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

2019

Gobernación del Huila Piso 5. Teléfonos 8713304 – Fax 8713114
www.contraloriahuila.gov.co – E-mail: info@contraloriahuila.gov.co

1. Objetivo

Controlar y minimizar riesgos asociados al proceso de gestión tecnológica existente en la Contraloría Departamental del Huila garantizando la protección de los activos de información, el manejo de medios, control de acceso y gestión de usuarios.

1.1. Objetivo Específicos

- Realizar un plan de trabajo general para el tratamiento de riesgos de seguridad y privacidad de la información de la **Contraloría Departamental del Huila**, teniendo en cuenta los recursos y la capacidad tecnológica de la entidad.

- Proteger los activos de información mediante la implementación de acciones y controles para mitigación del riesgo y preparar a la entidad para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI)

2. Definiciones

A continuación, se presentan definiciones de términos que se utilizan en la gestión de riesgos de seguridad de la información:

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.

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.

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

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.

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

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.

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.

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.

3. Identificación de riesgos o amenazas

El análisis de riesgos supone el hecho de calcular la posibilidad que ocurran cosas negativas; imaginarse lo que puede ir mal, tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles. De esta forma, se priorizarán los problemas y su costo potencial desarrollando un plan de acción adecuado:

Seguridad Física

- Al agua, que puede dañar los equipos y archivos.
- Al fuego, que puede destruir los equipos y archivos.
- A un robo común, llevándose los equipos y archivos
- Al vandalismo, que dañen los equipos y archivos.
- A terremotos, que destruyen el equipo y los archivos.
- A daños por cortos en el fluido eléctrico.

Seguridad Lógica

- A equivocaciones, que dañen los archivos.
- A la acción de virus, que dañen los equipos y archivos.
- A fallas en los equipos, que dañen los archivos.
- Al robo de datos, difundiéndose los datos sin cobrarlos.
- Al fraude, desviando fondos merced a la computadora.
- A accesos no autorizados, filtrándose datos no autorizados

Luego de elaborar esta lista, se evalúan los efectos que estos riesgos tendrán sobre la plataforma tecnológica

Tecnológica de la Contraloría Departamental del Huila:

- ¿Qué probabilidad hay de que tenga efecto alguno de los riesgos mencionados? Al agua, que puede dañar los equipos y archivos.
- ¿Se cuenta con protección para la filtración de aguas de un piso a otro?
- ¿Se realiza mantenimiento y revisión a las tuberías de agua?
- ¿Se toman las medidas necesarias al momento de realizar alguna reparación a las mismas?

Al fuego, que puede destruir los equipos y los archivos

- ¿La Institución cuenta con protección contra incendios?
- ¿Diversos extintores?
- ¿Detectores de humo?

¿Los empleados están preparados para enfrentar un posibleincendio?
A un robo común, llevándose los equipos y archivos

- ¿Hay personal de seguridad en la Institución?
- ¿Cuántos vigilantes hay?
- Robo común, se cierran las puertas de entrada y ventanas
- ¿Los vigilantes, están ubicados en zonas estratégicas?
- Al vandalismo, que dañen los equipos y archivos
- ¿Existe la posibilidad que algún individuo cause daños intencionados?

A fallas en los equipos, que dañen los archivos

- ¿Los equipos tienen un mantenimiento continuo por parte de personal calificado?
- ¿Cuáles son las condiciones actuales del hardware?
- ¿Es posible predecir las fallas a que están expuestos los equipos?

A terremotos, que destruyen los equipos y archivos

- ¿La Institución se encuentra en una zona sísmica?
- ¿Se encuentran asegurados los equipos?
- ¿El edificio cumple con las normas antisísmicas?
- Un terremoto, ¿cuánto daño podría causar?
- Vandalismo, se cierra la puerta de entrada.

A equivocaciones que dañen los archivos

- ¿Cuánto saben los empleados de computadoras o redes?
- Los que no conocen del manejo de la computadora, ¿saben a quién pedir ayuda?
- Durante el tiempo de vacaciones de los empleados.
- ¿Qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?

A la acción de virus, que dañen los archivos

- ¿Está permitido el uso de memorias USB en las oficinas?
- ¿Todas las máquinas tienen unidades para puerto USB?
- ¿Se cuentan con procedimientos contra los virus?

A accesos no autorizados, filtrándose datos importantes

- ¿Qué probabilidad hay que un competidor intente hacer un acceso no autorizado? Al robo de datos; difundiéndose los datos.
- ¿Cuánto valor tienen actualmente las bases de datos?
- ¿Cuánta pérdida podría causar en caso de que se hicieran públicas?

4. Análisis de la situación

Seguridad Física: La Contraloría Departamental se encuentra ubicada en el Edificio de la Gobernación del Huila, su entorno cuenta con la seguridad física apropiada; aislada de otras edificaciones en los alrededores, cuenta con la seguridad de celaduría y Policía Nacional que realizan las actividades de vigilancia y control del personal que ingresa y sale, como del que retira equipos de cómputo u otros bienes del edificio, exigiendo autorizaciones de retiro de cualquier máquina.

Una de las principales amenazas para la **Contraloría Departamental del Huila** son las inundaciones, ya que, por tratarse de una edificación antigua con tubería muy deteriorada, presenta fugas de agua y rotura de tubos que ocasionan inundaciones que provienen desde el 6º piso de la Gobernación. Este problema viene siendo tratado por la Gobernación del Huila, encargada del mantenimiento de la planta física del edificio.

Seguridad Lógica: Se lleva a cabo a través de administración de usuarios mediante claves de acceso a los servicios tecnológicos, con parámetros específicos como longitud mínima de las contraseñas, las cuales se ha fijado en 6 caracteres, frecuencia de cambio de contraseña y los períodos de vigencia de las mismas, entre otras.

- **Rol de Usuario:** Los sistemas operacionales, bases de datos y aplicativos tienen roles predefinidos que precisan las acciones permitidas por cada uno de estos.

Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

Se prohíbe tener identificaciones de usuario genéricos basados en sus funciones de trabajo. Las identificaciones de usuario deben únicamente identificar individuos específicos, con la siguiente estructura: nombre.apellido.

Todos los equipos tienen definidos los perfiles de usuario de acuerdo con la función y cargo de las personas que acceden a él.

Toda la información del servidor de base de datos que sea sensible, crítica o valiosa debe tiene controles de acceso y es sometida a procesos de respaldo para garantizar que no sea inapropiadamente descubierta, modificada, borrada o no recuperable.

Antes de que un nuevo sistema se desarrolle o se adquiera, los Jefes de Oficina, en conjunto con la Oficina Asesora de Planeación, deberán definir las especificaciones y requerimientos de seguridad necesarios.

La seguridad debe ser implementada por diseñadores y desarrolladores del sistema desde el inicio del proceso de diseño hasta la conversión a un sistema en producción.

Seguridad en comunicaciones: Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, son consideradas y tratadas como información confidencial.

Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la Entidad, debe pasar a través de los sistemas de defensa electrónica que incluyen servicios de ciframiento y verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.

Seguridad para usuarios terceros: Los dueños de los recursos tecnológicos e informáticos que no son propiedad de la **Contraloría Departamental del Huila** y deban

ser ubicados y administrados por ésta, deben garantizar la legalidad del recurso para su funcionamiento.

Los usuarios terceros tendrán acceso a los Servicios y Recursos Tecnológicos, que sean estrictamente necesarios para el cumplimiento de su función, servicios que deben ser aprobados por quien será el Jefe inmediato o coordinador del proyecto. En todo caso, deberán firmar el acuerdo de buen uso de los Recursos Informáticos. y/o certificado de confidencialidad para el manejo de la información.

Software utilizado: Todo software utilizado por la Contraloría Departamental del Huila es adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Entidad o reglamentos internos.

Existe un inventario de las licencias de software de la Contraloría Departamental del Huila que permite su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado.

La Entidad cuenta con otras herramientas, tales como las licencias antivirus y el Firewall con lo cual se minimizan los ataques informáticos. Igualmente, existe un software de filtración de contenidos, que restringe el acceso a algunas páginas de internet.

Servicio de mantenimiento de software: Los sistemas de información requieren de mantenimiento y actualizaciones realizadas por sus propietarios de tal manera que aseguren la continuidad de las operaciones evitando el deterioro y riesgo de no desempeñarse de acuerdo a los estándares establecidos, consistente en soporte técnico y actualización de nuevas versiones para optimizar la funcionalidad. Por ello, la entidad anualmente contrata los servicios de mantenimiento o actualización de los Aplicativos SINFA – Sistema de Administración Contable, Financiero y Nomina; al igual que SYSMAN; para la administración de documentos.

Lineamientos para el Mantenimiento de Hardware y Software: Presentar la solicitud de requerimiento de contratación del servicio de mantenimiento Preventivo y Correctivo de la plataforma tecnológica de la entidad.

Presentar el programa anual de mantenimiento preventivo y correctivo de equipos, teniendo en cuenta la evaluación del inventario, para determinar el número de equipos de cómputo, el número de aplicativos y el cubrimiento de garantías. Una vez realizado el trámite contractual, coordinar con los contratistas la prestación del servicio, estableciendo cronograma de actividades.

Será responsabilidad del servidor público encargado de tecnología supervisar e informar a la Dirección la inadecuada prestación del servicio de mantenimiento preventivo o correctivo o por parte del contratista.

Lineamientos Plan de Seguridad - Elaboración de Backup

El propósito es garantizar la custodia de las bases de datos de los aplicativos que se manejan en la Entidad, indispensables para la reinstalación ante cualquier calamidad, así como también de toda la información que se maneja, en consideración a que ésta es uno de los activos más valiosos de la entidad.

Medios y Datos que se deben preparar

Se disponen de cuatro (4) discos externos de 1 Tb distribuidos en la Oficina Asesora de Planeación y Oficina de Control Fiscal, para el procedimiento de copias de seguridad.

Backup a Sistemas Operativos: Se debe contar con una copia de cada uno de los tipos de Windows instalados en la plataforma tecnológica de la entidad.

Backup a las Bases de Datos: El profesional encargado del manejo de la plataforma tecnológica estará a cargo de la realización de copias de seguridad a las bases de datos de los diferentes aplicativos que se llevan en la entidad y que se encuentran instalados en el servidor de aplicativos. Para ello, de manera mensual ingresará con su clave de acceso y efectuará las respectivas copias, conservándolas en discos externos.

Backup a la Información de los Usuarios: La realización de copias de seguridad estará a cargo de cada usuario, en coordinación con el profesional encargado de tecnología, a través del servidor de copias de seguridad, donde a cada usuario del dominio contraloría.local le ha sido entregado previamente la conexión a una unidad de red, de tal manera que en cada equipo existe una carpeta correspondiente a copia de seguridad, en la que se pueden realizar los Backus necesarios y las veces que se considere conveniente; no obstante, el profesional encargado de tecnología revisará semestralmente que se haya efectuado el backup correspondiente a cada semestre; y efectuará una copia en medio magnético, la cual será debidamente rotulada y conservada en el gabinete designado para ello.

Este procedimiento debe ser realizado con periodicidad de seis meses, o cuando se requiera por necesidad del servicio, ya sea que el usuario sea reemplazado en el cargo por otro, o por fallas de los mismos equipos. De todas formas, el encargado de tecnología deberá coordinar y estar pendiente del backup de esta información.: En el caso de no encontrar respuesta positiva con algún usuario sobre el cumplimiento de la copia

semestral se registrará este incumplimiento a través del Formato F06-F05 Reporte de Incumplimiento Copias de Seguridad.

Backup de Hardware: El profesional encargado de tecnología tendrá identificados los equipos que podrán ser utilizados como equipos de emergencia o de respaldo.

Resultados Esperados: La información de respaldo se encontrará disponible para ser usada en cualquier momento que se presente la falla o contingencia y ante cualquier evento la recuperación rápida a partir del último Backup que se encuentra en el servidor y en las copias en medio magnético conservadas en el gabinete especial que se halla debidamente rotulada con el nombre del usuario y fecha correspondiente. En el caso de bases de datos de los aplicativos, el restablecimiento de la información, se efectuará en coordinación con los propietarios de los aplicativos.

Aseguramiento de Equipos: Como parte de la protección de los activos institucionales, anualmente se contrata el seguro contra todo riesgo para la plataforma tecnológica de la entidad.

PROBABILIDAD			
Concepto	**Valor**	**Descripción**	**Frecuencia**
Raro	1	El evento puede ocurrir sólo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años
Improbable	2	Es muy poco factible que el evento se presente.	Al menos de 1 vez en Los últimos 5 años.
Posible	3	El evento podría ocurrir en algún momento.	Al menos de 1 vez en Los últimos 2 años.
Probable	4	El evento probablemente ocurrirá en la mayoría de las circunstancias,	Al menos de 1 vez en El último año.
Casi Certeza	5	Se espera que ocurra en la mayoría de las circunstancias	Más de 1 vez al año.

IMPACTO		
Concepto	**Valor**	**Descripción**
Insignificante	1	La materialización del riesgo **puede ser controlado** por los participantes del proceso, y **no afecta los objetivos del proceso**.
Menor	6	La materialización del riesgo ocasiona **pequeñas demoras** en el cumplimiento de las actividades del proceso, y **no afecta significativamente el cumplimiento de los objetivos** de la Entidad. Tiene un impacto bajo en los procesos de otras áreas de la Entidad.
Moderado	7	La materialización del riesgo **demora el cumplimiento de los objetivos del proceso,** y tiene un **impacto moderado en los procesos de otras áreas** de la

		Entidad. Puede además causar un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma normal.
Mayor	11	La materialización del riesgo **retrasa el cumplimiento de los objetivos** y tiene un **impacto significativo en la imagen pública** de la Entidad y/o de la Nación. Puede además generar impactos en: la industria; sectores económicos, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras
Catastrófico	13	La materialización del riesgo **imposibilita el cumplimiento de los objetivos,** tiene un **impacto catastrófico en la imagen pública de la entidad**. Puede además generar impactos en: sectores económicos, los mercados; la industria, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras.

Tratamiento de riesgos

IMPACTO		
Concepto	**Valor**	**Descripción**
Insignificante	1	La materialización del riesgo **puede ser controlado** por los participantes del proceso, y **no afecta los objetivos del proceso**.
Menor	6	La materialización del riesgo ocasiona **pequeñas demoras** en el cumplimiento de las actividades del proceso, y **no afecta significativamente el cumplimiento de los objetivos** de la Entidad. Tiene un impacto bajo en los procesos de otras áreas de la Entidad.
Moderado	7	La materialización del riesgo **demora el cumplimiento de los objetivos del proceso,** y tiene un **impacto moderado en los procesos de otras áreas** de la Entidad. Puede además causar un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma normal.
Mayor	11	La materialización del riesgo **retrasa el cumplimiento de los objetivos de la entidad** y tiene un **impacto significativo en la imagen pública** de la Entidad y/o de la Nación. Puede además generar impactos en: la industria; sectores económicos, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras
Catastrófico	13	La materialización del riesgo **imposibilita el cumplimiento de los objetivos de la Entidad**, tiene un **impacto catastrófico en la imagen pública de la Entidad**. Puede además generar impactos en: sectores económicos, los mercados; la industria, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras.