CONTRALORÍA
GENERAL DEL DEPARTAMENTO DE SUCRE
Control Fiscal Oportuno y Participativo

POLÍTICA DE SEGURIDAD DIGITAL

CONTRALORÍA GENERAL DEL DEPARTAMENTO DE SUCRE

JORGE VÍCTOR BELEÑO BAGGOS

CONTRALOR GENERAL DEL DEPARTAMENTO DE SUCRE

2020

PRESENTACIÓN

De conformidad con lo establecido en la Política Nacional de Seguridad Digital, Documento Conpes 3854 de 2016, los lineamientos para la ciberseguridad y ciberdefensa Documentos Conpes 3701 de 2011 y el Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD) 2018, la Contraloría General del Departamento de Sucre reconoce que el crecimiento exponencial del uso del entorno digital para el desarrollo de actividades económicas y sociales, causa incertidumbre y riesgos de seguridad digital y de allí la necesidad de identificarlos, gestionarlos y hacerles seguimiento constantemente.

Esta política de seguridad digital, bajo el enfoque de ciberseguridad y ciberdefensa, se centra en evitar la ocurrencia de las amenazas cibernéticas mediante la administración del riesgo, para que las partes interesadas tengan mayor confianza en la entidad, por el adecuado tratamiento a los riesgos de seguridad digital.

El objetivo principal de la presente política es brindar un marco de gestión de riesgos de seguridad digital en el cual se identifiquen las amenazas y vulnerabilidades a las que la Contraloría General del Departamento de Sucre pueda estar expuesta desde la perspectiva del entorno cibernético, con el fin de fortalecer el ambiente de control e intensificar la confianza de las múltiples partes interesadas en el medio digital.

En cumplimiento de ese propósito y observando los lineamientos del Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD) 2018 del gobierno nacional, la Contraloría General del Departamento de Sucre acoge la gestión de riesgos como un proceso sistemático de identificación, análisis, evaluación, valoración, y tratamiento de los riesgos; aplicando los controles necesarios para evitar, reducir, compartir, transferir o asumir el riesgo con medidas preventivas o correctivas que deberá generar como resultado minimizar pérdidas, maximizar rendimientos y proteger su información digital.

1. ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DIGITAL

La Contraloría General del Departamento de Sucre gestionará los riesgos de seguridad digital de conformidad con los lineamientos establecidos en la Guía para la gestión de riesgos de seguridad digital para entidades públicas, disponible en el siguiente enlace,

Esta política busca orientar a las organizaciones del sector público en el desarrollo de la metodología para la gestión de riesgos de seguridad digital (GRSD), enmarcadas en un ciclo Deming o PHVA para un mayor entendimiento e integración con los sistemas de gestión implementados en las diferentes organizaciones.

Asimismo, acoge la guía para la administración de riesgos y establecimiento de controles versión 4, elaborada por la Función Pública en octubre de 2018, la cual, para la gestión de riesgos de seguridad digital, a su vez, se basada en la guía anteriormente señalada. La guía para administración de riesgos y establecimiento de controles se encuentra disponible en el siguiente enlace.

Por último, la administración de riesgos de seguridad digital de la Contraloría General del Departamento de Sucre se basa en la política de administración de riesgos institucional, la cual establece los pasos e instrumentos para la gestión de riesgos en la entidad.

Para cada fase de la gestión del riesgo digital es necesario tener en cuenta la comunicación y la consulta y los principios fundamentales y generales, con el fin de crear las condiciones para que las múltiples partes interesadas y la ciudadanía en general puedan gestionar los riesgos de Seguridad Digital de sus actividades económicas y sociales, fomentando la confianza en el entorno digital.

La administración del riesgo se fundamenta en el método Deming o Ciclo PHVA y contempla las actividades de identificación, análisis, evaluación y tratamiento; Así mismo, todo lo referente al grado de aceptación, al nivel de riesgo

definido por la entidad y el aseguramiento para llevar a cabo el plan de tratamiento de riesgos respectivo, conforme a los periodos establecidos para tal efecto.

En los siguientes numerales se desarrolla paso a paso el proceso de gestión del riesgo, conforme a lo establecido en el modelo nacional de gestión del riesgo de seguridad digital.

La primera Fase es la de planeación de la "**GRSD**", que constituye el punto de partida para llevar a cabo el proceso de la gestión de riesgos de seguridad digital. Por tanto, es considerada una fase esencial donde se identifica el contexto de la organización, el ecosistema digital de la organización, los criterios de impacto y probabilidad, así como el apetito de riesgo, entre otros parámetros que resultan necesarios para llevar a cabo de buena forma la gestión de riesgos de seguridad digital.

De acuerdo con lo anterior, se desarrolla con mayor énfasis la definición de los elementos que la organización deberá precisar durante la etapa de planificación: compromiso de la lata dirección y el contexto de la organización.

La segunda Fase es la de ejecución de la **GRSD**", a través de la cual se realizan las siguientes actividades de forma secuencial:

i) identificación de activos de información (inventario de activos, clasificación de activos e identificación de infraestructura critica cibernética)
ii) Identificación de riesgos inherentes a la seguridad digital (identificación de amenazas, identificación de vulnerabilidades e identificación de riesgos inherentes la SD),
iii) Valoración de riesgos (determinación y probabilidad de ocurrencia del impacto),
iv) Identificación y evaluación de controles,
v) Determinación del riesgo residual y
vi) Tratamiento de los riesgos residuales (opciones de tratamiento para los riesgos de seguridad digital).

La tercera Fase, de Monitoreo y Revisión está dirigida a evaluar periódicamente los riesgos residuales para determinar la efectividad de los planes de tratamiento y de los controles, de acuerdo a lo definido por la entidad, así mismo contribuye a la toma de decisiones en el proceso de revisión de riesgo por parte de la Alta Dirección y las partes interesadas internas.

En esta fase se deben registrar los riesgos de seguridad digital, el cual constituye el reporte de los riesgos de seguridad digital que se han materializado, con el fin de analizar sus causas, las deficiencias de los controles y las pérdidas que estos pueden generar.

En los reportes se debe entregar la siguiente información:

a. Matriz de riesgos identificados de seguridad digital
b. Listado de activos críticos TI/TO y lista de ICC
c. Reportes de criticidad /impacto de la organización
d. Plan de Tratamiento de riesgos
e. Reporte de evolución de riesgos y modificación del apetito del riesgo
f. Cantidad de riesgos por fuera de la tolerancia del riesgo identificados de acuerdo con la periodicidad de la evaluación realizada.
g. Impacto económico que podría presentarse frente a la materialización de los riesgos.

Esta Fase comprende elementos como la ejecución de auditorías internas y externas y la revisión por la alta dirección a los riesgos de seguridad digital, la medición del desempeño los cuales deben reflejar el cumplimiento de los objetivos propuestos; y por ultimo, la rendición de cuentas que deben formular las partes interesadas sobre la base de sus funciones y su capacidad para actuar, teniendo en cuenta el posible impacto de sus decisiones.

La cuarta y última Fase, de Mejoramiento continuo de la gestión del riesgo de seguridad digital, plantea las acciones de mejorar continua que la entidad debe establecer:

i) Establecer acciones para controlar o prevenir el riesgo o mitigar el impacto, cuando existan hallazgos o no conformidades.
ii) Enfrentar las consecuencoas propias de la no conformidad cuyo riesgo se materializó.
iii) Establecer acciones para disminuir las causas de las no conformidades.

La entidad debe llevar el registro documentado en el formato Plan de Mejoramiento donde se registre el tratamiento realizado a la no conformidad, así como las acciones realizadas para mitigar el impacto de ésta y su resultado, para futuras no conformidades.

En esta misma fase de carácter transversal, se desarrolla el componente de comunicación y consulta que permite asegurar el entendimiento de todas las acciones de la gestión del riesgo por parte de las múltiples partes interesadas.

2. CRITERIOS PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL

a. En relación con el establecimiento del contexto externo

Para determinar el contexto externo la Contraloría General del Departamento de Sucre, deberá considerar, sin limitarse, los siguientes factores relacionados con el entorno digital:

- Factores del entorno cultural, político, jurídico, normativo, financiero, económico y de la competencia (si aplica), ya sea internacional, nacional, regional o local.
- Factores clave y tendencias que tengan impacto en la misión de la entidad o de los objetivos trazados.
- Las capacidades y valores de las partes interesadas externas (clientes, proveedores de servicios).
- Identificación de Partes Interesadas.
- Entes de Control y rectores de políticas de gestión y desempeño.

- Clientes, Proveedores de servicios y Entidades o empresas que sean competencia directa y se relacionen con la misión de la Contraloría General del Departamento de Sucre.
- Aspectos externos que pueden verse afectados con los riesgos de seguridad digital, tales como el ambiente social, económico y ambiental que tengan alguna relación con las operaciones asociadas a la organización.

b. En relación con el establecimiento del contexto interno

El contexto interno considera factores que impactan directamente a:

- La Contraloría General del Departamento de Sucre en general, su funcionamiento, sistemas de información, reglamentación interna, empleados, entre otros aspectos.
- Cada uno de los procesos sobre los cuales están soportadas sus operaciones.

Para determinar los factores de la organización y los procesos, debe considerarse, sin limitarse, los siguientes factores relacionados con el entorno digital:

A. Para la organización

- Recursos económicos, sociales, ambientales, físicos, tecnológicos, financieros, jurídicos, entre otros.
- Sistemas de información o la tecnología informática que soporta las operaciones del negocio.
- Partes interesadas internas.
- Objetivos estratégicos de la Contraloría General del Departamento de Sucre, así como la forma de alcanzarlos.
- La misión, visión, valores y cultura de la organización.
- Las políticas, procesos y procedimientos.
- Sistemas de gestión (Calidad, seguridad en el trabajo, seguridad de información riesgos, entre otros).

- Estructura interna de la organización (organigramas, roles responsabilidades).

B. <u>Para los procesos</u>

- Identificación de los procesos y su respectiva caracterización.
- Detalle de las actividades que se llevan a cabo en el proceso.
- Flujos de información.
- Recursos.
- Alcance de las actividades de gestión del riesgo
- Relaciones con otros procesos de la organización.
- Cantidad de clientes afectados por el proceso.
- Procesos de gestión de riesgos que se tienen actualmente implementados.
- Personal involucrado en la toma de decisiones.

C. En relación con la identificación de activos de información

<u>Para la identificación de activos de información la CGDS deberá:</u>

- Realizar un inventario de los activos de información por cada proceso.
- Identificar el dueño del riesgo sobre el activo y el responsable del activo de información.
- Clasificar los activos.
- Determinar el nivel de importancia del activo.
- Identificar si existe infraestructura crítica cibernética (ICC) e identificar activos relacionados con las tecnologías de la información de TI y con las tecnologías de operación TO asociados a la Infraestructura crítica cibernética (ICC).
- Clasificar la información.

D. En relación con el riesgo inherente de seguridad digital

Los riesgos se deberán identificar basados en las amenazas y vulnerabilidades asociadas al activo de información sobre el cual se está haciendo la identificación.

En este caso hay referencias que permiten vislumbrar la claridad que habría que tenerse para esta definición, en este caso los anexos de la NTC ISO27005:2011.

Identificación de amenazas: Las amenazas representan situaciones o fuentes que pueden hacer daño a los activos digitales.

A manera de ejemplo se citan las siguientes amenazas:

a. **Deliberadas (D), Fortuito (F) o Ambientales (A).**

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fallas en el sistema de suministro de agua	A
Pérdidas de los servicios esenciales	Fallas en el suministro de aire acondicionado	F, D, A
Perturbación debida a la radiación	Radiación electromagnética	F, D, A
	Radiación térmica	F, D, A
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D
Fallas técnicas	Fallas del equipo	D, F
	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F

Acciones no autorizadas	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
Compromiso de las funciones	Error en el uso o abuso de derechos	D, F
	Falsificación de derechos	D

Amenazas dirigidas por el hombre: empleados con o sin intención, proveedores, piratas informáticos, entre otros.

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto	Piratería
	Ego	Ingeniería social
Criminal de la computación	Destrucción de la información	Crimen por computador
	Divulgación ilegal de la información	Acto fraudulento
Terrorismo	Chantaje	Ataques contra el sistema DDOS
	Destrucción	Penetración en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva	Ventaja de defensa
	Espionaje económico	Hurto de información
Intrusos (empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad	Asalto a un empleado
	Ganancia monetaria	Chantaje

E. En relación con la identificación de vulnerabilidades

La Contraloría General del Departamento de Sucre, puede identificar vulnerabilidades en las siguientes áreas:

- Organización de la entidad
- Procesos y procedimientos.
- Rutinas de gestión.
- Personal.
- Ambiente físico.
- Configuración del sistema de información.
- Hardware, software y equipos de comunicaciones.
- Dependencia de partes externas.
- Otras áreas donde se transmita o almacene información digital.

Algunos ejemplos de vulnerabilidades y amenazas.

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Ubicación física de los equipos	Incumplimiento en el mantenimiento del sistema de información
	Fallas en la configuración del hardware	
	Valor económico de los equipos	
Software	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Obsolescencia de software	
Red	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
Bases de datos	Obsolescencia de base de datos	Obsolescencia
	Valor económico de datos	
Personal	Error humano	Incumplimiento en la disponibilidad del personal
	Ausencia de soporte por parte del fabricante	
	Mantenimiento no adecuado de los equipos	
Tipo organización	Falta de planeación	Abuso de los derechos
	Administración de seguridad insuficiente	

F. En relación con la Identificación del riesgo inherente de seguridad digital:

Para cada tipo de activo hay una serie de riesgos, los cuales la Contraloría General del Departamento de Sucre debe identificar. A continuación, se relacionan ejemplos de riesgos con sus respectivas amenazas y vulnerabilidades de acuerdo al tipo de activos.

Tipo de activo	Amenazas	Vulnerabilidades	Riesgo
Software	Exceso de confianza	Ausencia de un procedimiento escrito para el desarrollo y cambios de software	Modificación no autorizada de información o configuración
Base de datos	Hackeo no ético	Contraseñas de bases de datos no seguras	Modificación sin autorización
Red	Negación de acciones	Ausencia de pruebas de envío o recepción de mensajes	Fraude y robo de información
Software	Personal externo	Administración inadecuada de la base de datos	Daño o mal funcionamiento
Hardware	Ubicación física de los equipos	Incumplimiento en el mantenimiento del sistema de información	Fallas en la prestación de servicios

G. DEFINICIÓN DE LOS CRITERIOS DE PROBABILIDAD

Criterios de valoración de la probabilidad de ocurrencia

Nivel asignado	Valor de la probabilidad	Frecuencia del evento	Posibilidad de ocurrencia del evento

Raro	**1**	La situación se ha presentado al menos cada diez años	La situación puede suceder al menos **cada diez años**
Improbable	**2**	La situación se ha presentado al menos una vez cada año	La situación puede suceder al menos **una vez cada año**
Posible	**3**	La situación se ha presentado al menos una vez cada semestre	La situación puede suceder al menos **una vez cada semestre**
Probable	**4**	La situación se ha presentado al menos una vez al mes	La situación puede suceder al menos **una vez al mes**
Casi seguro	**5**	La situación se ha presentado al menos una vez a la semana	La situación puede suceder al menos **una vez a la semana**

H. DEFINICIÓN DE LA ZONA O NIVEL DEL RIESGO

La combinación de impacto y probabilidad estará representada por unos intervalos de valor y una descripción que establece a su vez una representación gráfica lo que se ha denominado en el contexto de la gestión de riesgos, “mapa de calor”.

Zona de riesgo: Las zonas de riesgo según lo dispuesto por la Función Pública (*para aquellas entidades del sector de la economía mixta*), para 5 niveles de impacto y 5 niveles de probabilidad (donde 25 será el mayor valor) se consideran los siguientes:

Zona de riesgo	Valor asignado	Valor asignado
Extremo	Mayor o igual a 15 y hasta 25	Requiere acciones inmediatas para evitar la materialización de los riesgos asociados a la seguridad digital
Alto	Mayor o igual a 9 y menor de 15	Requiere acciones rápidas, a corto plazo, por parte de la alta dirección

		para disminuir los riesgos asociados a la seguridad digital
Moderado	Mayor o igual a 4 y menor de 9	Requiere medidas a mediano plazo y adecuadas, que permitan disminuir los riesgos asociados a la seguridad digital
Bajo	Menor de 3	Requiere monitoreo y seguimiento a través de actividades propias de la entidad y preferiblemente de acciones de detección y prevención

Valor asignado: El valor asignado se refiere a los valores sobre los que se establece la combinación del Impacto y la Probabilidad de un riesgo identificado.

Por ejemplo, si el valor del Impacto de un Riesgo (analizadas las variables de Confidencialidad, Integridad, Disponibilidad, Social, Ambiental o Económica) es igual a 4 y el valor de la Probabilidad es 2 el nivel de riesgo es igual a 8, lo que lo ubica en la zona de riesgo Moderado, según las zonas de riesgo de la siguiente tabla:

IMPACTO	5 Catastrófico					
	4 Mayor					
	3 Moderado					
	2 Menor					
	1 Insignificante					
		1 Raro	2 Improbable	3 Posible	4 Probable	5 Certeza
		PROBABILIDAD				

I. IDENTIFICACIÓN Y EVALUACIÓN DE LOS CONTROLES

Una vez identificado los riesgos inherentes se procede a la identificación y evaluación de los controles. Se busca:

- Determinar si existe uno o varios controles asociados a los riesgos inherentes identificados.
- Si no hay controles asociados a los riesgos inherentes identificados, entonces se registra y se aplica un tratamiento inmediato que implique la implementación de alguna actividad compensatoria, en este caso el nivel de riesgo seguiría igual ya que no se evidenciaría ningún desplazamiento en el mapa de calor y,
- Si los controles existen, se realiza la identificación de los criterios para su evaluación en cuanto a las características de dichos controles

Características de los controles

A continuación, se presentan algunas características de los controles a manera de ejemplo. La Contraloría General del Departamento de Sucre puede adoptarlas, desarrollarlas o referenciarse de acuerdo con sus criterios.

Categoría o niveles del control	Se dan los siguientes tipos de control de acuerdo con los niveles que desarrollan las entidades. **Operativo:** considera cada tarea u operación. Orientado a corto plazo. **Táctico:** considera cada unidad de la empresa (departamento) o cada conjunto de recursos por separado. Orientado a mediano plazo. **Estratégico:** considera a la empresa en su totalidad como un sistema. Orientado a largo plazo.
Naturaleza del control	La naturaleza del control se refiere a las siguientes posibilidades: **Manual:** control donde existe la presencia y la intervención de una persona; ejemplo: autorizaciones a través de firmas.

	Mixto: control donde existe la presencia y la intervención de una persona y una máquina; ejemplo: control de video cámaras. **Automático:** utilizan herramientas tecnológicas; ejemplo: sistemas de información.
Documentación	Esta característica se refiere a determinar si: ¿El control está documentado? ¿El control no está documentado?
Complejidad	Esta característica establece el grado de complejidad de la ejecución del control: ¿El control es complejo para ejecutar? ¿El control no es complejo para ejecutar?
Tipo de control	**Preventivo:** evitan que un evento suceda. Actúan sobre la causa de los riesgos con el fin de disminuir su probabilidad de ocurrencia, y constituyen la primera línea de defensa contra ellos; también actúan para disminuir la acción de los agentes generadores de los riesgos; ejemplo una clave de acceso. **Detectivas:** se diseñan para descubrir un evento, irregularidad o un resultado no previsto; alertan sobre la presencia de los riesgos y permiten tomar medidas inmediatas; pueden ser manuales o automáticos. Sirven para supervisar la ejecución del proceso y se usan para verificar la eficacia de los controles preventivos. Ofrecen la segunda barrera de seguridad frente a los riesgos, pueden informar y registrar la ocurrencia de los hechos no deseados, accionar alarmas, bloquear la operación de un sistema, monitorear o alertar a los funcionarios; ejemplo: un cortafuego o firewall. **Correctivo:** estos no evitan que un evento suceda, pero permiten enfrentar la situación una vez se ha presentado. Permiten el restablecimiento de una actividad, después

	de ser detectado un evento no deseable y posibilita la modificación de las acciones que propiciaron su ocurrencia. Estos controles se establecen cuando los anteriores no operan y permiten mejorar las deficiencias. Por lo general, actúan con los controles Detectivos, implicando re procesos. Son de tipo administrativo y requieren políticas o procedimientos para su ejecución; **ejemplo**: la restauración de una copia de seguridad o back up
Importancia sobre la mitigación del riesgo	Percepción del dueño del riesgo, del riesgo del activo: establece si este control es relevante para mitigar el riesgo: importante o no importante.
Responsable del control	Significa establecer si: ¿El control tiene asignado un responsable? ¿El control no tiene asignado o definido un responsable?
Puede disminuir la probabilidad	Percepción del dueño del riesgo: establece si el control llega a disminuir la probabilidad de ocurrencia del riesgo: si/no
Puede disminuir el impacto	Percepción del dueño del riesgo: establece si el control llega a disminuir el impacto del riesgo: si/no.

J. RESPONSABLE DE LA ADMINISTRACIÓN DE LOS RIESGOS DE SEGURIDAD DIGITAL

El **área de sistemas** será el responsable de la administración de los riesgos de seguridad digital y podrá contar con el apoyo de los demás procesos, a partir del diligenciamiento de la herramienta "***Mapa de riesgos de seguridad digital***", su monitoreo y seguimiento.

K. PLAN DE ACCIÓN DE SEGURIDAD DIGITAL

El resultado de la administración del riesgo de seguridad digital será un **Plan de Acción – Cronograma** que establezca las actividades a desarrollar las acciones asociadas a los controles establecidas en el mapa de riesgo.

Adicionalmente, el plan de acción de seguridad digital deberá integrarse al plan de acción de la entidad.

L. MONITOREO, EVALUACIÓN Y SEGUIMIENTO.

El monitoreo al plan de acción de seguridad digital estará a cargo del área de sistemas, y la evaluación, a cargo de Control Interno, de conformidad con las líneas de auditoría que esta desarrolle y de acuerdo con su Plan de Auditorías.

(ORIGINAL FIRMADA POR)
JORGE VÍCTOR BELEÑO BAGGOS
Contralor General del Departamento de Sucre