METODOLÓGICA DE ANÁLISIS DE RIESGOS PARA CORNARE

ABRIL DE 2017

ELABORADO POR	APROBADO POR:	FECHA
Grupo trabajo SIAR-TIC	Director General	Junio 30 de 2017

CONTENIDO

OBJETIVO

Definir la metodología de gestión de riesgos de seguridad y privacidad de la información, a través de la identificación de activos de información, amenazas, vulnerabilidades, riesgos y controles, los niveles aceptables y tratamiento de riesgo, teniendo en cuenta los lineamientos descritos en la Norma Técnica Colombiana NTC ISO 31000.

GLOSARIO

Amenaza: Circunstancia o evento que puede provocar daños en los sistemas de información produciendo pérdidas tangibles o intangibles.

Confidencialidad: Brinda un nivel de seguridad, el cual asegura que la información sea asequible por las personas autorizadas.

Disponibilidad: Permite la disposición, fiabilidad y el acceso oportuno a los datos y servicios a ser usados cuando sea necesario. La falta de disponibilidad causa una interrupción del servicio y afecta directamente la productividad de las organizaciones. Por ello es importante contar con mecanismos y acciones correctivas disponibles (backups, servicios redundantes) que permitan tomar acciones rápidamente.

Integridad: Certeza de que la información y los datos contenidos en el sistema no han sido modificados por entes externos, previniendo cualquier tipo de modificación no autorizada que pueda alterar los datos.

Modelo de Seguridad y Privacidad de la Información (MSPI): reúne el conjunto de lineamientos, políticas, normas, procesos e instituciones que proveen y promueven la puesta en marcha, supervisión, mejora y control de la implementación del modelo, así como a la implementación de la Estrategia de Gobierno en Línea, establecida en manual GEL.

Riesgo: Grado de exposición de un activo en donde un agente de amenaza pueda tomar ventaja de una vulnerabilidad causando impacto a la organización.

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.

Vulnerabilidad: Son Aquellas debilidades que se presentan en los sistemas, lo cual la hace susceptibles de ser afectada, alterada o destruida por alguna circunstancia indeseada afectando su correcto funcionamiento.

FASES

Un Plan Estratégico de Seguridad informática está basado en un conjunto de políticas de seguridad elaboradas a partir de una evaluación de los riesgos a los que están expuestos los activos de información, que indicará el nivel de seguridad en el que se encuentre la Corporación. Con el fin de identificar, medir, controlar y monitorear los riesgos existentes, se proponen las siguientes fases:

1. Identificación de activos de información

Se identifican los activos más relevantes y con mayor valor para la Corporación con el apoyo del área de sistemas, ponderando su impacto a nivel de confidencialidad, integridad, y disponibilidad. Los activos se agrupan en las siguientes categorías: Datos e Información, Claves Criptográficas, Servicios, Software, Hardware, Redes de Comunicaciones, Soportes de Información, Equipamiento Auxiliar e Instalaciones.

2. Identificación de los riesgos

Se identifican las diferentes amenazas y vulnerabilidades a los que están expuestos los activos de información. Generalmente se distinguen tres tipos de amenazas:

- **Criminalidad:** acciones causadas por la intervención humana, que violan la ley y que son penalizados.

- **Sucesos de origen físico:** son todos los eventos naturales y técnicos, y también aquellos que son causados indirectamente por la intervención humana.
- **Negligencia y decisiones institucionales:** son todas las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema.

Las vulnerabilidades, a su vez, se puede agrupar en las siguientes categorías: Ambiental, Económica, Social e Institucional.

3. Estimación del impacto

Luego de identificados los riesgos, se estima el daño sobre el activo, derivado de la materialización de la amenaza. Para obtener el impacto consolidado, se toma el mayor valor de los 3 impactos (Confidencialidad, Integridad y Disponibilidad).

Escala	Valor
Muy bajo	1
Bajo	2
Medio	3
Alto	4
Muy alto	5

4. Estimación del riesgo

Se estima el impacto ponderando con la probabilidad de ocurrencia de la amenaza. Se definen dos criterios para obtener la probabilidad de ocurrencia de una amenaza, que pueden usarse de manera conjunta o de manera individual.

Criterio 1: Motivación y capacidad de la amenaza
Criterio 2: Ocurrencia de la amenaza en el último año

Escala	Probabilidad	Criterio 1	Criterio 2
1	Muy baja	Amenaza poco motivada	1 vez al año o nunca ha ocurrido

2	Baja	Amenaza con motivación media	2 veces al año
3	Media	Amenaza motivada y con capacidad baja	3 veces al año
4	Alta	Amenaza motivada con capacidad media	4 veces al año
5	Muy alta	Amenaza muy motivada y con alta capacidad	5 o más veces al año

Para facilitar la visualización y gestión del riesgo, se propone el siguiente mapa de calor:

Probabilidad					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5
			Impacto		

Con base en la determinación de la probabilidad y la valoración del impacto, se establecen los niveles de riesgos teniendo en cuenta la siguiente clasificación:

Dimensión	Valor	Acción Requerida
Riesgo Extremo	Mayor a 20	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. Compartir o transferir el riesgo mediante la ejecución de pólizas.
Riesgo Alto	Mayor a 15 y menor o igual a 20	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado. Compartir o transferir el riesgo.

Riesgo Moderado	Mayor a 10 y menor o igual a 15	Evitar o mitigar el riesgo mediante medidas prontas y adecuadas que permitan llevarlo a la zona de riesgo menor. Compartir el riesgo.
Riesgo Menor	Mayor a 5 y menor o igual a 10	Mitigar el riesgo mediante de medidas momentáneas y efectivas del proceso que permitan prevenirlo o llevarlo a la zona de riesgo bajo. Asumir el riesgo.
Riesgo Bajo	Menor o igual 5	Asumir el riesgo. Mitigar el riesgo con actividades propias del proceso y por medio de acciones detectivas y preventivas.

En concordancia y alineación con los niveles de riesgos, las acciones requeridas se complementan en la siguiente tabla:

Zona de Riesgo Aceptable	**Asumir el Riesgo:** Riesgos para los cuales se determina que el nivel de exposición es adecuado y por lo tanto se acepta.
Zona de Riesgo Tolerable	**Mitigar el Riesgo:** Riesgos que se puede permitir gestionar, que en caso de materialización la entidad se encuentra en la capacidad de asumirlo.
Zona de Riesgo Moderado	**Mitigar o Evitar el Riesgo:** Riesgos para los cuales se requiere fortalecer los controles existentes y/o agregar nuevos controles.
Zona de Riesgo Importante	**Mitigar o Evitar el Riesgo:** Implementación de controles adicionales como parte del fortalecimiento de los actuales o como resultado de haberlo compartido o transferido.
Zona de Riesgo Inaceptable	**Evitar el Riesgo:** Se requiere de acciones inmediatas que permitan reducir la probabilidad y el impacto de materialización.

5. Matriz de Riesgos y Seguridad de la Información F-DE-01

La documentación del registro de activos de información, su valoración en cuanto a las dimensiones de confidencialidad, integridad, disponibilidad y el análisis de riesgos de seguridad y privacidad de la información, se realiza utilizando el formato Matriz de Riesgos y Seguridad de la Información F-DE-01, disponible en la carpeta de Anexos del Sistema de Gestión / Procesos de Apoyo / Gestión de TIC.

6. Plan de tratamiento

La formulación de actividades de tratamiento de riesgos de seguridad de la información implica la identificación de los controles existentes y la implementación de nuevos controles, acorde al nivel de riesgo y a la disponibilidad de recursos.

Es importante además definir el tipo de control a implementar:

- **Preventivo:** aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.
- **Correctivo:** aquellos que permiten el restablecimiento de la actividad, después de ser identificado un evento no deseable, también la modificación de las acciones que propiciaron su ocurrencia.
- **Detectivo:** aquellos que detectan un evento no deseable cuando se están ejecutando y por tal razón impiden la materialización del riesgo.

7. Seguimiento y evaluación

Es importante llevar el registro de acciones de seguimiento para cada uno de los controles implementados en el Plan de tratamiento, con el fin de evaluar la eficacia en su implementación, adelantando verificaciones como mínimo semestralmente o cuando se considere necesario, evidenciando todas aquellas situaciones o factores que pueden estar influyendo en la aplicación de las acciones de tratamiento.

El monitoreo semestral debe estar a cargo de los responsables de los procesos, la Oficina de Control Interno y la Oficina de Tecnologías de la Información, aplicando y sugiriendo los correctivos y ajustes necesarios para propender por un efectivo manejo del riesgo de seguridad y privacidad de la información.