SEGUNDA LÍNEA DE DEFENSA

Subdirección de Gestión Organizacional – DATIC

Mejoramiento Gestión Integral del Riesgo – Efectividad de controles

www.cali.gov.co

Puro Corazón por Cali

ALCALDÍA DE SANTIAGO DE CALI

Mejoramiento en la Implementación de la Metodología

Segunda Línea de Defensa Gestión Integral de Riesgos

Articular el inventario de sistemas de información y las bases de datos del registro nacional con la matriz de activos de información del organismo, que a su vez será fuente de identificación de los riesgos gestionados por el proceso en el contexto de seguridad de la información. En el caso de que dentro de los riesgos que gestiona el proceso se identifiquen nuevos activos de información primarios y nuevos activos de información secundarios, estos deberán retroalimentarse en las herramientas del inventario de sistemas de información, las bases de datos del registro nacional y la matriz de activos de información.

Inventario Sistemas de Información + Inventario Hardware y Software + Bases de datos de registro nacional =Matriz Activos de Información = Aseguramiento del Riesgo Seguridad de la Información.

En la formulación de riesgo se tendrá en cuenta el alcance y el objetivo del proceso que se identifica para realizar su gestión, así como el rol que cumple este proceso frente al esquema de líneas de defensa, por lo anterior, los procesos líderes de políticas y planes institucionales, deben gestionar los riesgos asegurando el cumplimiento de los objetivos estratégicos del Modelo Integrado de Planeación y Gestión y el Modelo de Operación por Procesos de la entidad

Es indispensable conocer el objetivo estratégico que se busca asegurar como segunda línea de defensa

Mejoramiento en la Implementación de la Metodología

Segunda Línea de Defensa Gestión Integral de Riesgos

Para la identificación de los riesgos de seguridad de la información, sobre todo con relación al tipo de activo secundario como contenedor de la información, se deben tener en cuenta el capítulo términos y definiciones de la ***política de administración de riesgos.***

"Activos secundarios o de apoyo. son activos de los cuales dependen los activos primarios y estos pueden presentar vulnerabilidades que son explotables por amenazas, cuya meta es deteriorar los activos primarios."(…)

En el caso de que los activos de información identificados no se encuentren como activos críticos en la matriz de activos de información, será decisión de los líderes de proceso la gestión del riesgo de dichos activos de información tanto primarios como secundarios, se debe tener en cuenta el capítulo responsabilidades de la **política de administración de riesgos.**

"identificar y valorar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera. "

Mejoramiento en la Implementación de la Metodología

Segunda Línea de Defensa Gestión Integral de Riesgos

En la formulación de los riesgos de seguridad de la información, hacer referencia a la afectación de la triada (disponibilidad, confidencialidad e integridad), así como tener en cuenta que la palabra pérdida se considera cuando haya lugar la materialización del riesgo identificado y por ende se debe registrar como una consecuencia y/o efecto.

" Generar la trazabilidad de la criticidad (impacto) de las diferentes variables afectadas con base a la triada en las diferentes herramientas documentales"

La(s) vulnerabilidad(es) y amenaza(s) debe(n) estar asociada(s) a los activos de información secundarios que contienen los activos de información primarios, el análisis es particular de cada proceso, pues se pueden encontrar una o varia(s) vulnerabilidad(es) en un mismo tipo de activo de información secundario. De acuerdo con la identificación del riesgo, la vulnerabilidad describe la causa inmediata del riesgo y en el caso de la amenaza esta describe la causa raíz.

"Las vulnerabilidades y amenazas deben estar asociadas entre ellas con base al activo de información secundario"

Mejoramiento en la Implementación de la Metodología

Segunda Línea de Defensa Gestión Integral de Riesgos

Las vulnerabilidades y amenazas identificadas deben tener relación directa frente al tipo de activo secundario identificado, es decir, si en la vulnerabilidad se hace referencia a la falta de conciencia como una conducta del recurso humano que gestiona el activo de información primario, el tipo de activo de información secundario debe ser la persona, por el contrario, en el caso de que el tipo de activo de información secundario se identifique como hardware la vulnerabilidad debe estar asociada al equipo que se está identificando como vulnerable (capacidad de procesamiento, configuración, interfaz, entre otros).

Consultar el capítulo términos y definiciones de la Política Administración de Riesgos; los diferentes activos secundarios

La tipología de los controles está acorde con el momento en el cual se ejecuta el control, así como su propósito. Por lo tanto, en los casos de que el control se realice posterior a la generación de salidas (productos, servicios) este será de tipo correctivo y/o detectivo. Por el contrario si es previo a la entrega de dichas salidas entonces este será preventivo.

"La zona de riesgo inherente que usted tiene hasta antes de crear los controles está conformada de acuerdo con el peso de la probabilidad y el impacto, sea estratégico al establecer el o los control(es)"

Mejoramiento en la Implementación de la Metodología

Segunda Línea de Defensa Gestión Integral de Riesgos

La desviación del control está acorde con el propósito del mismo, es decir, la desviación se da cuando no se cumple el propósito para el cual fue creado o se da un cumplimiento parcial, sin embargo, el incumplimiento en la ejecución de un control no es una desviación.

"La desviación del control es una forma de prevenir el incumplimiento del propósito, no debe suplir el control inicial"

Busque asociar controles mixtos para evitar acciones que no incidan sobre la zona de riesgo residual, pues las acciones son cuando no se logra bajar la zona de riesgo inherente después de aplicados los controles, en el caso de tener controles mixtos y complementarios (preventivos – correctivos) esto hará que el cuadrante de la zona baje de inmediato.

"Es importante idear maneras de prevenir, sin embargo, de acuerdo con las situaciones del entorno y las amenazas que a diario se presentan, es esencial buscar maneras de corregir lo que se ocasiona por defecto"

Resultados de Riesgos migrados con ZR = ZI

La gestión integral del riesgo buscar reductir tanto la probabilidad como el impacto que se puede presentar en la gestión de los procesos orientados a los objetivos de la organización



Inefectividad de Controles
Establecimiento: 19%
Valoración:

Puro Corazón por Cali

ALCALDÍA DE SANTIAGO DE CALI

www.cali.gov.co

¡GRACIAS POR SU ATENCIÓN!

