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

CONTRALORÍA GENERAL DE BOYACÁ
DIRECCIÓN TÉCNICA DE SISTEMAS
TUNJA, BOYACÁ
2022

FIRMA		FIRMA		FIRMA	
ELABORÓ		REVISÓ		APROBÓ	
CARGO		CARGO		CARGO	

TABLA DE CONTENIDO

1. OBJETIVOS 4
   1.1. OBJETIVO GENERAL 4
   1.2. OBJETIVOS ESPECÍFICOS 4
2. ALCANCES Y LIMITACIONES 5
   2.1. ALCANCES 5
   2.2. LIMITACIONES 5
3. GESTIÓN DE RIESGOS 6
   3.1. IMPORTANCIA DE LA GESTIÓN DE RIESGOS 6
   3.2. DEFINICION GESTION DEL RIESGO 7
   3.3. IDENTIFICACIÓN DEL RIESGO 7
   3.4. SITUACION NO DESEADA 8
4. ORIGEN DEL PLAN DE GESTION 9
   4.1. PROPÓSITO DEL PLAN DE GESTION DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN 9
   4.2. ANALISIS DE RIESGOS 10
5. DESCRIPCIÓN DE VULNERABILIDADES 12
   5.1.1. PROPUESTA DE SEGURIDAD 16
   5.1.2. PLAN SEGURO PARA EL ACOPIO DE COPIAS DE SEGURIDAD 16
   5.1.3. PLAN DE CONTINUIDAD DEL NEGOCIO 17
   5.1.4. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD PARA LA INFORMACIÓN 17
   5.1.5. PLAN DE CAPACITACIÓN 18
   5.1.6. PLAN DE TRANSICIÓN DE IPV4 A IPV6 18

INTRODUCCIÓN

El presente documento contiene los lineamientos necesarios para la Protección de Datos Personales a cargo de La Contraloría General de Boyacá. La adecuación a la normativa sobre protección de datos puede resultar compleja, por esta razón, a través del presente documento se pone a disposición de los sujetos de control y se explican las actividades requeridas para garantizar la protección de los datos personales recolectados por la Entidad. El documento tiene como finalidad lograr el cumplimiento y adecuación de la normativa vigente en materia de Protección de Datos Personales y la implementación de la Ley de Habeas Data.

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 de Boyacá. 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

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Desarrollar un plan de gestión de seguridad y privacidad que permita minimizar los riesgos de pérdida de activos de la información en la Contraloría General de Boyacá.

1.2. OBJETIVOS ESPECÍFICOS

- Gestionar los eventos de seguridad de la información para detectar y tratar con eficiencia, en particular identificar si es necesario o no clasificarlos como incidentes de seguridad de la información.
- Determinar el alcance del plan de gestión de riesgos de la seguridad y privacidad de la información.
- Definir los principales activos a proteger en la entidad.
- Identificar las principales amenazas que afectan a los activos.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo.
- Evaluar y comparar el nivel de riesgo actual con el impacto generado después de implementar el plan de gestión de seguridad de la información.

2. ALCANCES Y LIMITACIONES

2.1. ALCANCES

- Lograr el compromiso de la Contraloría 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 General de Boyacá.

3. GESTIÓN DE RIESGOS

3.1. IMPORTANCIA DE LA GESTIÓN DE RIESGOS

En el ámbito empresarial se está dando mayor prioridad a salvar, proteger y custodiar el activo de la información, debido a que los sistemas de información y los avances tecnológicos están siendo implementados en todas las empresas del mundo.

La información es el pilar y activo intangible más importante de las organizaciones y por ello se deben consolidar estrategias que mejoren su seguridad, disponibilidad, y confidencialidad, dentro de la Entidad.

La digitalización de la información física a los sistemas de información y los inventarios documentales que se deben administrar por largos periodos de tiempo, estimados dentro de los procesos documentales institucionales obliga a que se establezcan políticas y procedimientos en los que todos los integrantes de la organización deben hacer aportes y tener responsabilidades definidas, además de velar por el correcto uso de los servicios y elementos dispuestos para la labor diaria en búsqueda del cumplimiento de los objetivos misionales y administrativos.

La Contraloría General de Boyacá, 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.

Considerando la situación actual de la Contraloría, 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”.

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

Figura 1. Proceso para la administración del riesgo

3.3. IDENTIFICACIÓN DEL RIESGO

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.

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

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.

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.

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.

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.

3.4. SITUACIÓN NO DESEADA

- Hurto de información o de equipos informáticos.
- Hurto de información durante el cumplimiento de las funciones laborales, por intromisión Incendio en las instalaciones de la empresa por desastre natural o de manera intencional. Alteración de claves y de información.
- Pérdida de información.
- Baja Cobertura de internet.
- Daño de equipos y de información Atrasos en la entrega de información Atrasos en asistencia técnica Fuga de información Manipulación indebida de información.

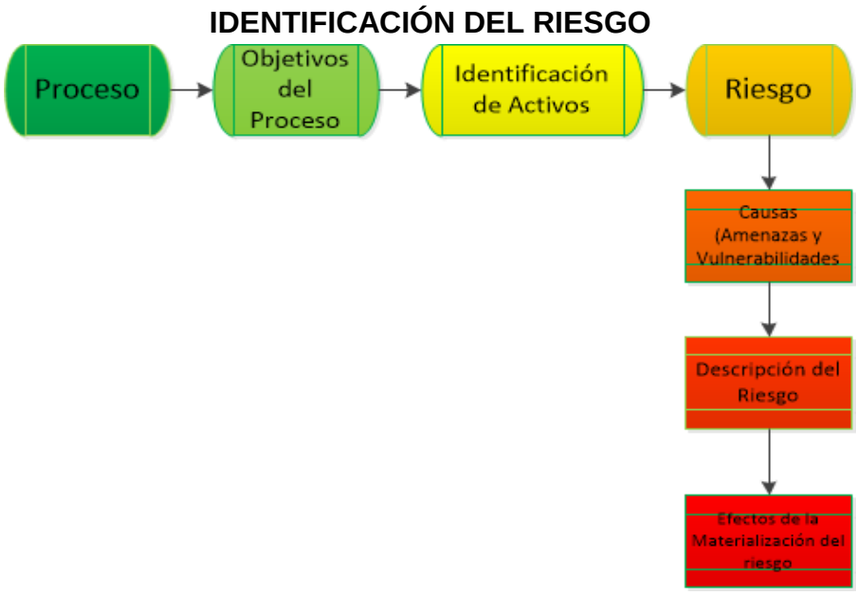
4. ORIGEN DEL PLAN DE GESTIÓN

Debido a que en la Contraloría General de Boyacá a diario se hace necesario tomar acciones para el bloqueo de spam malicioso que llega a las diferentes cuentas de correo de la entidad y que al abrir este tipo de mensajes no sólo descargan virus sino que también secuestran las cuentas institucionales para fines fraudulentos y de otro lado los intentos de hackeo que hoy en día se han convertido en una generalidad y gran preocupación para las entidades; puesto que no sólo realizan espionaje sino incluso borrado y daños a nivel estratégico en las entidades.

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

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. ANÁLISIS DE RIESGOS

De acuerdo a la evaluación y verificación de la posibilidad de ocurrencia de un evento que afecte la operatividad de la infraestructura de TI, se han evaluado a través de la matriz de riesgo, verificando su impacto y posibilidad de ocurrencia, así como el nivel de afectación dentro de la Entidad.

La Calificación del Riesgo*:* Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo. La primera representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse y la segunda se refiere a la magnitud de sus efectos.

Probabilidad	Descripción	Frecuencia	Valor
Casi seguro	El evento probablemente ocurriría en la mayoría de los casos	Más de una vez al año	5
Probable	El evento probablemente ocurriría en la mayoría de los casos	Al menos una vez en el último año	4
Posible	El evento podría ocurrir en algún momento	Al menos una vez en los últimos dos años	3
Improbable	El evento podría ocurrir en algún momento	Al menos una vez en los últimos cinco años.	2
Raro	El evento podría ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos cinco (5) años	1

Probabilidad: Posibilidad de ocurrencia del riesgo. Se puede medir con criterios de:

1. *Frecuencia*, si se ha materializado.
2. *Factibilidad* teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo.

La **Evaluación del Riesgo***:* permite comparar los resultados de su calificación, con los criterios definidos para establecer el grado de exposición de la entidad al riesgo; de esta forma es posible distinguir entre los riesgos EXTREMOS, ALTOS, MODERADOS, BAJOS y fijar las prioridades de las acciones requeridas para su tratamiento.

MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS					
PROBABILIDAD	**Insignificante (1)**	**Menor (2)**	**Moderado (3)**	**Mayor (4)**	**Catastrófico (5)**
Casi Seguro (5)	A	A	E	E	E
Probable (4)	M	A	A	E	E
Posible (3)	B	M	A	E	E
Improbable (2)	B	B	M	A	E
Raro (1)	B	B	M	A	A

B: Zona de riesgo baja: Asumir el riesgo M: Zona de riesgo moderada: Asumir el riesgo, reducir el riesgo A: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir E: Zona de riesgos extrema: Reducir el riesgo, evitar, compartir o transferir

.

Procedimientos de Riesgo Extremos. Son actuaciones inmediatas al incidente que tratan de proteger la integridad de la infraestructura y la información, atajar la progresión del incidente y pararlo en la medida de lo posible, realizando la correspondiente evaluación de daños.

Procedimientos de Riesgo Moderado. Son actuaciones de cada área o servicio que tienden a sustituir los procedimientos habituales de trabajo por otros alternativos que, aunque no reproduzcan totalmente las funcionalidades de cada área o servicio, permiten atender las necesidades más inmediatas y críticas de los mismos.

Procedimientos de recuperación. Normalmente referidos a actividades de los sistemas de información, como son los procedimientos que permiten volver a utilizar datos, aplicaciones, sistemas operativos, etc.

Los riesgos que se tendrán en cuenta en este Plan de Contingencias de TI son los catalogados como EXTREMOS Y ALTOS, es decir aquellos que afectan en forma drástica la operación de la entidad, la pérdida de información confidencial estratégica, la suspensión parcial o total del funcionamiento del hardware, software y/o sistemas de información, considerados como críticos; esta valoración se da en términos de las consecuencias que acarrearía dicha suspensión.

Los riesgos potenciales que pueden afectar la continuidad y operatividad normal del hardware, software y/o los sistemas de información de la entidad, son:

TIPO RIESGO	Riesgo	Probabilidad	Impacto	Zona de Riesgo (Calificación)
Externo	Posibles cambios a la normatividad de control fiscal que afecten el funcionamiento de los sistemas de información.	1	4	ALTO
Externo	Incumplimiento al objeto contractual por parte de los contratistas.	2	3	MODERADO
Externo	Caída o interrupción del sistema eléctrico	5	3	EXTREMO
Externo	Caída del canal de internet	5	3	EXTREMO
Externo	Caída en el servicio telefónico	4	2	ALTO
Externo	Caída de servicios por virus informático	2	3	MODERADO
Externo	Suspensión del servicio por Sismo, inundación o incendio	1	5	EXTREMO

Interno	Retrasos en el Proceso precontractual de la entidad en contratos relacionados con la infraestructura tecnológica de la entidad.	3	3	ALTO
Interno	Contratación sin asistencia técnica, Soluciones Inadecuadas o Incompatibilidad frente a los Requerimientos y Recursos Disponibles	2	4	ALTO
Interno	Pérdida de información considerada confidencial o de reserva por robo, alteración o extracción.	5	4	EXTREMO
Interno	Falla técnica en equipos servidores, de escritorio o de comunicaciones.	5	3	EXTREMO
Interno	Falla técnica en sistemas de información.	5	4	EXTREMO

5. DESCRIPCIÓN DE VULNERABILIDADES

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

- Algunos cables de energía están sueltos, no están cerca a los escritorios o no son suficientes para la cantidad de equipos que tiene cada oficina, existe riesgo de pérdida de información en el caso que sean desconectados por accidente y la información procesada por el funcionario no alcanza a ser guardada.
- 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.

- No hay control para el uso de memorias portátiles en los equipos de la Contraloría, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.
- Se identificó desconocimiento del tema de seguridad y privacidad de la información en la contraloría.
- El sistema ofimático Microsoft Office que se utiliza en la contraloría no cuenta con licencia de funcionamiento en todos los equipos de la entidad. En este caso la entidad está incumpliendo la Ley 603 de 2000.
- Falta personal en el área de sistemas para poder dar soporte a todos los procesos de la Contraloría General de Boyacá. Ya que el Director Técnico de Sistemas debe dar todo el soporte a la Entidad en todos los aspectos tecnológicos y de igual manera brinda soporte y capacitación a nivel Departamental a los Sistemas de Información de Rendición SIA.
- No existe un historial de reportes de los procesos de asistencias y/o mitigación de vulnerabilidades realizados por el personal de sistemas en la entidad.
- Se sacan copias de seguridad en un único disco externo para los servidores y en otro disco para los pc de escritorio. Ésta solución no es óptima, ya que existe riesgo de pérdida total de información en caso de ocurrir desastres naturales, incendios u otros que afecten las copias de respaldo almacenadas.
- No existe un plan de continuidad de negocio que permita reanudar las operaciones normales durante o después de interrupciones significativas a las operaciones de la Contraloría. (en caso de incendio o desastre natural existen altas probabilidades de perder la información de los servidores)
- No se cuentan con los tipos de extintores adecuados para cada emergencia.
- La Contraloría no cuenta con una planta de energía; en la actualidad se han presentado cortes de energía suspendiendo los procesos laborales en todas las oficinas.

5.1. MATRIZ DE VULNERABILIDADES Y MITIGACIÓN DEL RIESGO

					ANALISIS		VALORACION	VIGENCIA DE CUMPLIMIENTO
VULNERABILIDAD	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICACION	CALIFICACION	EVALUACION	MITIGACION DEL RIESGO	
*Fallas eléctricas	Las conexiones no son suficientes, no cumplen con las exigencias el tamaño de la red de equipos de cómputo (cables sueltos, inadecuada estructura y adecuación)	Inadecuada conexión d e cableado eléctrico	Posible pérdida de información	*Riesgo tecnológico *Riesgo físico *Riesgo humano	40	Riesgo moderado	Plantear un nuevo diseño de la red eléctrica	Vigencia 2020
*Afectación de activos de información y activos informáticos.	Desconocimiento de las políticas y normas de seguridad d e la información.	No socialización No capacitación de las políticas y normas d e seguridad.	Acciones no adecuadas en el tratamiento de los activos de información e	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información * Riesgo en personal	60	Riesgo Alto	Diseñar, socializar e implementar un Manual de políticas y normas de seguridad de la información en la Contraloría General de Boyacá.	Vigencia 2020
Incumplimiento de las actividades de seguridad de la información.	El personal encargado de los sistemas no es suficiente. No se están siguiendo protocolos y normas para garantizar la seguridad de la información en la entidad.	No exist e personal encargado del proceso d e aseguramiento de la información	Ausencia de transferencia de conocimiento y falta de capacitación	*Riesgo de información. *Riesgo de servicio. *Riesgo tecnológico	60	Riesgo Alto	Encargar a personal capacitado para el aseguramiento de la información. Capacitar al personal de la Contraloría para el cumplimiento de procesos y actividades de seguridad de la información	Vigencia 2020

Confidencialidad e Integridad de la información	En la entidad se trabaja en la campaña cero papel, sin embargo aún se siguen realizando demasiadas impresiones incluso que se desperdician. Se encuentran impresiones con información personal y/o de la entidad sin protección o una debida salvagurada.	Exposición de datos personales	incumplimiento de confidencialidad e integridad de la información	*riesgo de Información	60	Riesgo Alto	Socializar con los funcionarios de la entidad acerca de las políticas de seguridad y confidencialidad de la información.	Vigencia 2020
Pérdida total de Información	No se cuentan con los tipos de extintores adecuados para cada necesidad.	No se cuentan con los tipos de extintores adecuados para cada necesidad.	*No hay extintores *La planta de energía no funciona	*Riesgo de información. *Riesgo de servicio. *Riesgo tecnológico	60	Riesgo Alto	Adquirir los extintores necesarios. Revisar el funcionamiento y puesta en marcha de la planta de energía	Vigencia 2020
Pérdida de Información	Los funcionarios no realizan copias de seguridad a la información producto de sus funciones. Equipos compartidos en algunas dependencias Uso de memorias extraíbles y unidades extraíbles	No hacen copias de seguridad No hay control de uso	Posible pérdida de información Infección por Virus	*Riesgo de Información *Riesgo en Servicio *Riesgo Tecnológico	40	Riesgo Importante	*Crear un instructivo de copias de seguridad *Capacitar al personal de la Contraloría para el dominio de este tema. *Adquirir un servidor para almacenar las copias de seguridad .	Vigencia 2020

5.1.1. PROPUESTA DE SEGURIDAD

- Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de las oficinas.
- Socializar las políticas de seguridad y privacidad de la información con el personal de la Contraloría.
- Crear un rubro del presupuesto para la adquisición de la licencia del sistema ofimático Office para los equipos de la Contraloría.
- En caso de usar office libre se debe capacitar al personal en el manejo del sistema ofimático.
- Implementar el sistema de documentación digital en la Contraloría para reducir riesgos de pérdida de información física.
- La Contraloría comprometida con la campaña cero papel, debe capacitar a los funcionarios para hacer uso eficiente del SIDCAR – Sistema de Gestión Documental.

5.1.2. PLAN SEGURO PARA EL ACOPIO DE COPIAS DE SEGURIDAD

Adquirir un servidor con características específicas para el almacenamiento de copias de seguridad de la información local manejada en las diferentes dependencias.

- Obtener una nube dedicada para la información de la Contraloría con el fin de tener un respaldo en caso de accidentes en los servidores.
- 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.

5.1.3. PLAN DE CONTINUIDAD DEL NEGOCIO

- Diseñar un formato de chequeo de acuerdo a las necesidades de la organización que permita realizar la auditorías periódicas al con la finalidad de verificar que los objetivos de control, procesos y procedimientos se cumplan.
- Socializar con los directivos, la importancia del Plan de Gestión de Riesgo en Seguridad TIC, para hacer frente a incidentes 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 Contraloría
  3) Procedimientos de gestión de emergencias, por desastre natural, por incendio o por inundaciones

5.1.4. 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.

5.1.5. PLAN DE CAPACITACIÓN

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

1) Detectar los requerimientos tecnológicos
2) Determinar objetivos de capacitación para personal
3) Evaluar los resultados de evaluaciones y monitoreo al sistema de seguridad.
4) Elaborar un programa de capacitación en temas de ciberseguridad y políticas de seguridad de la información para todos los funcionarios de la entidad.
5) Evaluar los resultados de cada actividad.

5.1.6. PLAN DE TRANSICIÓN DE IPV4 A IPV6

Se debe establecer un plan para hacer la transición de las direcciones IPv4 existente actualmente por la IPv6 debido a que los equipos informáticos de la Contraloría General de Boyacá soportan todos, la nueva versión de IP.

Es importante señalar que para este punto en específico se está desarrollando un contrato con la Gobernación de Boyacá a través del cual se recibirá para la Contraloría General de Boyacá un edificio inteligente que contempla dentro de su infraestructura estas actualizaciones tecnológicas.

INFOGRAFÍA

GUÍA DE GESTIÓN DE RIESGOS. MINISTERIO. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. MINISTERIO DE LAS TIC. http://www.mintic.gov.co/gestionti/615/w3- propertyvalue-7275.html