PLAN DE TRATAMIENTOS DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Elaborado por: Julián Adolfo Vásquez Ospina – Asesor de Informática

Revisado Por: Comité de Gobierno Digital – INCIVA

Aprobado Por: Álvaro Rodríguez Morante – Director del INCIVA

DICIEMBRE DE 2018

Tabla de contenido

1. INTRODUCCION

El INCIVA como ente descentralizado de la Gobernación del Valle, está en la obligación de cumplir la política de gobierno digital impuesta en el decreto No 1008 del 14 de junio del 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

Que en la política de gobierno digital en su artículo 2.2.9.1.1.3 –Principios, tiene como prioridad la seguridad de la información, el cual dice así textualmente: “Este principio busca crear condiciones de uso confiable V en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano”.

La oficina asesora de informática en conjunto con la oficina asesora de planeación, vienen actualizando los riesgos informáticos que puedan afectar las labores de los funcionarios.

Por lo tanto, el INCIVA, en asesoría de la oficina de informática, implementara, socializara y actualizara el plan de tratamientos de riesgos de seguridad y privacidad de la información de la sede central del INCIVA.

Para la realización del documento se tomara en base los lineamientos de seguridad de la información establecidos en la política de gobierno digital del 14 de junio del 2018.

El INCIVA adoptara los lineamientos normativos de: la NTC/ISO 27005, la cual contiene la descripción de los procesos para la gestión del riesgo en la seguridad de la información y sus actividades; y los lineamientos del Decreto 1499 del 11 de septiembre de 2017, del Departamento Administrativo de la Función Pública, aterrizados en el manual de riesgos versión 01, adoptado el 12 de octubre de 2016, para el INCIVA.

2. OBJETIVO

Establecer un plan de tratamiento de riesgos de seguridad y privacidad de la información para la sede central del INCIVA, en asesoría de la oficina de informática, tomando como base la norma técnica colombiana NTC-ISO/IEC 27005 y el Decreto 1499 del 11 de septiembre de 2017, del Departamento Administrativo de la Función Pública.

2.1. OBJETIVOS ESPECIFICOS

- Implementar y socializar el plan de tratamiento de riesgos de seguridad y privacidad de la información para la sede central del INCIVA.
- Aplicar efectivamente los lineamientos de la norma NTC-ISO/IEC 27005.
- Seguir los lineamientos del Decreto 1499 del 11 de septiembre de 2017, del Departamento Administrativo de la Función Pública.

3. ALCANCE

Teniendo en cuenta que el INCIVA cuenta con una sede central y 5 centros operativos, los cuales 4 se encuentran fuera de la ciudad de Cali, el alcance inicial de este plan de tratamiento de riesgos de seguridad y privacidad de la información será para la sede central del INCIVA y el Museo de Ciencias Naturales Federico Carlos Lehmann, ubicado en la Avenida Roosevelt # 24-80 de la ciudad de Cali, Valle del Cauca, aplicando todos los requisitos de la NTC-ISO/IEC 27005 y el Decreto 1499 del 11 de septiembre de 2017, del Departamento Administrativo de la Función Pública.

4. DEFINICIONES

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar

negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

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.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
Consecuencia: Resultado de un evento que afecta los objetivos.
Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Control: Medida que modifica el riesgo.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo: Proceso para asignar valores a la probabilidad y las

consecuencias de un riesgo.

Evitación del riesgo: Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o

las diferentes auditorías de los sistemas integrados de gestión.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

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.

Reducción del riesgo: Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo: Aceptación de la pérdida o ganancia proveniente de un riesgo particular.

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.

Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI: Sistema de Gestión de Seguridad de la Información.

5. NORMAS APLICABLES

- NTC-ISO/IEC 27001:2013
- Decreto 1499 del 11 de septiembre de 2017, del Departamento Administrativo de la Función Pública.

6. INFORMACION GERENAL DE UN PLAN DE TRATAMIENTO DE RIESGOS EN LA SEGURIDAD DE LA INFORMACION

La gestión del riesgo en la seguridad de la información debería ser un proceso continuo. Tales procesos deberían establecer el contexto, evaluar los riesgos, tratar los riesgos utilizando un plan de tratamiento para implementar las recomendaciones y decisiones. La gestión del riesgo analiza los que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir lo que se debería hacer y cuando hacerlo, con el fin de reducir el riesgo hasta un nivel aceptable.
La gestión del riesgo en la seguridad de la información debería contribuir a:

- La identificación de los riesgos.
- La valoración de los riesgos en términos de sus consecuencias para el negocio y la probabilidad de su ocurrencia.
- La comunicación y entendimiento de la probabilidad y las consecuencias de estos riesgos.
- El establecimiento del orden por prioridad para el tratamiento de los riesgos.
- La priorización de las acciones para reducir la ocurrencia de los riesgos.
- La participación de los interesados cuando se toman las decisiones sobre gestión del riesgo y mantenerlos informados sobre el estado de la gestión del riesgo.
- La eficacia del monitoreo del tratamiento del riesgo.
- El monitoreo y revisión con regularidad del riesgo y los procesos de gestión de riesgos.
- La captura de información para mejorar el enfoque de la gestión del riesgo.

- La educación de los directores y del personal acerca de los riesgos y las acciones que se toman para mitigarlos.

Tomado de: Instituto Colombiano de Normas Tecnicas y Certificacion (ICONTEC), Norma Técnica Colombiana NTC-ISO/IEC 27005, 2009, página 5.

7. VISION GENERAL DEL PROCESO DE GESTION DEL RIESGO EN LA SEGURIDAD DE LA INFORMACION

En la siguiente imagen se visualiza la interactividad de las actividades para la valoración y tratamiento del riesgo en un proceso de la gestión del riesgo, estas actividades son: Establecimiento del contexto, valoración del riesgo, tratamiento del riesgo, aceptación del riesgo, comunicación del riesgo y monitoreo y revisión del riesgo.

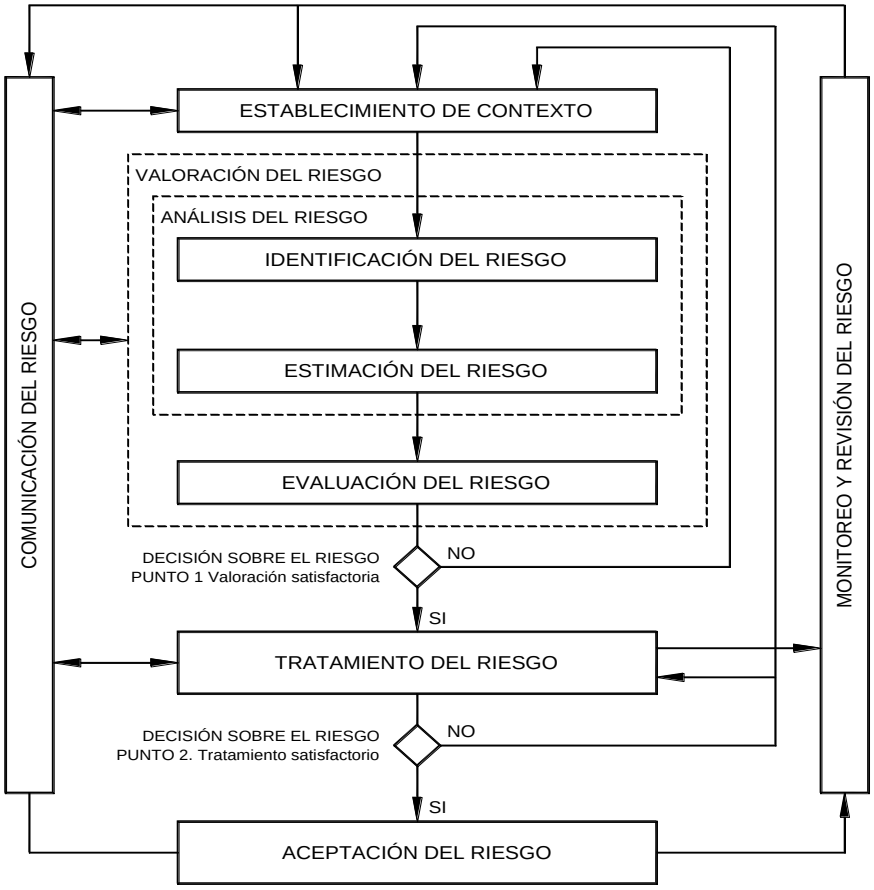

Imagen 1, tomada de: Instituto Colombiano de Normas Tecnicas y Certificacion (ICONTEC), Norma Técnica

Colombiana NTC-ISO/IEC 27005, 2009, página 6.

8. ALINEAMIENTO DEL SGCI Y EL PROCESO DE GESTION DEL RIESGO EN LA SEGURIDAD DE LA INFORMACION

En la siguiente tabla se muestra las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del SGCI.

Proceso de SGSI	Proceso de gestión del riesgo en la seguridad de la información
Planificar	▪ Establecer el contexto. ▪ Valoración del riesgo. ▪ Planificación del tratamiento del riesgo. ▪ Aceptación del riesgo.
Hacer	▪ Implementación del plan del plan del tratamiento del riesgo.
Verificar	▪ Monitoreo y revisión continuos de los riesgos.
Actuar	▪ Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información.

Tabla 1. Alineamiento del SGCI y el proceso de gestión del riesgo en la seguridad de la información. Tomada de Instituto Colombiano de Normas Tecnicas y Certificacion (ICONTEC), Norma Técnica Colombiana NTC-ISO/IEC 27005, 2009, página 7.

9. PROCESO PARA LA ADMINISTRACION DEL RIESGO EN EL INCIVA

El INCIVA, en su manual de riesgos versión 01, adoptado el 12 de octubre de 2016, nos muestra unos lineamientos para la mitigación de riesgos, como se visualiza en la siguiente imagen:

Imagen 2, proceso para la administración del riesgo en el INCIVA

10. ESTABLECIMIENTO DEL CONTEXTO DE RIESGOS DE LA SEGURIDAD DE LA INFORMACION

Para establecer el contexto de riesgos de la seguridad de la información se debe definir los parámetros básicos para la gestión del riesgo, así como el alcance y los criterios para el resto del proceso. Para ello, se deben considerar, tanto los parámetros internos como los externos relevantes, así como los antecedentes de los riesgos que se están evaluando. En el contexto de riesgos se debe tener en cuenta unos criterios básicos, los cuales son: criterios de evaluación del riesgo, criterios de impacto y unos criterios de aceptación del riesgo; los cuales nos ayudaran a determinar el tratamiento que debemos darle a cada riesgo.

11. DEFINICION DE LOS CRITERIOS SEGÚN LA NTC-ISO/IEC 27005

11.1. CRITERIOS DE EVALUACION DEL RIESGO

La NTC-ISO/IEC 27005 recomienda desarrollar criterios para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la organización, teniendo en cuenta los siguientes aspectos:

- El valor estratégico del proceso de información del negocio.
- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, confidencialidad e integridad para las operaciones y el negocio.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación.

11.2. CRITERIOS DE IMPACTO

En el se define el grado de impacto o daños causados cuando un riesgo se materializa y los costos que debe asumir la entidad, los aspectos a considerar son los siguientes:

- Nivel de clasificación de los activos de información impactados.
- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad).

- Operaciones deterioradas (afectación a partes internas o terceras partes).
- Pérdida del negocio y del valor financiero.
- Alteración de planes o fechas límites.
- Daños en la reputación.
- Incumplimiento de los requisitos legales, reglamentarios o contractuales.

11.3. CRITERIOS DE LA ACEPTACION DEL RIESGO

El INCIVA, debe definir para aceptar e identificar el nivel aceptable del riesgo, ya que dependen de las políticas, metas, objetivos de la organización y de las partes interesadas. Los criterios de aceptación del riesgo se deberían establecer considerando los siguientes elementos:

- Criterios del negocio.
- Aspectos legales y reglamentarios.
- Operaciones
- Tecnología.
- Finanzas.
- Factores sociales y humanitarios.

12. IDENTIFICACION DEL RIESGO EN EL PROCESO DE INFORMATICA P7 EN INCIVA

La identificación de los riesgos de la seguridad de la información del INCIVA se encuentra en la intranet de la entidad en la siguiente ruta: Z:\P7_INFORMATICO\PINF_RIESGOS.

La identificación de riesgos se realiza a nivel del Componente Administración del Riesgo de los Procesos, Elemento identificación de riesgos del nuevo MECI-2014; hay de diferentes clases: Riesgo Estratégico, de Imagen, Operativo, Financiero, de Cumplimiento, de Tecnología y de corrupción.

13. ANALISIS DEL RIESGO

El análisis del riesgo en el INCIVA se determina dependiendo de la probabilidad y el impacto del riesgo. Este análisis se puede ver en la ruta: Z:\P7_INFORMATICO\PINF_RIESGOS.

13.1. PROBABILIDAD DEL RIESGO

Nivel	Concepto	Criterios de Factibilidad	Criterios de frecuencia
1	Raro	Puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años
2	Improbable	Pudo ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
3	Posible	Podría ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
4	Probable	Probablemente ocurrirá en la mayoría de las circunstancias	Al menos 1 vez en el año
5	Casi Seguro	Se espera que ocurra en la mayoría de las circunstancias	Mas de una vez al año

Tabla 2. Probabilidad del riesgo

13.2. IMPACTO DEL RIESGO

Nivel	Descriptor	Descripción	Criterios de frecuencia
5	Insignificante	Si se presenta tendría consecuencias mínimas sobre la entidad	Mas de una vez al año
10	Menor	Si se presenta tendría bajo impacto sobre la entidad	Al menos 1 vez en el año
15	Moderado	Si se presenta tendría mediana consecuencia sobre la entidad	Al menos 1 vez en los últimos 2 años
20	Mayor	Si se presenta tendría una alta consecuencia sobre la entidad	Al menos 1 vez en los últimos 5 años
25	Catastrófico	Si se presenta tendría desastrosa consecuencia sobre la entidad	No se ha presentado en los últimos 5 años

Tabla 3. Impacto del riesgo

PROBABILIBAD	IMPACTO				
	Insignificante (5)	Menor (10)	Moderado (15)	Mayor (20)	Catastrófico (25)
Raro (1)	5	10	15	20	25
Improbable (2)	10	20	30	40	50
Posible (3)	15	30	45	60	75
Probable (4)	20	40	60	80	100
Casi Seguro (5)	25	50	75	100	125

14. EVALUACION Y TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LOS ACTIVOS DE INFORMACION DEL INCIVA

Estas acciones se realizan con los lineamientos escritos en el mapa de procesos y de corrupción, ver anexo: Z:\P7_INFORMATICO\PINF_RIESGOS. En este anexo se muestra la metodología a utilizar, el mapa de riesgos, la valoración de los controles y la matriz probabilidad – impacto.

(ORIGINAL FIRMADO)

_____

ALVARO RODRIGUEZ MORANTE

DIRECTOR