PLAN DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

30 / 01 / 2020
Oficina De Sistemas – Secretaría de Planeación
Alcaldía Municipal de Cota

TABLA DE CONTENIDO

INTRODUCCIÓN

El Municipio de Cota (Cundinamarca) es una Entidad Territorial que hace parte de la Rama Ejecutiva del Poder Público de Colombia, que goza de autonomía de gestión de sus intereses, dentro de los límites de la Constitución y de la ley, hace parte de las entidades públicas que ha apropiado las iniciativas del Gobierno Nacional y las ha desplegado a todos sus niveles organizacionales, incluyéndolas en los objetivos estratégicos de la entidad.

En atención a lo anterior, la entidad asumió el reto de implementar el SGSI, siguiendo los lineamientos del MSPI de la Estrategia de Gobierno en Línea, a su vez reglamentado a través del Decreto 1078 de 2015 para el sector de tecnologías de la información y comunicaciones y el Decreto 2573 de 2014 por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea.

La defensa y protección de los activos de información es una tarea esencial para asegurar la continuidad y el desarrollo de los objetivos institucionales, así como para mantener el cumplimiento normativo y regulatorio aplicable a la entidad, además traslada confianza a las partes interesadas.

Cuanto mayor es el valor de la información, mayores son los riesgos asociados a su pérdida, deterioro, manipulación indebida o malintencionada. Por lo anterior, el SGSI de la alcaldía de Cota adopta una metodología para la evaluación y tratamiento de los riesgos; siendo éste el medio más eficaz de tratar, gestionar y minimizar los riesgos, considerando el impacto que éstos representan para la entidad y sus partes interesadas.

Así mismo, el SGSI que se quiere implementar en la alcaldía de Cota define políticas y procedimientos eficaces y coherentes con la estrategia de la entidad, como desarrollo de los controles adoptados para el tratamiento de los riesgos, los cuales están en continuo seguimiento y medición, a través del establecimiento de indicadores que aseguran la eficacia de los controles; apoyado en los programas de auditoria y la revisión por la dirección, que concluyen en la identificación de oportunidades de mejora las cuales son gestionadas para mantener la mejora continua del SGSI.

Lo anterior se complementa con los programas de formación y transferencia de conocimiento en seguridad de la información y las campañas de sensibilización que se lideran al interior de la entidad.

Así pues, la entidad expone a través de este manual el modelo del SGSI adoptado por la entidad de acuerdo con el ciclo PHVA (planear, hacer, verificar y actuar), con el propósito de cumplir con el marco normativo, la misión fijada y la visión trazada. Dicho manual describe las disposiciones acogidas por la entidad para establecer el contexto, las políticas, los objetivos, el alcance, los procedimientos, las metodologías, los roles, las responsabilidades y las autoridades del SGSI; de acuerdo con los requisitos legales, los contractuales y los normativos, que le aplican a la entidad, en el marco de seguridad de la información.

Para tal fin, la entidad ha adoptado los lineamientos normativos de: la NTC/ISO 27001:2013, la cual establece los requisitos para la implementación del SGSI, la NTC/ISO 31000:2011 que proporciona el esquema para la gestión de riesgos y las mejores prácticas, tales como ISO 27002:2015, ISO 27005:2009, entre otras; buscando mejorar el desempeño y la capacidad para prestar un servicio que responda a las necesidades y expectativas de las partes interesadas.

1 OBJETIVO

Presentar el Plan de Seguridad y Privacidad de la Información, el cual es el documento que dirige la implementación de controles de seguridad según el modelo del Sistema de Gestión de Seguridad de la Información, en adelante SGSI, adoptado por la alcaldía municipal de Cota Cundinamarca; este documento expone las prioridades de implementación de los controles en relación con seguridad de la información enmarcado en el ciclo de mejoramiento continuo PHVA (planear, hacer, verificar y actuar).

2 OBJETIVOS ESPECÍFICOS

1. Comunicar e implementar la estrategia de seguridad de la información.
2. Incrementar el nivel de madurez en la gestión de la seguridad de la información.
3. Implementar y apropiar el Plan de Seguridad y Privacidad de la Información – PSPI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
4. Hacer uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.
5. Asegurar los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.

3 ALCANCE

El Plan de Seguridad y Privacidad de la Información considera los controles de la norma NTC/ISO 27001:2013, el análisis de riesgos realizado, los procesos de la Alcaldía de Cota, y los lineamientos del Modelo de Seguridad y Privacidad de la Información - PSPI de la Estrategia de Gobierno en Línea

4 MARCO LEGAL

NORMA	DESCRIPCIÓN
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

NORMA	DESCRIPCIÓN
NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.
NTC/ISO 27002:2013	Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.

5 CONOCIMIENTO DE LA ENTIDAD

5.1 MISIÓN

El Municipio de Cota, como entidad territorial de la división política y administrativa del Estado, con autonomía política, administrativa y fiscal, dentro de los límites que le señala la Constitución y la Ley, tiene como misión y objetivos generales asegurar el desarrollo social, político, económico, físico y ambiental del municipio, el bienestar general y el mejoramiento continuo de la calidad de vida de su población; mediante el ejercicio a través de la Administración Municipal de las competencias y funciones establecidas en el artículo 311 de la constitución Política, las disposiciones legales en concordancia con los Planes de Desarrollo Nacional, Departamental.

5.2 VISIÓN

Para el 2036, Cota será un municipio ejemplo regional en iniciativas de desarrollo económico, social y ambiental incluyentes y sostenibles, articulando el contexto regional y nacional. Como líder estratégico impulsara la creación de la región agropecuaria, industrial y comercial de la sabana, que desde criterios de desarrollo sostenible y sustentable elevara el nivel de vida y bienestar general de los cotenses.

5.3 ESTRUCTURA ORGÁNICA

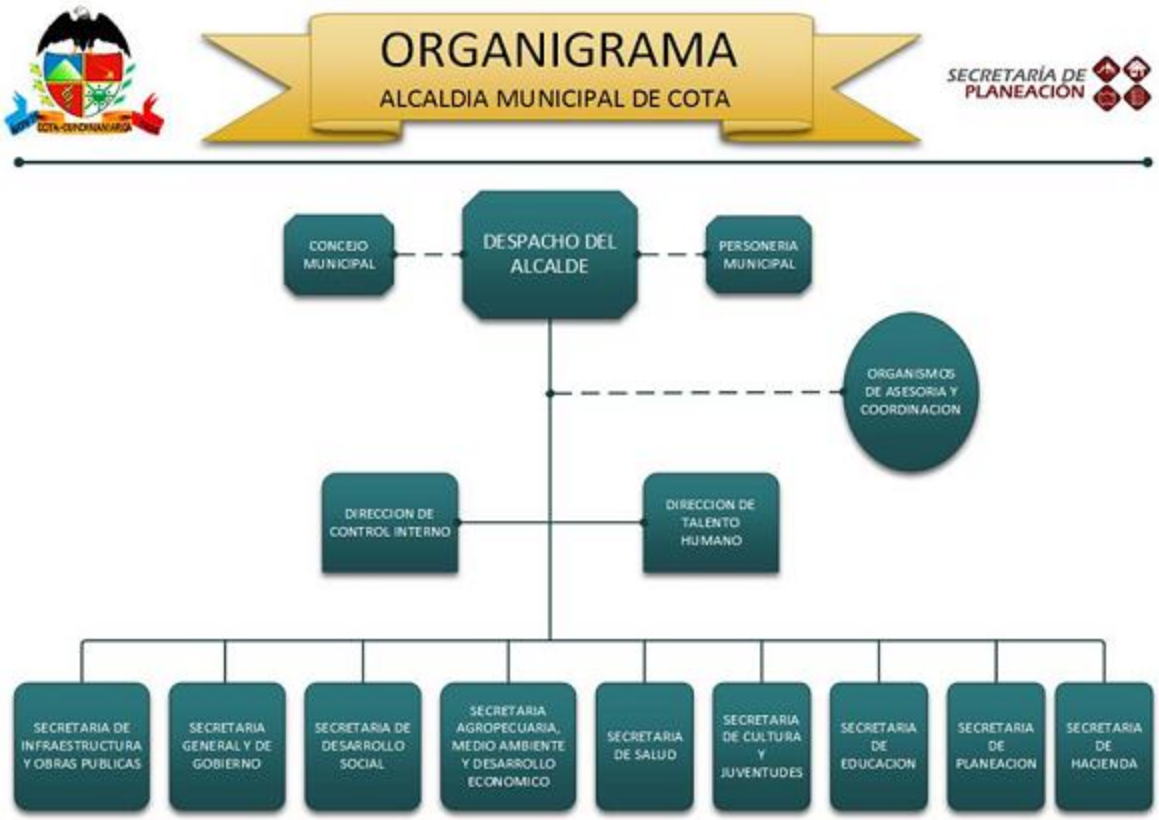


Ilustración 1. Estructura Orgánica Alcaldía de Cota

6 MODELO SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI

6.1 ANTECEDENTES

En la actualidad y de acuerdo con la expedición del Decreto 2573 de 2014 contenida en el Decreto Único Reglamentario 1078 de 2015 del sector de Tecnologías de la información y las Comunicaciones; la alcaldía de Cota trabaja permanentemente en los de implementar el SGSI siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL con el fin de preservar la integridad, confidencialidad, disponibilidad y privacidad de la información mediante la adecuada gestión del riesgo, la aplicación de la normatividad vigente y la implementación de mejores prácticas relacionadas con seguridad de la información.

En efecto, el modelo del SGSI de la Alcaldía de cota se encuentra basado en el ciclo de mejoramiento continuo PHVA (Planear, hacer, actuar y verificar), el cual asegura que el SGSI esté expuesto a revisiones continuas cuando existe un cambio importante en la infraestructura o se requiera mejorar su efectividad dependiendo de las mediciones de parámetros claves de su operación. Se cuenta, entonces, con un ciclo que permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI.

A continuación, se listan los componentes de cada una de estas fases del ciclo:

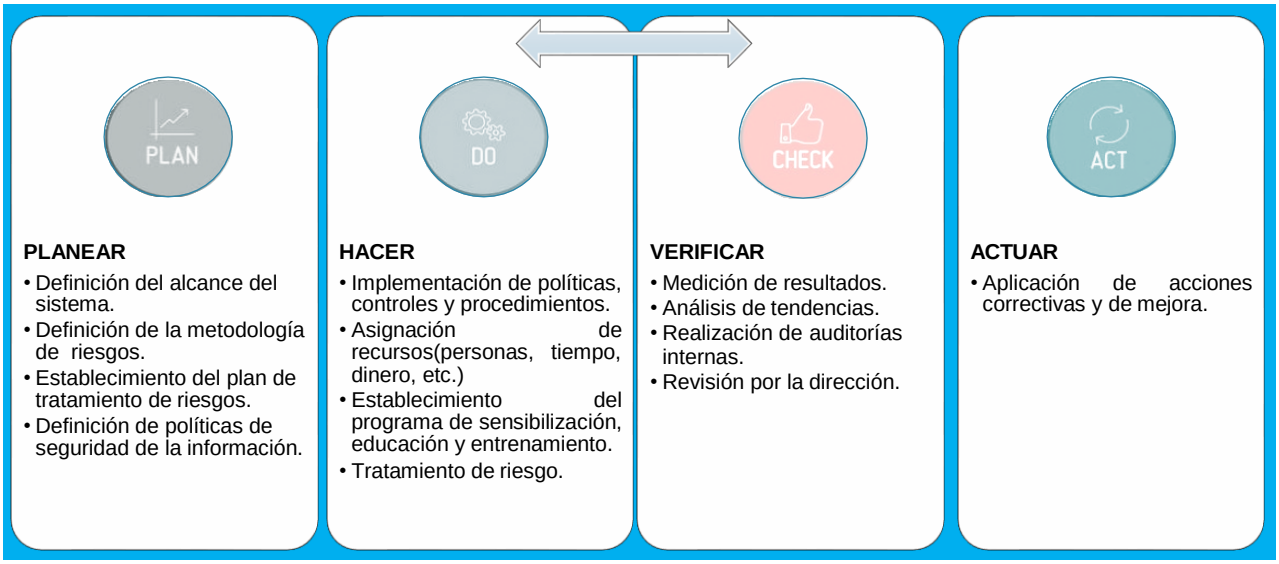


Ilustración 2. Fases del Ciclo PHVA

6.2 ALCANCE DEL SGSI

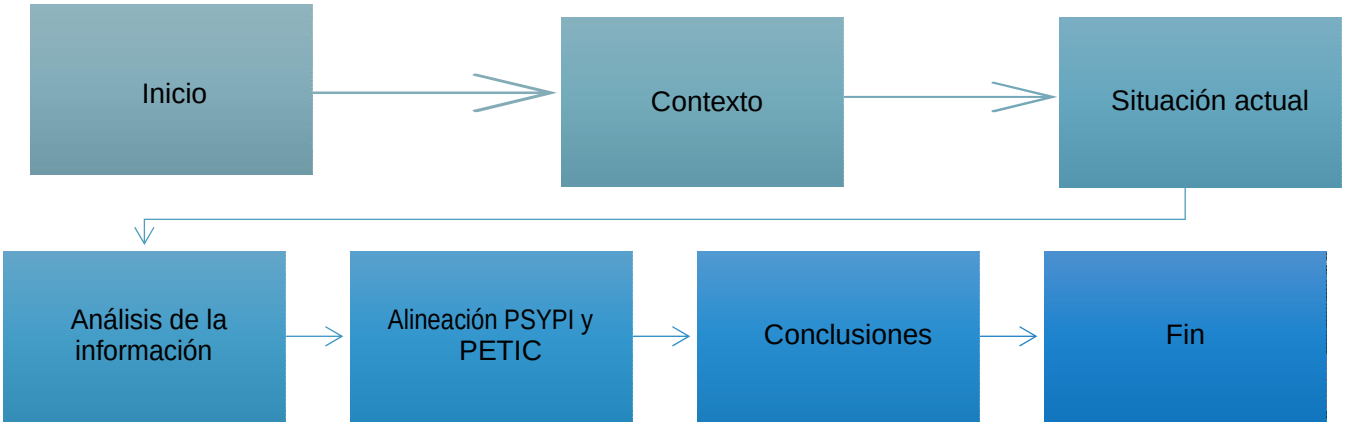
Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Alcaldía de Cota, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad del presente manual. Los usuarios tienen la obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por la Dirección General.

7 MARCO CONCEPTUAL

Para la alcaldía de Cota, son muy importantes los resultados obtenidos en el Plan de Seguridad y Privacidad de la Información con el fin de apoyar la implementación del SGSI. El plan se apoya en el Plan Estratégico Institucional el cual a su vez se fundamenta en los marcos de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información: ITIL, COBIT y las normas ISO 27001, ISO 27002, ISO/IEC 27005, NTC/ISO 17799.

8 METODOLOGÍA UTILIZADA

La metodología utilizada para el desarrollo del Plan de Seguridad y Privacidad de la Información se muestra y se explica a continuación:



8.1 CONTEXTO

En esta fase inicial del desarrollo del Plan de Seguridad y Privacidad de la Información, se busca entender las características principales de la entidad con el fin de que los objetivos de este Plan estén alineados con los objetivos estratégicos de la entidad. Entre los aspectos que se deben considerar para lograr este entendimiento están:

1. La misión
2. La visión
3. Historia y antecedentes
4. Estructura organizacional
5. Procesos
6. Cultura y valores
7. Legislación pertinente

8.2 SITUACIÓN ACTUAL

Por situación actual el nivel de importancia que posee el área de sistemas con relación a la seguridad de la información. se planteó el SGSI de acuerdo con las necesidades de la alcaldía de Cota, Para poder realizar el Plan de Seguridad y Privacidad de la Información es indispensable que se tenga en cuenta la implementación de las políticas desarrolladas en SGSI con el fin de plantear prioridades sobre su implementación.

Dominio ISO 27001	Objetivo de control
Política de clasificación de la información.	Objetivo de control A.5
Política de uso de los activos	Objetivo de control A.6
Gestión de activos.	Objetivo de control A.8
Control de accesos.	Objetivo de control A.9
Criptografía.	Objetivo de control A.10
Seguridad física y ambiental.	Objetivo de control A.11
Seguridad en las comunicaciones.	Objetivo de control A.13
Adquisición de sistemas, desarrollo y mantenimiento.	Objetivo de control A.14
Relación con proveedores.	Objetivo de control A.15
Cumplimiento con requerimientos legales y contractuales.	Objetivo de control A.18

UMERAL	CLAUSULA	ESTADO ACTUAL	BRECHA	ESTADO ESPERADO	NIVEL
A.5	**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN**	60%	40%	100%	*Definido*
A.6	**POLÍTICA DE USO DE LOS ACTIVOS**	62%	38%	100%	*Administrado*
A.8	**GESTIÓN DE ACTIVOS**	63%	37%	100%	*Administrado*
A.9	**CONTROL DE ACCESO**	67%	33%	100%	*Administrado*
A.10	**CRIPTOGRAFÍA**	50%	50%	100%	*Definido*
A.11	**SEGURIDAD FÍSICA**	55%	45%	100%	*Definido*
A.13	**SEGURIDAD DE LAS COMUNICACIONES**	40%	60%	100%	*Repetible*
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**	40%	60%	100%	*Repetible*
A.15	**RELACIONES CON LOS PROVEEDORES**	50%	50%	100%	*Definido*
A.18	**CUMPLIMIENTO**	83%	17%	100%	*Optimizado*
PROMEDIO CLAUSULAS		**58%**			*Definido*

Ilustración 8. Resultados por Dominio

- **Prioridad de Planeación**: Esta variable considera los aspectos relacionados con el dominio desde el punto de vista de las categorías del tipo de control o dominio: administrativo (3), tecnológico (2) y físico (1) y los aspectos referentes a los niveles de planeación: estratégico (3), táctico (2) y operativo (1). Dependiendo de la conjunción de estos dos criterios (nivel de planeación y categorías del tipo del control o dominio) se asigna un valor que ayudará a definir la prioridad de implementación teniendo en cuenta la magnitud de este valor tal como se muestra en la siguiente figura (los valores de mayor a menor son: 9, 6, 4, 3, 2,1).

Categorías				
	Estratégico (3)	**3**	**6**	**9**
	Táctico (2)	**2**	**4**	**6**
	Operativo (1)	**1**	**2**	**3**
		Físico (1)	Tecnológico (2)	Administrativo (3)
		Niveles de planeación		

Tabla 2. Prioridad

- **Documentación política**: El esfuerzo asociado con la documentación de políticas por cada uno de los dominios se mide en esta variable. La cantidad de políticas y normas que hay que desarrollar por dominio es un estimativo que ayuda a estimar su prioridad de implementación.

Los niveles utilizados para calificar esta variable se muestran a continuación:

DOCUMENTACIÓN DE POLÍTICAS		
VALOR	**NIVEL**	**Rango Número de Políticas**
5	MUY ALTO	Entre 10 y 11
4	ALTO	Entre 7 y 9
3	MEDIO	Entre 5 y 6
2	BAJO	Entre 3 y 4
1	MUY BAJO	Entre 1 y 2

Tabla 3. Documentación de políticas

- **Documentación procedimientos:** El esfuerzo requerido por cada dominio en el número de procedimientos requeridos para lograr la preservación de la seguridad de la información es uno de los aspectos considerados con el fin de asignarle una prioridad a la implementación de los diferentes dominios. Los valores estimados de criticidad relacionados con el número de procedimientos estimado requerido se presenta a continuación:

DOCUMENTACIÓN DE PROCEDIMIENTOS		
VALOR	**NIVEL**	**Rango Número de Políticas**
5	MUY ALTO	Entre 8 y 9
4	ALTO	Entre 6 y 7
3	MEDIO	Entre 4 y 5
2	BAJO	Entre 2 y 3
1	MUY BAJO	Igual a 1

Tabla 4. Documentación de procedimientos

- **Documentación estándares:** El esfuerzo requerido por cada dominio en el número de estándares requeridos para lograr la preservación de la seguridad de la información es uno de los aspectos considerados con el fin de asignarle una prioridad a la implementación de los dominios.

Los valores estimados de criticidad relacionados con el número de estándares estimado requerido se presenta a continuación:

DOCUMENTACIÓN DE ESTÁNDARES		
VALOR	**NIVEL**	**CRITERIOS (CANTIDAD)**
5	MUY ALTO	3
4	ALTO	2
3	MEDIO	1
2	BAJO	0
1	MUY BAJO	0

Tabla 5. Documentación de estándares

- **Complejidad**: La variable complejidad considera las calificaciones requeridas en el recurso humano con el fin de acometer la implementación del dominio o control en cuestión, para ello se consideran los siguientes aspectos:

- Especialista
- Ingeniero
- Técnico
- Estudiante técnico o profesional
- Personal no calificado

La tabla utilizada para estimar de manera cualitativa la complejidad asociada a un dominio es la siguiente:

COMPLEJIDAD		
VALOR	**NIVEL**	**CRITERIOS**
5	MUY ALTO	Especialista
4	ALTO	Ingeniero
3	MEDIO	Técnico
2	BAJO	Estudiante técnico o profesional
1	MUY BAJO	Personal no calificado

Tabla 8. Complejidad

- **Tiempo:** La variable tiempo le imprime al dominio unas restricciones importantes en lo referente al tema de cuándo se debe abordar su implementación. Se considera que si un control o dominio toma mucho tiempo para su implementación es recomendable abordarlo posteriormente para que de esta manera podamos implementar muchos más controles que sean de corta duración en su implementación y se aumenta rápidamente el porcentaje de cumplimiento de la norma de seguridad. No obstante, se debe considerar que estos controles de largo tiempo de implementación sean acometidos sin violar los requerimientos de tiempo de todo el proyecto.

La tabla utilizada para estimar de manera cualitativa el tiempo asociado a la implementación de un dominio determinado es la siguiente:

TIEMPO		
VALOR	**NIVEL**	**CRITERIOS**
5	MUY ALTO	Más de un año
4	ALTO	de 9 a 12 meses
3	MEDIO	de 6 a 9 meses
2	BAJO	de 3 a 6 meses
1	MUY BAJO	menos de 3 meses

Tabla 9. Tiempo

Dominio	Prioridad en %	Fase
A.5. Políticas de la seguridad de la información	100,0%	1
A.10. Criptografía	30,0%	1
A.15. Relaciones con los proveedores	10,0%	1
A.16. Gestión de incidentes de seguridad de la información	20,0%	1
A.18. Cumplimiento	26,7%	1
A.6. Organización de la seguridad de la información	2,1%	2
A.7. Seguridad de los recursos humanos	1,1%	2
A.8. Gestión de activos	1,3%	2
A.12. Seguridad de las operaciones	3,0%	2
A.13. Seguridad de las comunicaciones	1,3%	2
A.17. Aspectos de seguridad de la información de la gestión de continuidad de negocio	3,0%	2
A.9. Control de acceso	0,2%	3
A.11. Seguridad física y del entorno	0,0%	3
A.14. Adquisición, desarrollo y mantenimiento de sistemas	0,8%	3

Ilustración 11. Prioridad estratégica por dominio

En la siguiente gráfica se pueden observar los dominios asociados por cada una de las fases consideradas, teniendo en cuenta la prioridad estratégica calculada para los dominios. Los dominios de la Fase I son: A5, A.18, A.16, A.10, A.15, los de la Fase II son: A.17, A.6, A.12, A.8, A.7, A.13 y los de la última fase son: A.14, A.9, A.11.

9 RECOMENDACIONES PARA LA IMPLEMENTACIÓN

9.1 A.5. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

La política determina los objetivos de seguridad, lo que se quiere hacer en temas de seguridad, se basa en los análisis de riesgos y en los resultados de la gestión de incidentes de seguridad. Las políticas siempre responden a la pregunta ¿Qué voy a hacer? y en ese sentido hay que redactar la política. La política define los objetivos a alcanzar y no cómo se va a implementar, es un error incluir en una política algo operativo por ej. *"la contraseña debe tener 8 caracteres alfanuméricos, al menos una mayúscula y números"*, esto no es una política, sino la forma como cumpliría el objetivo, responde a cómo lo voy a hacer y no a ¿qué voy a hacer? una política correcta podría ser algo como "*Todos los usuarios que acceden a los sistemas de información de la alcaldía de Cota deben disponer de un medio de identificación y el acceso debe ser controlado a través de una autenticación personal."*. Lo anterior, lo que se refería a las características de las contraseñas, es lo que se conoce como norma, la cual, no es otra cosa, que, enunciados de obligatorio cumplimiento, que responden a la forma en que se cumplirá una política.

Como se mencionó anteriormente, la política determina los objetivos de seguridad, y la forma de cumplir con estos objetivos en el modelo de seguridad es a través de normas y procedimientos. Las normas y procedimientos siempre deben responder a una política, por lo tanto, en cada norma o procedimiento debe especificarse a qué política responde, si no se puede determinar a qué política corresponde debe razonarse, o que el procedimiento o norma no es necesario, o que el documento de políticas está incompleto. El documento de políticas SIEMPRE debe ser conocido y firmado por la alta gerencia.

Como ayuda para elaborar el documento de políticas de la alcaldía de Cota debe revisar la norma GTC/ISO 27002:2015 y adicionalmente adquirir en la medida de lo posible plantillas para la implementación de políticas que se pueden conseguir en internet.

Las políticas se deben revisar periódicamente, y medir la eficiencia y eficacia con la que se están cumpliendo estos objetivos de seguridad, por lo que la entidad debe implementar un procedimiento del área de seguridad de la información que estandarice el mecanismo por el cual se realizan las revisiones periódicas de los documentos del modelo de seguridad (incluyendo el documento de políticas), de manera que forme parte del modelo de seguridad y sea sujeto de ser auditado.

9.2 A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información realmente es una cultura, en la cual se deben involucrar todos los colaboradores, tanto servidores públicos, usuarios y contratistas para que contribuyan a crear un clima de seguridad tanto al interior como al exterior de la entidad. La organización de seguridad debe estar distribuida por toda la entidad en diferentes funciones con responsabilidades relacionadas con la seguridad de la información.

Se deben utilizar roles para la realización de las actividades que los colaboradores realizan en cada procedimiento, y posteriormente asociar a los cargos, los roles previamente definidos, que contienen las actividades y las funciones de cada rol.

A la hora de realizar esta asignación de roles a cargos se debe:

1. Realizar una matriz RACI[2] para cada procedimiento, de tal forma que puedan ser controladas las actividades por diferentes personas.
2. Realizar una matriz de segregación de funciones entre los roles con el fin de asegurarse que para un cargo no se presenten conflictos de intereses en temas de seguridad de la información.

Dentro del modelo de seguridad, la organización de seguridad debe tener al menos:

- Un **comité de seguridad de la información** en el cual se debe integrar la alta gerencia. Este comité es el órgano máximo del modelo de seguridad. Sus funciones principales, entre otras, podrían ser:
    - Definir los lineamientos y estrategias de Seguridad de la información en función de los objetivos del negocio.
    - Aprobar el modelo de seguridad de la entidad (políticas, normas, procedimientos, etc.).
    - Aprobar el Plan de seguridad y Privacidad de la Información, así como los resultados de su implementación.
- **Líder de seguridad de la Información de la Entidad.** Es el encargado de coordinar todo el modelo de seguridad. Debería estar dedicado tiempo completo a temas de seguridad y debe velar por el mejoramiento continuo del modelo de seguridad. Debe establecer contacto con las autoridades pertinentes, así como con grupos de interés en temas de seguridad.
- **Analista de seguridad de la información.** Son funcionarios dedicados tiempo completo a temas de seguridad de la información y que realizan labores operativas del modelo de seguridad. Son dirigidos por el líder de seguridad de la información. En lo posible, la entidad debe contar como mínimo con dos funcionarios para este rol.

Otros roles sugeridos a futuro dentro de la entidad de seguridad podrían ser:

- Administrador de recursos informáticos
- Administrador de control de acceso lógico
- Operador de seguridad de la información
- Líder de seguridad física
- Líder de recursos humanos
- Líder de organización y métodos o líder del sistema de calidad

---

Auditor de Seguridad

- Asesor legal

Entre otros…

Este dominio también contempla el aseguramiento de dispositivos móviles y el teletrabajo. Con referencia a este tema se sugieren las siguientes recomendaciones:

- Contar con un inventario con el registro de todos los dispositivos móviles de la entidad, en el cual se registre al menos: la persona responsable del dispositivo, los activos de información que maneja el dispositivo y los lugares a los que tiene acceso.
- Contar con estándares de seguridad para dispositivos móviles que pueden contener entre otras, cifrado de disco duro, restricciones de instalación de software, actualización de parches de seguridad, restricción a conexiones de acceso de información, protecciones contra software malicioso, deshabilitar borrado remoto, copias de respaldo, entre otros.
- Contar con un documento formal de normas para uso de dispositivos móviles, donde se den recomendaciones sobre el uso de los dispositivos móviles y los cuidados de seguridad que se deben tener.

9.3 A.7. SEGURIDAD DEL RECURSO HUMANO

Con relación a la seguridad de los recursos humanos se debe tener en cuenta el ciclo de vida del recurso humano, esto es, antes, durante y después de su contratación. En este sentido se darán recomendaciones en estas tres etapas.

Antes de la contratación:

Contar con un procedimiento de selección de personal que, de acuerdo con las leyes y reglamentos de ética pertinentes, incluya:

- Verificación de referencias
- Verificación de la hoja de vida completa
- Verificación de la identidad del aspirante
- Verificación de competencia
- Pruebas psicotécnicas
- Verificar en términos generales que sea una persona confiable.

Durante el periodo de contratación:

- Todos los colaboradores y contratistas que accedan a información reservada o sensible deben firmar un acuerdo de confidencialidad y no divulgación ANTES de tener acceso a dicha información por cualquier medio.
- Todo el personal (sea de planta o contratista) deberán usar los equipos entregados por la administración municipal para su labor diaria.
- Todos los colaboradores deben firmar una cesión de derechos de propiedad intelectual a favor de la entidad sobre los desarrollos que se realicen fruto de su trabajo en la entidad.
- Todos los colaboradores deben seguir fielmente las normas sobre el manejo de cada tipo de información de acuerdo con lo definido en la clasificación de activos de información.
- Contar con un proceso disciplinario sí se incumple cualquiera de las normas de seguridad establecidas.
- Contar con un proceso disciplinario frente a la responsabilidad en incidentes de seguridad de la información en los que se demuestre la participación de algún colaborador.
- Brindar capacitaciones del modelo de seguridad aprobado, así como capacitaciones periódicas en temas de seguridad con el fin de tomar conciencia sobre la seguridad de la

información pertinente a sus roles, y lograr crear una cultura de seguridad al interior y exterior de la entidad.

- Contar con un canal anónimo mediante el cual los colaboradores puedan reportar posibles incidentes de seguridad de la información.

Se debe crear un programa de capacitaciones continuas en seguridad que deberán cubrir como mínimo los siguientes aspectos

- Concientización sobre riesgos de seguridad.
- Conocimiento del modelo de seguridad.
- Conocimiento de las normas y procedimientos de seguridad.
- Puntos de contacto para información de problemas de seguridad.
- Mecanismos para el reporte de incidentes de seguridad de la información.
- Tips prácticos de seguridad orientado a las labores que realiza cada colaborador según sus funciones.

Al terminar la contratación:

- Dentro del procedimiento de terminación de contrato se debe incluir: backup de la información que el colaborador manejaba, eliminación de todos los usuarios y contraseñas del colaborador, eliminación de los accesos remotos de teletrabajo a los que tenía acceso el colaborador.
- El funcionario deberá entregar el equipo con el cual desarrollabas sus funciones.
- El área de seguridad de la información debe dar un visto bueno, o un paz y salvo después de analizar que los activos de información permanezcan en la entidad. Este paz y salvo debe ser requisito para completar el proceso de desvinculación.

9.4 A.8. GESTIÓN DE ACTIVOS

Este dominio pretende identificar los activos de información de la entidad, clasificarlos, asignarles responsables a dichos activos y brindarles un tratamiento apropiado de acuerdo con su clasificación.

Las recomendaciones en este punto son:

- Realizar un inventario de todos los activos de información, para este fin normalmente se realiza una búsqueda de los activos de información en los procesos y procedimientos, buscando el flujo de información en los mismos.
- Incluir en el inventario, el tipo de activo (físico o digital), ubicación, activos de soporte,

redes, medios, servidores o servicios en las que se encuentra, proceso al que pertenece, entre otros.

- Asignar a cada activo de información un dueño. El dueño del activo de información es el responsable del activo de información y velará por salvaguardar dicho activo y hacer cumplir el tratamiento de seguridad de este de acuerdo con su clasificación. Se considera a los activos de información como cualquier otro activo, con un valor financiero y estratégico.
- Realizar una clasificación de los activos de información teniendo en cuenta criterios de disponibilidad, integridad y confidencialidad de dicha información.
- Asignar un tratamiento de seguridad detallado para cada nivel de la clasificación de los activos de información, definiendo normas de uso, etiquetado, y controles de seguridad para cada nivel de clasificación.

Cuando se terminen los vínculos contractuales con la entidad se debe devolver todos los activos de información a los que el colaborador tuvo acceso.

Con respecto a la gestión de medios removibles, se debe:

- Inicialmente bloquear todos los accesos a medios removibles en todos los equipos de la entidad (bloqueo de USB)
- Habilitar los puertos USB, sólo con una justificación escrita y debe ser autorizada por el área de seguridad. Sólo se deberá habilitar el uso de medios removibles, si hay una razón de negocio para hacerlo.

- Se deben redactar normas para el uso de dispositivos removibles
- Se debe tener registro de la información en medios removibles
- Sí la información ya no se requiere tener en dispositivos removibles o cuando el colaborador se retire de la entidad, debe realizarse un borrado seguro del medio removible
- Sí la confidencialidad o integridad de la información contenida en un medio removible se considera importante, debería utilizar mecanismos criptográficos apropiados para cada medio.
- La disposición final para los medios removibles debe realizarse en forma segura, por ejemplo, incineración o borrado seguro.

9.5 A.9. CONTROL DE ACCESO

El objetivo del dominio de control de acceso consiste en limitar el acceso a la información y a las instalaciones con el fin de salvaguardar los activos de información.

- Se debe realizar unas políticas de control de acceso, con sus respectivas normas y procedimientos que las implementen. Las recomendaciones para esta política son:
    - Tener en cuenta para este fin la clasificación de la información, la legislación pertinente de acuerdo con las leyes de protección de datos.
    - Implementar un procedimiento de gestión de derechos de acceso a los diferentes tipos de activos de información en los que se involucre a los dueños de los activos de información.
    - El criterio fundamental a la hora de definir la política de control de acceso debería ser: “Permitir sólo lo que necesita conocer para realizar sus funciones, de lo contrario no se permite”
- Se debe realizar unas políticas de control de acceso a redes y servicios de red, con sus respectivas normas y procedimientos que las implementen. Las recomendaciones al respecto son:
    - El acceso a redes o servicios de red debe justificarse en función de los activos a los que se necesita acceder, en la clasificación de los activos puede encontrar en qué redes o a que servicios se le debe permitir acceso para acceder al activo de información.
    - Se debe incluir procedimientos para monitorear las redes, tráfico y quién tiene acceso de acuerdo con la política, y en caso de accesos no autorizados,

      considerarlos como un incidente de seguridad e iniciar inmediatamente una investigación de seguridad.
- Se debe implementar un procedimiento de gestión de acceso a usuarios. Este procedimiento incluye la creación, modificación y eliminación de usuarios. Generalmente está asociado con el proceso de contratación y desvinculación. El procedimiento debe tener en cuenta la autorización al acceso de activos de información, redes y servicios, y estas autorizaciones deben ser avaladas por el dueño del activo de información y por el área de seguridad de la información como mínimo.
- Se debe revisar periódicamente todos los accesos a los activos de información, redes y servicios. En estas revisiones identificar y eliminar o deshabilitar permisos redundantes y obsoletos de acuerdo con las solicitudes de acceso.
- Se debe tener especial cuidado con usuarios con altos privilegios.

- Se debe habilitar logs de acceso a los sitios restringidos.
- Se debe realizar auditoría periódica a los permisos de acceso
- A nivel de aplicativos, durante su desarrollo, desde la etapa de diseño, se debe tener en cuenta:
    - La posibilidad de restringir el acceso a la información de la aplicación, para esto utilizar roles, permitir auditar el acceso a información sensible y a operaciones sensibles dentro del aplicativo, entre otras.
    - Utilizar técnicas de autenticación adecuadas para corroborar la identidad de un usuario.
    - Durante el log-on se debe proteger de intentos de ingreso por fuerza bruta, evitar mensajes de ayuda en el log-on, utilizar contraseña protegida (que no se vea la contraseña al momento de ingresarla), llevar registro de intentos de log-on (exitosos y fallidos). No transmitir las contraseñas en texto plano.
    - Se debe cerrar las sesiones por inactividad.

9.6 A.10. CRIPTOGRAFÍA

El objetivo de este dominio es asegurar la confidencialidad mediante el uso de métodos apropiados de criptografía**.** Los sistemas centralizados de gestión de llaves garantizan la seguridad de las diferentes llaves utilizadas por los sistemas de cifrado.

Los proyectos recomendados para este dominio son:

9.7 A.11. SEGURIDAD FÍSICA Y DEL ENTORNO

La seguridad física en Colombia es y ha sido un aspecto muy importante de la forma como las empresas protegen sus activos económicos. Se requiere contar con una metodología que permite evaluar qué tan efectivos son los controles existentes en la infraestructura de la Entidad con el fin de actuar como factor disuasivo y control, contra eventos que pongan en peligro la disponibilidad, confidencialidad e integridad de la información.

Es importante considerar que factores como el control de variables ambientales, tecnologías de control de acceso, y sistemas de CCTV, permiten implementar los controles. Estos controles deben ser el resultado del análisis de riesgo, en donde se determinan las prioridades de cada uno de los elementos anteriormente mencionados.

Zonas de mejora o posibles proyectos (mejora de controles de acceso y protección contra amenazas naturales)

1. Centros de Procesamiento normales o de emergencia
2. Áreas con servidores, ya sean de procesamiento o dispositivos de comunicación
3. Áreas donde se encuentren concentrados dispositivos de información
4. Áreas donde se almacenen y guarden elementos de respaldo datos (CD, Discos
5. Duros, Cintas etc.)
6. Áreas donde se deposite salidas de impresoras o fax.

9.8 A.12. SEGURIDAD EN LAS OPERACIONES

El objetivo de este dominio consiste en asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información. Para ello, lo divide en siete grandes subdominios que se tratarán individualmente:

9.8.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

Para este subdominio se debe:

- Tener procedimientos documentados de cada uno de los elementos de procesamiento de información, como servicios, aplicativos, dispositivos de red y de infraestructura. La documentación por cada elemento debería incluir como mínimo:
    - Instalación y configuración de los sistemas
    - Procedimientos de encendido y apagado
    - Procedimientos de respaldo tanto de los datos como de la configuración

- Contar con un procedimiento de gestión de la capacidad. El principio fundamental consiste en monitorear todos los recursos de procesamiento y comunicación, tales como ancho de banda de los canales, memoria, capacidad de almacenamiento, capacidad de cálculo, entre otros, y alertar cuándo lleguen a valores críticos con el fin de gestionar la capacidad de cómputo, bien sea optimizando o adquiriendo más capacidad.
- Contar con separación de ambientes, la norma se refiere a que el ambiente de desarrollo debe ser diferente al ambiente de producción. Cuando se refiere a ambientes, lo ideal

  sería que fuesen ambientes totalmente independientes. En lo posible, se debe procurar cinco ambientes como se describen a continuación:

- **Terceros**: cuando se desarrolla software por terceros y es necesario que tengan acceso a los sistemas de la entidad, es recomendable construir un ambiente independiente para el proveedor que no interfiera con la entidad ni afecte la seguridad de la misma. La información con la que se realiza estos desarrollos debe ser información de prueba, nunca con datos reales.
- **Desarrollo**: El ambiente de desarrollo es un ambiente diseñado para este fin no debe tener acceso directo a los sistemas de producción. Debería brindarle a los desarrolladores una infraestructura lo más similar posible a la que se tiene para producción. La información con la que se realiza estos desarrollos debe ser información de prueba, nunca con datos reales.
- **Pruebas y Calidad de Software**: Es un ambiente destinado para todas las pruebas de software: funcionales, no funcionales y pruebas de seguridad. Debería tener una infraestructura lo más similar posible a la que se tiene para producción. La información con la que se realiza estos desarrollos debe ser información de prueba, nunca con datos reales.
- **Producción**: Es el ambiente productivo, donde se realizan las operaciones reales de la entidad.
- **Contingencia**: Es el ambiente de respaldo que se analiza en detalle en la gestión de continuidad, debe ser lo suficientemente robusto para soportar los servicios mínimos requeridos por la entidad.
-

9.8.2 REGISTRO Y SEGUIMIENTO

El objetivo de este subdominio es dejar rastro de los eventos y evidencia de todas las operaciones relevantes con el fin de que sirvan de apoyo en una investigación de seguridad en un momento dado. Se debe tener en cuenta para estos registros que contengan entre otros la siguiente información:

9.8.2.1 Identificación de usuarios;
9.8.2.2 Actividades del sistema;
9.8.2.3 Fechas, horas y detalles de los eventos clave, por ejemplo, entrada y salida;
9.8.2.4 Identidad del dispositivo o ubicación, si es posible, e identificador del sistema;
9.8.2.5 Registros de intentos de acceso al sistema exitosos y rechazados;
9.8.2.6 Registros de datos exitosos y rechazados y otros intentos de acceso a recursos;
9.8.2.7 Cambios a la configuración del sistema;

9.8.2.8 Uso de privilegios;

9.8.2.9 Uso de utilidades y aplicaciones del sistema;

9.8.2.10 Archivos a los que se tuvo acceso, y el tipo de acceso;

9.8.2.11 Direcciones y protocolos de red;

9.8.2.12 Alarmas accionadas por el sistema de control de acceso;

9.8.2.13 Activación y desactivación de los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusión;

9.8.2.14 Registros de las transacciones ejecutadas por los usuarios en las aplicaciones.

9.9 A.13. SEGURIDAD EN LAS COMUNICACIONES

La transferencia de información está expuesta a múltiples riesgos, por ello la entidad debe implementar medidas preventivas para evitar su divulgación o modificación. Para lograr esto la alcaldía de Cota debe:

Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte y mantener la seguridad de la información transferida dentro de la entidad y con cualquier entidad externa.

9.10 A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

La seguridad en los procesos de desarrollo de software debe estar a lo largo de cada parte del ciclo de desarrollo de software, las recomendaciones por cada parte son:

Análisis de Requerimientos

9.10.1 Definir claramente con el usuario final el alcance de los requerimientos.

9.10.2 Determinar la confidencialidad de la información que se maneja

9.10.3 Definir el control de autenticación requerido

9.10.4 Definir los roles y los privilegios de cada rol

Diseño

9.10.5 Acceso a componentes y administración del sistema

9.10.6 Logs para auditoría

9.10.7 Gestión de sesiones

9.10.8 Datos históricos

9.10.9 Manejo apropiado de errores

9.10.10 Segregación de funciones

9.10.11 Defina adecuadamente la administración de identidades

9.10.11.1 Exija el uso de contraseñas seguras

9.10.11.2 En el caso de que se produzca un error en la autenticación, devuelva la mínima información posible

9.10.12 Compruebe siempre la validez de los datos de entrada

9.10.12.1 Suponga que todos los datos especificados por los usuarios tienen mala intención

9.10.12.2 Compruebe la validez del tipo, longitud e intervalo de los datos

9.10.13 Administración de la configuración y las sesiones

9.10.14 Datos confidenciales y criptografía

9.10.15 Auditoría y registro, siempre dejar registro de las actividades sensibles del aplicativo, (log-in y log-out, Tiempo de sesión, accesos a la base de datos)

9.11 A.15. RELACIONES CON LOS PROVEEDORES

Los proveedores por su naturaleza son una de las fuentes externas de riesgos, pero a su vez son importantes para el cumplimiento de la misión y la visión de la entidad, por esta razón se deben implementar controles para: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores y mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con proveedores.

Las auditorías nos ayudan a determinar el nivel de cumplimiento de los proveedores con respecto a la seguridad de la información:

9.12 A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Construir un proceso consistente para gestionar los incidentes de seguridad de la información, el cual debe contener como mínimo:

9.12.1 Reporte de incidente de seguridad de la información

9.12.2 Investigación de incidente de seguridad de la información

9.12.3 Adecuado control de cadena de custodia para gestión de evidencias.

La adecuada gestión de los incidentes de seguridad de la información permite proteger los tres pilares de la seguridad: la confidencialidad, la integridad y la disponibilidad de la información. La implementación de estos controles permite asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

9.13 A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE

CONTINUIDAD DE NEGOCIO

La continuidad del negocio en lo relacionado a la información es un componente fundamental en la implementación del SGSI. La Gestión de la Continuidad del Negocio (BCM, por sus siglas en inglés Business Continuity Management) debe ser un proceso establecido en nuestra sociedad moderna, globalizada, interconectada, con tecnologías novedosas, más complejas y, además, con una alta presencia de riesgos de tipo operativo que en cualquier momento podrían llegar a materializarse.

Finalmente, el BCP ha sido estandarizado en el año 2012 bajo la norma internacional ISO 22301; norma certificable que ha servido de consulta permanente e indispensable para la realización de este documento y del proceso en general.

Recientemente, se ha concedido una importancia creciente a la implementación de planes, procedimientos y estructuras que garanticen la continuidad de los productos y servicios críticos de una determinada organización ante incidentes de diversas categorías y de diferentes niveles de impacto.

Estos factores, junto con una legislación cada vez más exigente en lo relacionado a la confiabilidad y a la seguridad en la prestación de estos productos y servicios, hacen necesario, en la actualidad, que se cuente con un BCP/DRP con el objetivo de lograr una sociedad cada vez más comprometida con la protección del talento humano, con la disponibilidad de los procesos del negocio, con la protección de la información (ISO 27001:2013), con fortalecimiento y preservación del conocimiento, con la tecnología propicia y segura, al igual, que con el incremento de la productividad, la agilidad, la efectividad y la eficiencia.

En un principio los factores de riesgo estaban asociados principalmente a contingencias de carácter natural y tecnológico, pero las consecuencias derivadas de sucesos como el terrorismo, la inestabilidad política, las pandemias, la pérdida de empleados claves, las amenazas naturales y el CIBERTERRORISMO3, entre otros, han mostrado la necesidad de incorporar nuevas amenazas en el BCP con el fin de garantizar la continuidad de las operaciones ante un escenario cada vez más dinámico en lo relacionado con el tipo de riesgos al que se está expuesto. De acuerdo con la firma Continuity Software de los Estados Unidos, las fallas a nivel de hardware en los diferentes dispositivos que conforman los sistemas de información, por dos años consecutivos, han permanecido en el primer lugar, como causa de activación de los BCP, de acuerdo con el 55% de los encuestados, le siguen migraciones de tecnología con el 51%; en el 2014, el error humano alcanzó un 47% y las fallas a nivel de las aplicaciones un 43%

Proyectos de Planes anexos al BCP

- **Plan de comunicación de crisis**: busca describir los procedimientos y comunicados que las organizaciones deben preparar para responder ante un incidente de manera correcta. Este plan debe estar coordinado con los otros planes de la organización para asegurar que sólo comunicados revisados y aprobados sean divulgados y que solamente el personal autorizado, previamente designado, sea el responsable de responder a las diferentes inquietudes y de diseminar los reportes de estado durante la contingencia a los empleados y al público en general.

- **Planes de evacuación por edificio**: estos planes contienen los procedimientos que deben seguir los ocupantes de una instalación o facilidad en el evento en que una situación se convierta en una amenaza potencial a la salud y a la seguridad del personal, al ambiente o a la propiedad. Tales eventos podrían incluir fuego, terremoto, huracán, ataque criminal o una emergencia médica, entre otros. Estos planes son normalmente desarrollados a nivel de instalación, específicos a la localización geográfica y al diseño estructural de la construcción.
- **Plan de respuesta a CIBERINCIDENTES**: este plan establece los procedimientos para responder a los ataques en el ciberespacio contra los sistemas de información de una organización. Son diseñados para permitirle al personal de seguridad identificar, mitigar y recuperarse de incidentes de cómputo maliciosos tales como: acceso no autorizado a un sistema o información, negación del servicio, cambios no autorizados al hardware y al software, entre otros. Ejemplos de elementos que pueden generar estos incidentes de seguridad pueden ser: la lógica maliciosa, los virus, los gusanos, los troyanos, por mencionar algunos. Estos planes normalmente pueden pertenecer o estar integrados al Sistema de Gestión de la Seguridad de la Información (SGSI), normalmente estipulados y estandarizados bajo la norma ISO 27001:2013.
- **Plan de recuperación de desastres**: este plan es conocido como DRP (Disaster Recovery Plan), y está orientado a responder a incidentes, usualmente catastróficos, que puedan afectar la prestación de los servicios de información. Frecuentemente, el DRP se refiere a un plan enfocado en TI, diseñado para restaurar la operatividad de los sistemas, aplicaciones y bases de datos. Por otra parte, como parte del DRP, se cuenta generalmente con un sitio alterno en donde

se realizarán las operaciones, definidas por el BIA, que fueron interrumpidas por el incidente o desastre en el sitio principal. El alcance de un DRP puede confundirse con el de un Plan de Contingencia de TI; sin embargo, el DRP es menos amplio en alcance y no cubre interrupciones menores que no requieran reubicación.

- **Planes de contingencia**: Según el NIST (National Institute of Standards and Technologies), los planes de contingencia representan un amplio espectro de actividades enfocadas a sostener y a recuperar los servicios críticos de TI, después de una interrupción, en el menor tiempo posible. Es factible en algunos casos contar con múltiples planes de contingencia, uno por cada componente, sistema o servicio crítico. Los planes de contingencia son de rápida activación y se puede asumir un RTO (Recovery Time Objective: Tiempo Objetivo de Recuperación), muy cercano a cero. Los planes de contingencia son típicos en los canales de comunicaciones y servidores, de tal manera que, ante la falla de uno de estos canales o servidor, otro, entrará en operación muy rápidamente y, en muchos casos, de manera automatizada

9.14 A.18. CUMPLIMIENTO

Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad es importante para no incurrir en demandas, multas u otra clase de afectación a la imagen o a las finanzas de la entidad.

Definir procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados, en el marco de la Ley 719 de 2001.

Establecer una política de privacidad y protección de la información de datos personales, en el marco de la Ley 1581 de 2012 y mantener una capacitación continua sobre estas leyes con expertos en el tema.

Adicionalmente, como parte del ciclo de mejoramiento continuo del SGSI, la entidad debe garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos organizacionales.

11 DEFINICIONES

- **Activo**: En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Contratistas**: Entenderemos por contratista aquella persona natural o jurídica que ha celebrado un contrato de prestación de servicios o productos con una entidad.
- **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Guía**: documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Norma**: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.
- **Parte interesada**: (Stakeholder) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Política del SGSI:** Manifestación expresa de apoyo y compromiso de la alta dirección con respecto a la seguridad de la información.
- **Política**: Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.
- **Privacidad de datos:** La privacidad de datos, también llamada protección de datos, es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una

organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros

- **Procedimiento**: Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Rol:** Papel, función que alguien o algo desempeña.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

12 REFERENCIAS

Salas, F. C. (06 de 2011). *Programa Gobierno en Línea*. Obtenido de http://programa.gobiernoenlinea.gov.co/apc-aa-files/5854534aee4eee4102f0bd5ca294791f/Documento_de_evoluci_n_de_la_pol_tica_GEL_20110630.pdf