
Fecha:19/12/2018

Página **11** de **13**

	Derrame de líquido	
	Falta de ambiente adecuado para los equipos	
	Falta Educación a los usuarios en el manejo de los equipos de computo	
<b>Perdida de conectividad</b>	Daño externo del Servicio de Internet	Interrupción en la continuidad de las actividades y/o tareas que requieran o dependan del servicio de Internet.
<b>Ataques Informáticos</b>	Estimulo o Reto personal	Daño en los equipos tecnológicos
	Rebelión	Incidente en la confidencialidad, integridad y disponibilidad de la información
	Ánimo de lucro	Denegación de servicios
	Espionaje	Secuestro de la información
		Divulgación ilegal de la información
		Suplantación de identidad
		Destrucción de la información
		Soborno de la información

Tabla 1. Tabla de Riesgos de Seguridad y Privacidad de la Información





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

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

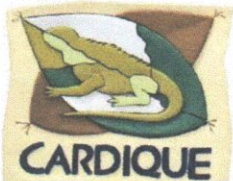
Fecha:19/12/2018

Página **12** de **13**

## 7. MONITOREO Y REVISIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Los Jefes de cada uno de los procesos realizarán el monitoreo anual o en el momento que se determine, de los mapas de riesgos con el apoyo de Control Interno, Calidad y Sistemas con la finalidad de analizar con sus equipos de trabajo el estado de sus riesgos frente a los controles establecidos. Según el resultado de la administración del riesgo, el líder del proceso solicitará ajuste a los riesgos o controles y elaborará acciones de mejoramiento o correctivas en el Plan de Mejoramiento del Proceso, para propender por un efectivo manejo de los Riesgos de Seguridad y Privacidad de la Información.





## PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:19/12/2018

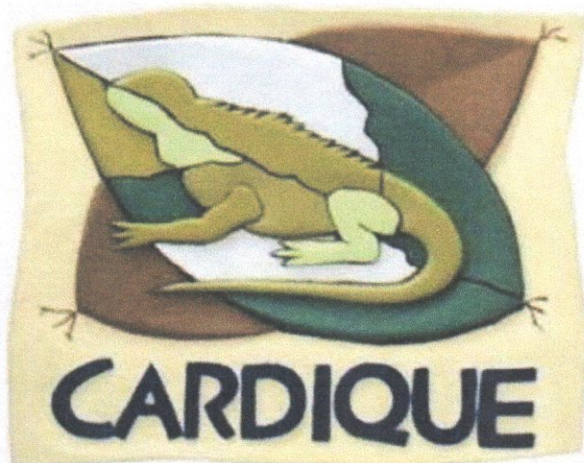
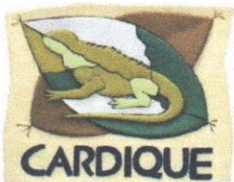
Página **13** de **13**

### 8. REFERENCIA Y DOCUMENTOS ASOCIADOS

El plan de tratamiento de riesgos de seguridad y privacidad de la información se articula con las siguientes referencias y documentos asociados:

- PLAN – MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MSPÍ
- MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN. Departamento Administrativo de Planeación Nacional
- ESTRATEGIA DE GOBIERNO DIGITAL. Ministerio de las TIC
- GUÍA – DILIGENCIAMIENTO DEL MAPA DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.
- POLITICA DE ADMINISTRACIÓN DE RIESGOS
- MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN DE CARDIQUE

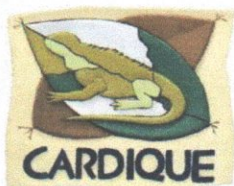




# Guía para el Diligenciamiento de Mapas de Riesgo de Seguridad y Privacidad de la Información

Diciembre de 2018

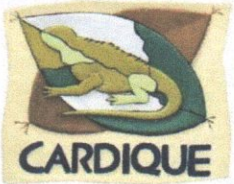




## Contenido

1. OBJETIVO .....	3
2. ALCANCE .....	3
3. APLICABILIDAD .....	3
4. IDENTIFICACIÓN DEL RIESGO .....	3
4.1 Causas .....	3
4.2 Riesgo.....	3
4.3 Consecuencias.....	3
5. CRITERIOS PARA LA VALORACIÓN DEL RIESGO.....	4
5.1 Probabilidad .....	4
5.2 Impacto .....	4
5.3 Valoración de los Riesgos .....	5
6. EVALUACIÓN DE CONTROLES.....	6
6.1 Tipo de Control.....	6
6.2 Estado del Control (Controles).....	7
6.3 Acciones según la Zona de Riesgo .....	7
7. ACCIONES ASOCIADAS AL CONTROL .....	8
8. EVALUACIÓN DE LOS CONTROLES .....	8
9. REFERENCIA Y DOCUMENTOS ASOCIADOS.....	11





## 1. OBJETIVO

Indicar las instrucciones para el diligenciamiento de los Mapas de Riesgos de Seguridad y Privacidad de la Información, mediante el cual se registran los riesgos de seguridad de la información que se identifiquen en la Corporación.

## 2. ALCANCE

Esta guía contempla las etapas para el registro de los riesgos de seguridad y privacidad de la información, inicia con la identificación y análisis del riesgo. Continúa con la evaluación de controles y el registro de los planes de tratamiento para mitigar los riesgos identificados. Termina con el seguimiento para verificar el cumplimiento de los planes de tratamiento establecidos.

## 3. APLICABILIDAD

La guía aplica a los procesos estratégicos, misionales, de apoyo y de evaluación y control de la Corporación.

## 4. IDENTIFICACIÓN DEL RIESGO

### 4.1 Causas

Registre la(s) causa(s) que podrían generar la materialización del riesgo identificado en el proceso.

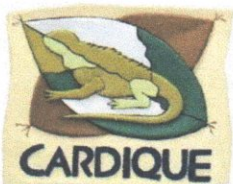
### 4.2 Riesgo

“Registrar el nombre del riesgo”.

### 4.3 Consecuencias

Registre la(s) consecuencia(s) que tendría(n) para el proceso o la entidad la materialización del riesgo identificado.





## 5. CRITERIOS PARA LA VALORACIÓN DEL RIESGO

Para la valoración de riesgos se toman como base dos variables: **la probabilidad** de ocurrencia del riesgo y su **impacto** en caso de que se materialice.

### 5.1 Probabilidad

Se define la probabilidad de ocurrencia para cada riesgo teniendo en cuenta los siguientes criterios de valoración:

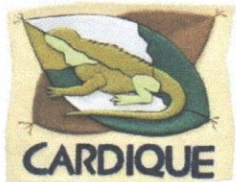
Niveles de Probabilidad		Descripción	Frecuencia
5	Muy alta	Se espera que el evento ocurra en la mayoría de las circunstancias. (Casi seguro)	Más de una vez al año.
4	Alta	Es viable que el evento ocurra en la mayoría de las circunstancias. (Probable)	Al menos una vez en el último año.
3	Moderada	El evento podrá ocurrir en algún momento. (Posible)	Al menos una vez en los últimos dos (2) años.
2	Baja	El evento puede ocurrir en algún momento. (Raro)	Al menos una vez en los últimos cinco (5) años.
1	Muy baja	El evento puede ocurrir sólo en circunstancias excepcionales. (Improbable)	No se ha presentado en los últimos cinco (5) años.

Tabla 1. Valoración de la Probabilidad de Ocurrencia

### 5.2 Impacto

La valoración del impacto que puede ocasionar en la Corporación la materialización de los Riesgos de Seguridad y Privacidad de la Información, se representa con la descripción de los siguientes niveles:





# GUIA PARA EL DILIGENCIAMIENTO DE MAPAS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión: 1

Fecha:19/12/2018

## PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Página 5 de 11

NIVEL	CONCEPTO	DESCRIPCIÓN	SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
1	Muy Bajo	Si el hecho llegara a presentarse tendría consecuencias o efectos mínimos sobre la organización	Afecta a una actividad del proceso.
2	Bajo	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la organización.	Afecta a un grupo de trabajo, a una persona, grupo de personas o algunas actividades del proceso.
3	Moderado	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la organización.	Afecta un proceso de la Corporación
4	Alto	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la organización.	Afecta varios procesos de la Corporación.
5	Muy Alto	Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la organización.	Afecta toda la organización. Multas por incumplimiento de la Legislación. Suspensión de las actividades misionales de la organización.

Tabla 2. Valoración del Impacto

Esta valoración se realiza sobre los principios de la Seguridad de la Información:

**Confidencialidad:** Mide el impacto que tendría para la Corporación Autónoma Regional del Canal del Dique - CARDIQUE la pérdida de confidencialidad sobre los activos de información, es decir, que sean conocidos por personas no autorizadas.

**Integridad:** Mide el impacto que tendría la pérdida de integridad, es decir, si la exactitud y estado completo de los activos de información o sus métodos de procesamiento fueran alterados.

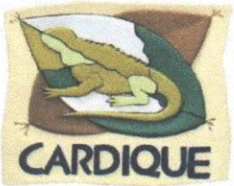
**Disponibilidad:** Mide el impacto que tendría la pérdida de disponibilidad, es decir, si los usuarios autorizados no tuvieran acceso a los activos de información en el momento que lo requieran.

### 5.3 Valoración de los Riesgos

Con base en la probabilidad y la valoración del impacto de cada riesgo, se establecen los niveles de riesgos (tanto los inherentes como los residuales luego de aplicar los controles identificados) teniendo una clasificación propia para la Corporación:

Dimensión del Riesgo de Seguridad y Privacidad de la Información	Valor Asignado	Acción Requerida
Riesgo Extremo	Mayor o igual a 16	Evitar el riesgo empleando controles que busquen reducir el nivel de probabilidad, reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa o compartir y/o transferir el riesgo mediante la ejecución de pólizas.
Riesgo Alto	Mayor que 12 y menor a 16	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado o compartir y/o transferir el riesgo.
Riesgo Moderado	Mayor que 4 y menor o igual 11	Evitar o mitigar el riesgo mediante medidas prontas y adecuadas que permitan llevarlo a la zona de riesgo menor o compartir el riesgo.





<b>Riesgo Bajo</b>	<b>Menor o igual a 3</b>	Asumir el riesgo. Mitigar el riesgo con actividades propias del proceso y por medio de acciones detectivas y preventivas.
--------------------	--------------------------	---

Tabla 3. Dimensión de Riesgos

El riesgo inherente se calcula automáticamente teniendo en cuenta el nivel de probabilidad y de impacto seleccionado, realizando el cálculo de Probabilidad por Impacto ( $P \cdot I$ ).

De igual forma, se distribuyen los riesgos (inherentes y residuales) en las zonas de riesgo de acuerdo con el siguiente Mapa de Calor:

Probabilidad	Valor	Evaluación				
Muy Alta	5	5	10	15	20	25
Alta	4	4	8	12	16	20
Moderada	3	3	6	9	12	15
Baja	2	2	4	6	8	10
Muy Baja	1	1	2	3	4	5
	Valor	1	2	3	4	5
	Impacto	Muy Bajo	Bajo	Moderado	Alto	Muy Alto

Tabla 4. Mapa de Calor para la Representación de los niveles de Riesgo por Zonas

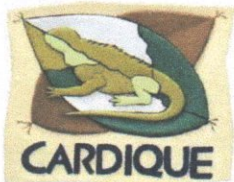
## 6. EVALUACIÓN DE CONTROLES

### 6.1 Tipo de Control

Se Selecciona los tipos de control, teniendo en cuenta las siguientes definiciones:

- **Correctivo:** control que permite el restablecimiento de la actividad, después de la materialización de un riesgo; también la mitigación del impacto del mismo.
- **Detectivo:** control que detecta la aparición de un riesgo, error, omisión o acto deliberado.
- **Preventivo:** control que actúa para eliminar las causas del riesgo o para prevenir su ocurrencia o materialización.





## 6.2 Estado del Control (Controles)

Seleccione de la lista el estado del control teniendo en cuenta las siguientes definiciones:

- **Implementado y Documentado:** el control se ejecuta y está descrito en un documento de la entidad.
- **Implementado y No Documentado:** el control se ejecuta y no está descrito en un documento de la entidad.
- **No implementado y No Documentado:** el control no se ejecuta y no está descrito en un documento de la entidad.
- **No implementado y Documentado:** el control no se ejecuta y está descrito en un documento de la entidad.

Y a la vez se detalla el nombre de los documentos. Ejemplos: Manuales, Procedimientos, Guías, Instructivos, y aquellos documentos que estén establecidos en la entidad para el control del riesgo.

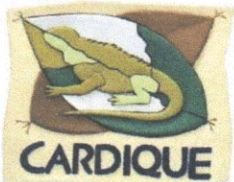
## 6.3 Acciones según la Zona de Riesgo

Las acciones requeridas según la zona de riesgo se identificaran de acuerdo con el resultado obtenido en el mapa de calor, y se tomara cualitativamente con el color descrito en la siguiente tabla:

Zona de Riesgo Aceptable	<b>Asumir el Riesgo:</b> Riesgos para los cuales se determina que el nivel de exposición es adecuado y por lo tanto se acepta.
Zona de Riesgo Moderado	<b>Mitigar o Evitar el Riesgo:</b> Riesgos para los cuales se requiere fortalecer los controles existentes y/o agregar nuevos controles.
Zona de Riesgo Importante	<b>Mitigar o Evitar el Riesgo:</b> Implementación de controles adicionales como parte del fortalecimiento de los actuales o como resultado de haberlo compartido o transferido.
Zona de Riesgo Inaceptable	<b>Evitar el Riesgo:</b> Se requiere de acciones inmediatas que permitan reducir la probabilidad y el impacto de materialización.

Tabla 5. Acciones según Zona de Riesgo





## 7. ACCIONES ASOCIADAS AL CONTROL

**Acciones:** registrar las acciones a realizar para aquellos riesgos que superan el riesgo de la entidad, es decir aquello cuyo nivel de riesgo es Alto o Extremo.

**Responsable:** registre el cargo del responsable de gestionar e implementar el plan de acción escrito anteriormente.

**Periodo de Ejecución:** registre el periodo de ejecución es decir la fecha planificada de inicio y de finalización de las acciones descrita anteriormente.

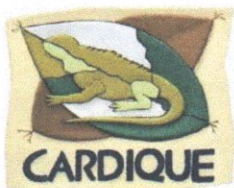
**Registro:** Soporte de evidencia de las acciones ejecutadas.

## 8. EVALUACIÓN DE LOS CONTROLES

Para la evaluación de los controles existentes se debe tener en cuenta la siguiente escala de calificación:

ANÁLISIS Y EVALUACIÓN DE LOS CONTROLES				
DESCRIPCIÓN DEL CONTROL	CRITERIOS PARA LA EVALUACIÓN	EVALUACIÓN		OBSERVACIONES
		SI	NO	
Describa el control determinado para el riesgo identificado.	Existen manuales, instructivos o procedimientos para el manejo del control?	15	0	
	Está (n) definido (s) el (los) responsable (s) de la ejecución del control y del seguimiento?	5	0	
	El control es automático? (Sistemas o Software que permiten incluir contraseñas de acceso, o con controles de seguimiento a aprobaciones o ejecuciones que se realizan a través de éste, generación de reportes o indicadores, sistemas de seguridad con scanner, sistemas de grabación, entre otros).	15	0	





# GUIA PARA EL DILIGENCIAMIENTO DE MAPAS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Versión: 1

Fecha:19/12/2018

Página 9 de 11

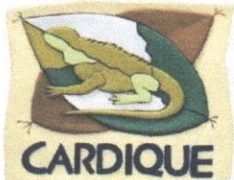
El control es manual? (Políticas de operación aplicables, autorizaciones a través de firmas o confirmaciones vía correo electrónico, archivos físicos, consecutivos, listas de chequeo, controles de seguridad con personal especializado, entre otros)	10	0	
La frecuencia de ejecución del control y seguimiento es adecuada?	15	0	
Se cuenta con evidencias de la ejecución y seguimiento del control?	10	0	
En el tiempo que lleva la herramienta ha demostrado ser efectiva?	30	0	
<b>TOTAL</b>	<b>100</b>	<b>0</b>	

De acuerdo con el tipo de control (preventivo o correctivo) se hace la promediación de los mismos y de acuerdo con el resultado se determina cuántos cuadrantes disminuye el riesgo en el mapa de calor en términos de probabilidad e impacto y teniendo en cuenta los siguientes rangos:

Rangos de Calificación de los controles	Dependiendo si el control afecta la probabilidad o impacto desplaza en la matriz de calificación, Evaluación y Respuesta a los Riesgos	
	Cuadrantes a Disminuir en la probabilidad	Cuadrantes a Disminuir en el impacto
Entre 0 - 50	0	0
Entre 51 - 75	1	1
Entre 76 -100	2	2

Así, una vez conocidos en cuánto se reduce la probabilidad y el impacto, automáticamente se calcula el nivel de riesgo residual con la nueva (P\*I).





# GUIA PARA EL DILIGENCIAMIENTO DE MAPAS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Versión: 1

Fecha:19/12/2018

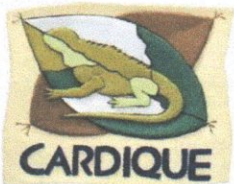
## PROCESO DE DIRECCIÓN Y MEJORA CONTINUA

Página 10 de 11

MAPA DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN														FECHA:17/12/2018								
PROCESO DE DIRECCIÓN Y MEJORA CONTINUA														VERSIÓN:01								
PROCESO DE DIRECCIÓN Y MEJORA CONTINUA														PÁGINA 1 DE 1								
IDENTIFICACIÓN DEL RIESGO			ANÁLISIS DEL RIESGO			EVALUACIÓN DE LOS CONTROLES			ANÁLISIS DEL RIESGO			ACCIONES ASOCIADAS AL CONTROL			EVALUACIÓN DE LOS CONTROLES							
CAUSAS	RIESGO	CONSECUENCIAS	PROBABILIDAD	IMPACTO	ZONA DE RIESGO	TIPO DE CONTROL	ESTADO DE LOS CONTROLES	PROBABILIDAD	IMPACTO	ZONA DE RIESGO	OPCIÓN DE MANEJO	ACCIONES	RESPONSABLE	PERIODO DE EJECUCIÓN	REGISTRO	Existen manuales, instructivos o procedimientos para el manejo del control?	Está (n) definido (s) el (los) responsable (s) de la ejecución del control y del seguimiento?	El control es automático o? El control es manual?	La frecuencia de ejecución del control y seguimiento es adecuada?	Se cuenta con evidencia de la ejecución y seguimiento del control?	En el tiempo que lleva la herramienta ha demostrado ser efectiva?	INDICADOR
Fallas en el proceso de copia de respaldo o de restauración de la información, o pérdida de la misma.		Afectación parcial o total de la continuidad de las operaciones de los servicios del Insumo de la información.				Decreto - Leyes aplicables al proceso (No implementado y Documentado)						Capacitación en Riesgos de Seguridad de la Información	Jefes de Proceso/Profeccional del Área de Sistemas		Registro de asistencia							No. De funcionarios capacitados/No funcionarios del proceso
Fallas en los análisis y socialización de las vulnerabilidades de la infraestructura de IT.						Procedimientos Asociados a la Política de Administración (No implementado y Documentado)						Revisión y ajustes procedimientos asociados	Jefes de Proceso/Profeccional del Área de Sistemas/ Área de Calidad/Área de Control Interno/Área de Planeación									No. Procedimientos Revisados /No total de Procedimientos asociados a la Política de Administración
No contar con acuerdos de confidencialidad con los empleados y terceros.						Manual de Políticas de Seguridad de la Información (No implementado y Documentado)																
Falta de autorización para la extracción de información generada por ingreso a la red.													Área de Control Interno/Área de Socialización									

A continuación se relaciona Mapa de Riego de Seguridad y Privacidad de la Información en formato Excel, como herramienta para ser diligenciada de forma dinámica por los Jefes de Proceso.





## 9. REFERENCIA Y DOCUMENTOS ASOCIADOS

La Guía para la gestión y clasificación de los activos de la información se articula con las siguientes referencias y documentos asociados:

- PLAN – MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MSPi
- MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN. Departamento Administrativo de Planeación Nacional
- ESTRATEGIA DE GOBIERNO DIGITAL. Ministerio de las TIC
- PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Decreto 612 de 2018 - DAFP
- MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN DE CARDIQUE
- NORMA TECNICA COLOMBIANA NTC/ISO 27001: 2013 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN







[illegible]



[illegible]