CONTRALORÍA
General del Departamento de Sucre
Control Fiscal Visible a la Comunidad

PLAN DE GESTIÓN DEL RIESGO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

MIGUEL ALFONSO ARRAZOLA SAENZ
Contralor General del Departamento Sucre

SINCELEJO - SUCRE

2018

CONTENIDO

Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co

Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co

INTRODUCCIÓN

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.

Es muy importante que las organizaciones cuenten con un plan de gestión de riesgos para garantizar la continuidad del negocio. Por este motivo, se ha visto la necesidad de desarrollar un análisis de riesgo de seguridad de la información aplicado en la Contraloría General del Departamento de Sucre. Antes de iniciar con este plan de gestión se ha revisado el documento con el diagnóstico del sistema actual de la empresa, donde se conoce la situación actual de la organización y la identificación de los activos con sus respectivas amenazas, para continuar con la medición de riesgos existentes y sugerir las protecciones necesarias que podrían formar parte del plan de gestión de riesgos en la seguridad de la información.

El aporte que arroja este plan permite identificar el nivel de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad existente y sobre todo incentivar al personal a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recursos.

Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co

2. ALCANCES Y LIMITACIONES

2.1 ALCANCES

- ✓ Alcanzar el compromiso de la Contraloría General del Departamento de Sucre, para emprender la implementación del plan de gestión del riesgo en la seguridad de la información.

- ✓ Designar funciones de liderazgo para apoyar y asesorar el proceso de diseño e implementación del plan de gestión.

- ✓ Capacitar al personal de la entidad en el proceso de plan de gestión del riesgo de la seguridad de la información.

2.2 LIMITACIONES

Crear el rubro del presupuesto necesario para apoyar la implementación del plan de gestión del riesgo de la seguridad de la información en la Contraloría Departamental de Sucre.

Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co

3. GESTIÓN DE RIESGOS

3.1 IMPORTANCIA DE LA GESTIÓN DE RIESGOS

La Contraloría General del Departamento de Sucre, sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno en Línea 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 al Decreto 1078 de 2015.

Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las empresas. Una entidad sin un plan de gestión de riesgos está expuesta a perder su información.

Todas las organizaciones deberían implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos informáticos, considerando que en la actualidad los riesgos más comunes son generados por ataques dirigidos al software empresarial, afectando la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación.

Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad del negocio tras sufrir alguna pérdida o daño en la información de la entidad.

Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co

Considerando la situación actual de la Contraloría General del Departamento de Sucre, para reducir los niveles de riesgo, es indispensable diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

3.2 DEFINICIÓN GESTIÓN DEL RIESGO

La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO), definiéndolo como "la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización".

3.3 VISIÓN GENERAL PARA LA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

Figura 1. Proceso para la administración del riesgo.

Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co

3.4 IDENTIFICACIÓN DEL RIESGO

1. Riesgo estratégico: Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

2. Riesgos de imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

3. Riesgos operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.

4. Riesgos financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

5. Riesgos de cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.

6. Riesgos de tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co

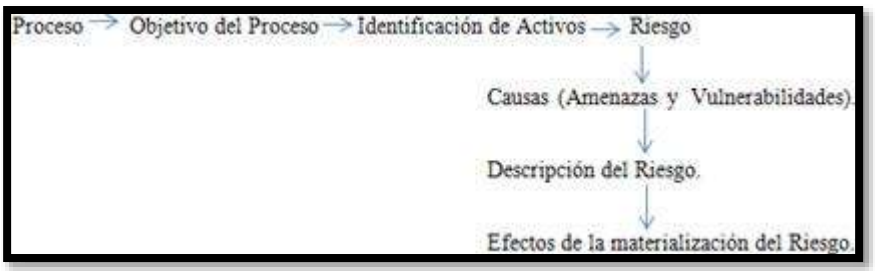
4. ORIGEN DEL PLAN DE GESTIÓN

El gobierno nacional y el ministerio de las TIC han abanderado los proyectos de Gobierno en Línea que permite conocer el funcionamiento de las Contralorías y entidades públicas en el país. Es por ello necesario que la Contraloría General del Departamento de Sucre cumpla con los requisitos necesarios para entregar la información de manera oportuna y eficiente a estas entidades, a la población y a la misma en la Contraloría Departamental de Sucre.

4.1 PROPÓSITO 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 entidad. Conformidad legal y evidencias de la debida diligencia.
- ✓ Preparación de un plan de respuesta a incidentes.
- ✓ Descripción de los requisitos de seguridad de la información para un producto un servicio o un mecanismo.
- ✓ Alcances, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

4.2 IDENTIFICACIÓN DEL RIESGO



Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co

5. ANÁLISIS DE VULNERABILIDADES

5.1 DESCRIPCIÓN DE VULNERABILIDADES

Aunque la protección de la información digital se ve amenazada frecuentemente por errores cometidos por los usuarios, en la Contraloría General del Departamento de Sucre se encontraron otras amenazas e impactos como los siguientes:

- ✓ Inestabilidad en la luz eléctrica, bajas de luz en el transformador, esto puede dañar los equipos de cómputo por tal motivo existe riesgo de pérdida de la información. en la actualidad se han presentado cortes de energía suspendiendo los procesos laborales de todas las oficinas.

- ✓ Las políticas y normas de seguridad de la información existentes no han sido socializadas con todo el personal, por eso es muy común identificar el incumplimiento a las reglas básicas del cuidado tanto de los equipos informáticos y como de la información física y digital, algunas son:

- ✓ Bebidas y alimentos cerca a los equipos de cómputo, cualquier derrame de líquidos afectan los activos de información y de informática.

- ✓ En algunos papeles reutilizables se encontró información personal que debe ser reservada, identificándose la falta de confidencialidad y privacidad.

- ✓ La información es llevada en memorias o discos duros portátiles personales, por ende la información sale de la entidad.

Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co

- ✓ No hay control para el uso de memorias portátiles en los equipos de la entidad, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.

- ✓ Se identificó un completo desconocimiento del tema de seguridad y privacidad de la información en la entidad.

- ✓ Los documentos físicos que se manejan en la entidad no se han digitalizado por lo tanto están expuestos a perdidas y daños físicos debido a que los sitios de almacenamiento en las oficinas no son los adecuados.

Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co

5.2 MATRIZ DE VULNERABILIDADES Y MITIGACIÓN DEL RIESGO

					Análisis		Valoración	Vigencia de
Vulnerabilidad	**Descripción**	**Causa**	**Efecto**	**Clasificación**	**Calificación**	**Evaluación**	**Mitigación del riesgo**	**cumplimiento**
Fallas eléctricas	Inestabilidad eléctrica	Bajas en el transformador de la luz de la entidad	Daño de equipos tecnologicos - perdida de información	Riesgo: Tecnológico - físico-humano	40	Riesgo Moderado	Realizar mantenimiento a la planta eléctrica de la entidad.	Vigencia 2019
Afectación de activos de informacion y activos informáticos.	Desconocimiento de las políticas y normas de seguridad de la informacion.	No. Capacitacion de las políticas y normas de seguridad	Posible pérdida de información - acciones inadecuadas en el tratamiento	Riesgo tecnológico - servicio	60	Riesgo alto	Diseñar, socializar e implementar un manual de seguridad y acceso a la informacion publica	Vigencia 2019

Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co

			de los activos de la informacion.					
Perdida de informacion	La entidad no cuenta con servidores donde se pueda alojar la informacion de la entidad.	Recurso económico	Pérdida de la informacion	* Riesgo en servicio y de la informacion	40	Riesgo Moderado	Adquisición de un servidor para la entidad.	Vigencia 2019
No hay respaldo de informacion en sistemas de informaicon	No existe un proceso establecido de copias de seguridad dentro de la entidad para la información generada en	No hay control para el uso de memorias portátiles en los equipos de la entidad, exponiendo a perder la información por virus no	Posible pérdida de informacion - acciones inadecuadas en el tratamiento de los activos de	Riesgo: Tecnologico - fisico-humano	60	Riesgo alto	implemetacion de un proceso de copias de seguridad y sencibilizacion a los epleados de la entidad.	Vigencia 2019

Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co

	los sistemas de información.	detectados o daños irreparables del hardware.	la informacio n.					
Perdida de informacion	No Existe un sistema de información para la documentación . sensible, como contratos y acuerdos.	No hay un sistemas (Software) documental, para el correcto manejo de la informacion de la entidad.	Posible pérdida de informacio n - acciones inadecuad as en el tratamiento de los activos de la informacio n.	Riesgo: Tecnologico - fisico-humano	40	Riesgo Moderado	compra de un software documental para el mejor manejo de la inforacion publica.	Vigencia 2019

Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co

6. ROPUESTA DE SEGURIDAD

Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de las oficinas.

Replantear las políticas de seguridad y privacidad de la información como también las políticas de seguridad informática.

Revisar las políticas existentes para identificar debilidades y fortalezas, si es necesario se hacen ajustes, teniendo en cuenta que seguridad informática no es igual a seguridad de la información.

Socializar las políticas de seguridad y privacidad de la información con el personal de la en la Contraloría Departamental de Sucre.

Crear un rubro del presupuesto para la adquisición de las licencias y software

Crear los procesos de la oficina de las TIC para la entidad.

Implementar el sistema de documentación digital en la Contraloría Departamental de Sucre para reducir riesgos de pérdida de información física.

La Contraloría Departamental de Sucre, comprometida con la campaña cero papel, está próxima en habilitar el software para digitalización de documentos y gestión documental en los próximos meses.

Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co

6.1 PLAN SEGURO PARA EL ACOPIO DE COPIAS DE SEGURIDAD

Contar con un plan alternativo que asegure la continuidad de la actividad del negocio en caso que ocurran incidentes graves. Nunca se debe olvidar que la realidad es que la entidad puede sufrir un incidente que afecte su continuidad y, dependiendo de la forma en que se gestionen dichos incidentes, las consecuencias pueden ser más o menos graves.

Siempre teniendo en cuenta que la información requiere ser protegida y se debe trabajar sobre los tres pilares fundamentales: confidencialidad, integridad y disponibilidad. Una de las principales características que debe poseer la entidad es buscar cómo establecer un Sistema de seguridad enfocado por procesos, resaltando la importancia que tienen las actividades de monitoreo y la correcta configuración para disminuir los riesgos y realizar tratamiento de las diferentes y constantes vulnerabilidades, para lo cual se deberán tener en cuenta los hallazgos y recomendaciones identificadas, cuyo propósito se encamine a mitigar los riesgos encontrados.

Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co

6.2 PLAN DE CONTINUIDAD DEL NEGOCIO

- ✓ Diseñar un formato de chequeo de acuerdo a las necesidades de la organización que permita realizar las auditorías periódicas con la finalidad de verificar que los objetivos de control, procesos y procedimientos se cumplan.

- ✓ Socializar con los directivos, la importancia del Plan de Continuidad de Negocio, para hacer frente a incidentes es graves de seguridad en la Entidad, resumiendo de forma clara y sencilla cada una de las actividades a desarrollar dentro del plan.

- ✓ Diseñar estrategias para el proceso de recuperación teniendo en cuenta los tiempos de reacción e implementación de contingencias ante la realización de los eventos identificados.

- ✓ Adoptar una de las tres posiciones, que permita minimizar la ocurrencia o los efectos colaterales sobre la red, esto de acuerdo con los siguientes enfoques:

  1) Detectar el riesgo
  2) Plantear controles y efectuar las implementaciones respectivas.
  3) Mitigar el riesgo.

- ✓ Diseñar un Plan de Contingencia teniendo en cuenta que la continuidad en el negocio dependerá de los riesgos y amenazas potenciales que serán tratados de acuerdo a lo siguiente:

  1) Política de copia de seguridad de datos
  2) Procedimientos de almacenamiento fuera de la Entidad

Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co

3) Procedimientos de gestión de emergencias, por desastre natural, por incendio o por inundaciones.

6.3 IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD PARA LA INFORMACIÓN

El análisis permitió identificar que se desconocen y poco se cumplen las políticas de seguridad; por lo cual debe quedar integrado con el documento actual. Se recomienda entre otros tener en cuenta:

- ✓ Socialización y capacitación de temas de seguridad.
- ✓ Ambiente con la seguridad física adecuada.
- ✓ Sistemas de respaldo para mantener soporte de la información en caso de eventualidades catastróficas.

Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co

6.4 PLAN DE CAPACITACIÓN

Contar con un plan de capacitación para el personal encargado de la seguridad de la información, aspectos a fortalecer como:

- ✓ Detectar los requerimientos tecnológicos
- ✓ Determinar objetivos de capacitación para personal
- ✓ Evaluar los resultados de evaluaciones y monitoreo al sistema de seguridad.
- ✓ Elaborar un programa de capacitación en temas de ciber seguridad y políticas de seguridad de la información para todos los funcionarios de la entidad.
- ✓ Evaluar los resultados de cada actividad.

6.5 PLAN DE TRANSICIÓN

Se debe establecer un plan para hacer la transición de las direcciones existente actualmente debido a que los equipos informáticos de la Contraloría General del Departamento de Sucre soportan la nueva versión de ipv4

Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co

7. CONCLUSIONES

El seguimiento constante a los procesos y la implementación del plan de mitigación de riesgo de seguridad de la información deben ser ejecutados, monitoreados y actualizados frecuentemente.

Es indispensable implementar el plan de gestión de riesgo que permitirá prevenir las posibles amenazas encontradas en la infraestructura tecnológica de la entidad.

Las políticas de seguridad de la información de la Contraloría General del Departamento de Sucre deben ser revisadas y actualizadas conforme al crecimiento, cambios de la estructura organizacional, exigencias del gobierno y los mismos procesos dentro de la entidad.

Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co

Calle 20 N°20-47 Edificio La Sabanera 4 Piso Sincelejo- Sucre
Nit: 892080017-1 Teléfonos 2747888-2740594 Telefax 2742040
E-mail: contrasucre@contraloriasucre.gov.co www.contraloriasucre.gov.co