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

CORPORACIÓN AUTÓNOMA REGIONAL PARA EL DESARROLLO SOSTENIBLE DEL CHOCÓ – CODECHOCÓ

Julio de 2018

Gestión ambiental con enfoque humano
Quibdó Carrera 1° N° 22-96 Tels.: 6711510
Correo electrónico: contacto@codechoco.gov.co
www.codechoco.gov.co

INTRODUCCIÓN

El presente documento tiene como fin generar una cultura de prevención contra los riesgos a los que día a día se pudieran ver sometidos los activos de información de la Corporación Autónoma Regional para el Desarrollo Sostenible del Chocó – CODECHOCO

Basados en un enfoque de planeación de gestión del riesgo se pretende realizar una estrategia que permita diagnosticar, evaluar, implementar y desarrollar la gestión de incidentes que afectan al activo de información e implantar unas contramedidas en el sistema de gestión informático para disminuir la probabilidad de su materialización.

Todos los servidores públicos, dentro de sus funciones, están expuestos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Como meta fundamental se orienta a gestionar los riesgos, desde su identificación hasta el monitoreo, con el reconocimiento de las causas, efectos, definición de controles y lineamientos claros para su adecuada gestión.

La gestión de los riesgos de seguridad de la información son aquellos procesos .que reducen las pérdidas y brindan protección de la información, permitiendo conocer las debilidades que afectan durante todo el ciclo de vida del servicio. Razón por la cual, se hace necesario identificar los riesgos existentes en la Corporación, unido a la capacitación del personal para que se sigan una serie de normas y procedimientos referentes a la seguridad de la información y recursos

1. OBJETIVOS

1.1 Objetivo General

Establecer una guía metodológica para el adecuado tratamiento de los riesgos a los que están expuestos los activos de información de la Corporación Autónoma Regional para el Desarrollo Sostenible del Chocó CODECHOCO, que permitan identificar, controlar y minimizar los riesgos asociados a los procesos tecnológicos, en busca de una adecuada toma de decisiones para disminuir la probabilidad que se materialice una amenaza o bien reducir la vulnerabilidad del sistema, permitir la recuperación del sistema o la trasferencia del problema a un tercero. Así como

también salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

1.2 Objetivos Específicos

- Consolidar una administración de riesgos acorde con las necesidades de la Corporación Autónoma Regional para el Desarrollo Sostenible del Chocó- CODECHOCO.

- Proteger los activos de información de la Corporación de acuerdo a su clasificación y criterios de Confidencialidad, Integridad y Disponibilidad.

- Gestionar eventos de seguridad de la información.

- Proponer soluciones frente a las amenazas identificadas para minimizar los riesgos a los que está expuesta la Corporación.

- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.

- Crear conciencia a nivel institucional de la importancia y la necesidad de una correcta gestión del riesgo de seguridad de la información.

2. ALCANCE Y LIMITACIONES

2.1 ALCANCE

- La guía metodológica contempla la implementación y la administración de la gestión del tratamiento riesgo de seguridad de la información en la Corporación Autónoma Regional para el Desarrollo Sostenible del Chocó- CODECHOCO, la cual será la pauta para desarrollar las actividades a través de la metodología PHVA (Planear – Hacer – Verificar - actuar) y las directrices de MINTIC.

2.2 LIMITACIONES

- Falta de presupuesto necesario para apoyar la implementación del plan de gestión del riesgo de la seguridad de la información en la Corporación Autónoma Regional para el Desarrollo Sostenible del Chocó- CODECHOCO.

3. RECURSOS

Humano:

Director General, líder del Proceso, Profesionales y contratistas.

Físico: PC, Equipos Servidores, recursos web y equipos de comunicación

Financieros: A estimar

4. RESPONSABLES

- Director General de la Corporación
- Subdirectores.
- Oficina de Gestión Tecnológica

5. DEFINICIONES

Acceso a la información Pública

Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

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…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información:

En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.

Archivo

Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia.

Amenazas

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría

Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Autorización

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, Artículo 3)

Bases de Datos Personales

Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

CIBERSEGURIDAD

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

CIBERESPACIO

Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

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. En una definición más simple, es una medida que modifica el riesgo.

DATOS ABIERTOS

Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

DATOS PERSONALES

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.(Ley 1581 de 2012, art 3)

DATOS PERSONALES PRIVADOS

Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

DATOS PERSONALES MIXTOS

Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

DATOS PERSONALES 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. (Decreto 1377 de 2013, art 3).

DERECHO A LA INTIMIDAD

Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

INFORMACIÓN PÚBLICA CLASIFICADA

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

INFORMACIÓN PÚBLICA RESERVADA

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

PRIVACIDAD

En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

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, basándose en un enfoque de gestión y de mejora continua.

TRAZABILIDAD

Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas

5. GESTIÓN DE RIESGOS

5.1 IMPORTANCIA DE LA GESTIÓN DE RIESGOS

Se ha establecido como prioridad salvar, proteger y custodiar el activo de la información, realizando un diagnóstico de los sistemas de información y los avances tecnológicos implementados en la Corporación La Corporación Autónoma Regional para el Desarrollo Sostenible del Chocó CODECHOCO, sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento con el Gobierno Abierto que viene impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento a la normatividad vigente, teniendo en cuenta que una entidad sin un plan de gestión de riesgos está expuesta a perder su información; se consideran como los riesgos más comunes los ataques dirigidos al software empresarial, daños en los equipos (PC y servidores), afectando la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación y entendiendo que el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad de las actividades de la Corporación tras sufrir alguna pérdida o daño en la información de la entidad. Por lo anterior expuesto es preciso diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

5.1.1 SITUACIÓN NO DESEADA –

- Hurto de información o de equipos informáticos.
- Incendio en las instalaciones de la empresa por desastre natural o de manera intencional.
- Alteración de claves y de información.
- Pérdida de información.

- Daño de equipos y de información
- Atrasos en la entrega de información
- Manipulación indebida de información

5.2 DEFINICIONES GESTIÓN DEL RIESGO

• **Análisis del riesgo**: etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).

• **Contexto estratégico**: son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.

• **Control preventivo**: acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.

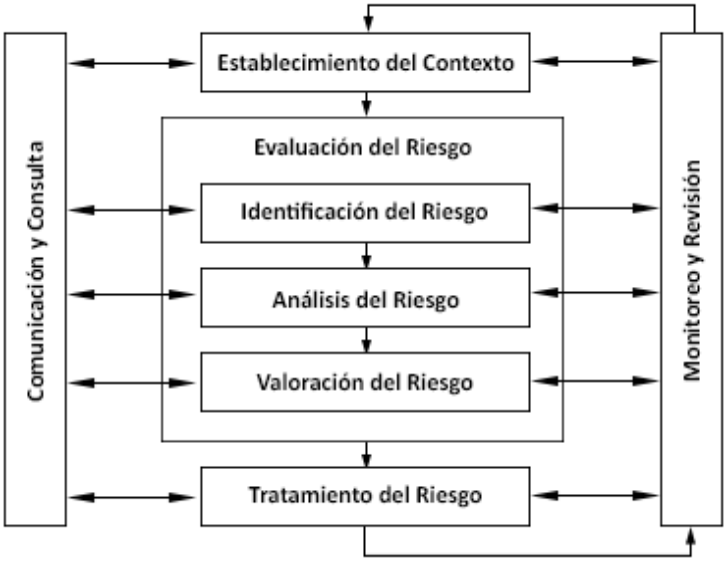
• **Control correctivo**: acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.

• **Materialización del riesgo**: ocurrencia del riesgo identificado

- **Riesgo institucional**: Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por procesos
- Los riesgos que han sido clasificados como estratégicos: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.
- Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.
- Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.

- Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de corrupción, serán considerados como riesgos de tipo institucional.

Administración del Riesgo



5.3 POLÍTICA DE ADMINISTRACIÓN DEL RIESGO.

CODECHOCÓ adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo, y para ello todos los servidores de la entidad se comprometen a:

- Conocer y cumplir las normas internas y externas relacionadas con la administración de los riesgos.
- Fortalecer la cultura de administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.
- Someter los procesos y procedimientos permanentemente al análisis de riesgos con base en la aplicación de las metodologías adoptadas para el efecto.
- Mantener un control permanente sobre los cambios en la calificación de los riesgos para realizar oportunamente los ajustes pertinentes.
- Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.

- Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos que afecten a los objetivos institucionales previstos y los intereses de los usuarios y partes interesadas.
- Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la entidad para así aumentar nuestra eficacia y efectividad.

Para lograr lo anteriormente enunciado la Dirección General en conjunto con la subdirección de Planeación y Direccionamiento Estratégico – PDE, asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

6. METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Plan de Seguridad y Privacidad de la Información en la Corporación Autónoma Regional para el desarrollo Sostenible del Chocó-CODECHOCO, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de la normatividad vigente,

Fases de implementación del **PLAN DE GESTIÓN DEL RIESGO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

1. Diagnosticar
2. Planear
3. Hacer
4. Verificar
5. Actuar

6.1 PROPÓSITO DE LA IMPLEMENTACIÓN DEL PLAN DE GESTIÓN DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN.

- Dar soporte al modelo de seguridad de la información al interior de la Corporación.
- Preparación de un plan de respuesta a eventualidades.
- Alcances, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

7. ACTIVIDADES

- Realizar Diagnóstico en el que se identifiquen vulnerabilidades.
- Elaborar el Alcance del Plan del Tratamiento de Riesgo de Seguridad y Privacidad de la Información
- Realizar la Identificación de los Riesgos
- Valorar los riesgos.
- Visualizar donde se ubican los riesgos y su incidencia.
- Plantear un plan de tratamiento de riesgos acorde con los recursos disponibles y aprobados por las directivas de la Corporación.

8. CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo a las actividades indicadas arriba, se describe a continuación que se debe desarrollar y plazos para su implementación de acuerdo a lo establecido por la Corporación.

- Revisión y/o Actualización de la actual Política de Seguridad.
- Aspectos organizativos de la seguridad de la información.
- Revisión del Control de acceso
- Seguridad en la operativa
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad de las actividades.

10. SEGUIMIENTO y EVALUACIÓN

Al finalizar cada etapa se realizará una socialización por parte del líder del proceso Gestión tecnológica con el Subdirector de Planeación, para presentar el informe respectivo de cada una de las actividades del avance del plan de gestión de riesgos para evaluar todos los pasos se ha ido realizado.

11. ENTREGABLES

- Informe de avance para cada actividad
- Acta de Reunión.
- Plan de tratamiento de riesgo aprobado por los responsables.
- Política de Seguridad.