**PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE TI**

[1. INTRODUCCIÓN 3](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365586)

[2. OBJETIVOS 3](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365587)

[2.1 Objetivo General 3](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365588)

[2.2 Objetivos Específicos. 3](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365589)

[3. ALCANCE 4](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365590)

[4. MARCO LEGAL 4](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365591)

[5. NORMAS TÉCNICAS 5](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365592)

[6. DEFINICIONES 5](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365593)

[7. ESTRUCTURA DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE TI 9](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365594)

[7.1 Elaborar y/o actualizar Política de Seguridad y Privacidad de la Información. 9](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365595)

[7.2 Actualizar el Inventario de Activos de Información 9](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365596)

[7.4 Declaración de Aplicabilidad 10](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365597)

[7.5 Categorización de los Servicios de TI 10](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365598)

[7.6 Definición de Estrategias de Continuidad de TI 10](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365599)

[7.7 Desarrollo de las estrategias de Continuidad de TI 10](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365600)

[7.8 Plan de Capacitación, Comunicaciones y Sensibilización de Seguridad y Privacidad de la Información. 10](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365601)

[7.9 Plan de Transición de IPv4 a IPv6. 11](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365602)

[7.10 Indicadores de Gestión para la Seguridad de la Información 11](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365603)

[8. CRONOGRAMA DE ACTIVIDADES 11](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365604)

[9. EVALUACIÓN Y SEGUIMIENTO 13](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365605)

[**ANEXOS 14**](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365606)

[DESCRIPCIÓN GENERAL DEL PLAN DE CAPACITACIÓN, SENSIBILIZACION Y COMUNICACIÓN 14](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365607)

[DISEÑO DEL PLAN DE CAPACITACIÓN, SENSIBILIZACION Y COMUNICACIÓN. 15](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365608)

[Materiales para el plan de capacitación, sensibilización y comunicación. 16](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365609)

[Instrumentos de sensibilización 16](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365610)

[ACCIONES PARA LA COMUNICACIÓN Y SENSIBILIZACIÓN. 17](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365611)

[ACCIONES PARA LAS CAPACITACIONES. 17](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365612)

[LOGROS ESPERADOS. 17](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365613)

[INSTRUMENTOS DE MEDICIÓN 17](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365614)

[CRONOGRAMA DE ACTIVIDADES 18](file:///C:\Users\fredyalayon\Documents\SGI\Documentación\A-OT-030Plan%20de%20%20Seguridad%20y%20ContinuidadTI%20%20vf.docx#_Toc515365615)

# INTRODUCCIÓN

La estrategia de Gobierno en Línea - GEL, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente[[1]](#footnote-1).

En el Plan Nacional de Desarrollo 2015-2018 se reconoce la seguridad y privacidad de la información, como un factor fundamental para la apropiación de las TIC; así mismo plantea un marco de seguridad necesario, que permita garantizar la prestación de servicios a los ciudadanos a través de las TIC, y que debe estar respaldado por unos planes, políticas y procedimientos orientados a preservar y minimizar el impacto a los activos de información de la entidad por eventos como fallas de seguridad, perdida del servicio y disponibilidad del servicio.[[2]](#footnote-2).

El Plan de Seguridad y Privacidad de la Información y Continuidad de TI para estar acorde con las buenas prácticas de seguridad y continuidad deberá ser actualizado periódicamente; así mismo recoger los cambios técnicos de la norma, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

La seguridad de la información garantiza que los responsables de la información sean capaces de gestionar la información de forma segura, independientemente del formato o soporte en el que se encuentra. Mediante el proceso de Gestión de TI y el modelo de seguridad y privacidad de la información y de continuidad de TI, se trabajará en el fortalecimiento de la seguridad de la información en APC-Colombia, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación colombiana.

# OBJETIVOS

* 1. Objetivo General

Definir en el Plan de Seguridad y Privacidad de la Información y Continuidad de TI, los lineamientos que respondan asertiva y oportunamente a eventos que afecten la seguridad de la información, así como gestionar la continuidad de los procesos soportados por TI.

* 1. Objetivos Específicos.
* Continuar con la implementación del Modelo de Seguridad y Privacidad de la Información, con el fin de dar cumplimiento al componente de Seguridad y Privacidad de la Información y gestionar la seguridad de la información al interior de APC-Colombia.
* Identificar las aplicaciones y las plataformas consideradas críticas para la operación de APC –Colombia entorno a los servicios de TI.
* Establecer los tiempos mínimos de recuperación de servicios de TI requeridos en los que no se vea afectado la operación de la Entidad.

1. ALCANCE

La estructura del Plan se basa en la metodología propuesta por MINTIC para el componente de Seguridad y Privacidad de la Información, así como la continuidad de TI.

El presente plan, aplican a todos los procesos soportados por el proceso de Gestión de TI de APC Colombia.

1. MARCO LEGAL

La normatividad que sustenta el Plan de Seguridad y Privacidad de la Información y Continuidad de TI es el siguiente:

* Constitución Política de Colombia.
* Ley 489 de 1998. (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=186)
* Ley Estatutaria 1266 de 2008 ““Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales”

(http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488).

* Ley 1273 de 2009, "Protección de la Información y de los datos”, http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492.
* Ley 1581 de 2012, "Protección de Datos personales". (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981)
* Ley 1712 de 2014, “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional” http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882)
* Decreto 943 de 2014, (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=59048 ).
* Decreto 103 de 2015 “ Por la cual se reglamenta parcialmente la Ley 1712 de 2014 y dictan otras disposiciones” (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60556).
* Decreto Único Reglamentario 1078 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las comunicaciones” (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=62513)
* A-OT-011 Política de Seguridad de la Información (http://192.168.1.231/sig/index.php?sesion=$sesion&op=2&sop=2.4.2&cod=A-OT-011&version=4)

1. NORMAS TÉCNICAS

* ISO/IEC 27001- Seguridad de la Información.
* ISO/IEC 27031- Guía para la preparación de las Tecnologías de Información y Comunicaciones para la continuidad del Negocio
* ISO 22301- Gestión de la Continuidad de Negocio
* ISO 31000 – Gestión de Riesgos

1. DEFINICIONES

* **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
* **Activo:** En relación con 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).
* **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
* **Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
* **Análisis del impacto al negocio (BIA por sus siglas en inglés).** Proceso del análisis de actividades las funciones operacionales y el efecto que una interrupción del negocio podría tener sobre ellas.
* **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
* **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).
* **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.
* **Confidencialidad**: La propiedad que esa información esté disponible y no sea divulgada a personas o procesos no autorizados.
* **Datos Personales**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
* **Datos Personales Públicos**: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
* **Datos Personales Privados**: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
* **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
* **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)
* **Declaración de aplicabilidad**: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
* **Derecho a la Intimidad**: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
* **Disponibilidad:** La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.
* **Encargado del Tratamiento de Datos**: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)
* **Gestión de incidentes de seguridad de la información**: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
* **Información Pública Clasificada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
* **Información Pública Reservada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
* **Información Pública**: Es aquella información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
* **Integridad**: La propiedad de salvaguardar la exactitud e integridad de los activos de información.
* **Interrupción:** Incidente, bien sea anticipado (ej. huracanes) o no anticipados (ej. Fallas de potencia, terremotos, o ataques a la infraestructura o sistemas de tecnología y telecomunicaciones) los cuales pueden afectar el normal curso de las operaciones en alguna de las ubicaciones de la organización.
* **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.
* **Ley de Transparencia y Acceso a la Información Pública**: Se refiere a la Ley Estatutaria 1712 de 2014.
* **Mecanismos de protección de datos personales**: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, cifrado etc.
* **Plan de Continuidad del Negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
* **Plan de tratamiento de riesgos** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
* **Punto objetivo de recuperación (RPO).** Punto en el tiempo en el cual los datos deben ser recuperados después de que una interrupción ocurra.
* **Punto Tiempo objetivo de tiempo de recuperación (RTO).** Periodo de tiempo en el cual los mínimos niveles de productos y/o servicios y los sistemas, aplicaciones, o funciones que los soportan deben ser recuperados después de que una interrupción ocurra.
* **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
* **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).
* **Seguridad de la información:** Son todos los controles técnicos y metodológicos que permiten mitigar los riesgos a los que se expone la información.
* **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).
* **Tecnología de la Información**: (TI) Es el estudio, diseño, desarrollo, implementación, soporte y administración de los sistemas de información basados en computadoras, particularmente aplicaciones de software y hardware de computadoras".
* **Trazabilidad**: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).
* **Vulnerabilidad**: Son la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño.

1. ESTRUCTURA DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y CONTINUIDAD DE TI

APC- Colombia ha estructurado el Plan de Seguridad y Privacidad de la Información y Continuidad de TI en concordancia con los marcos legal y conceptual presentados anteriormente, que permita cumplir con el objetivo definido en dicho plan, para esto se definen las actividades que se describen a continuación:

del estado relacionadas con las Seguridad de la Información y garantizará la Confidencialidad, Integridad y Disponibilidad de la Información.[[3]](#footnote-3)

* 1. Elaborar y/o actualizar Política de Seguridad y Privacidad de la Información.

La Política de Seguridad y Privacidad de la información está articulado con la Política de Gestión que incluye la voluntad de la Alta Dirección de APC-Colombia para apoyar la Seguridad y Privacidad de la Información. La política debe estar alineada a las necesidades identificadas en la fase de diagnóstico y debe contener los controles precisos que garanticen el adecuado uso de los activos de información al interior de APC-Colombia.

La actualización de la política debe realizarse al menos una vez al año o cuando se evidencie que nuevas amenazas pueden afectar la Seguridad de la Información en APC-Colombia, todos los cambios que surtan en la política debe ser aprobado y divulgado al interior de la entidad.

Para desarrollar estas actividades, la Guía No 2 – Política General MSPI v1, brinda información relacionada para tal fin. <http://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf>.

* 1. Actualizar el Inventario de Activos de Información

Realizar la actualización de los Inventario de los activos de información por parte de cada proceso, siendo el proceso de Gestión de TI quien recopila la información generando un solo documento con todos los activos de la entidad, con el fin de definir la criticidad, sus propietarios, custodios y usuarios.

La Guía No 5 - Gestión Clasificación de Activos, brinda información relacionada para poder llevar a cabo la realización de las actividades mencionadas previamente. <http://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf>

* 1. Declaración de Aplicabilidad

Una vez aprobado los documentos relacionados con los riesgos de seguridad se debe elaborar el documento de la declaración de aplicabilidad que enmarca los controles aplicables para la seguridad de la información, se deben indicar si los objetivos de control y los controles aplican a APC-Colombia y se debe justificar cada uno de los controles así mismo como aquellos que han sido excluidos. La declaración de aplicabilidad será revisada ante cambios significativos de los elementos de la plataforma tecnológica y/o de personal. Esta información, será material de revisión y aprobación.

* 1. Categorización de los Servicios de TI

Categorizar los servicios apoyados por TI, para definir el nivel con el cual cada actividad soportada por TI, es crítica para APC-Colombia y necesita contar con un plan para su reanudación, estas actividades deberán contar con un tiempo objetivo de recuperación (RTO) y un punto objetivo de recuperación (RPO) para el objetivo mínimo de continuidad de TI por producto o servicio.

* 1. Definición de Estrategias de Continuidad de TI

La aproximación para implementar la resiliencia requerida, de tal manera que los principios de prevención de incidentes, detección, respuesta, recuperación y restauración de los productos y servicios soportados por TI se pongan en marcha en APC-Colombia, éstas deberán ser aprobadas por la alta dirección y sensibilizadas al interior de APC-Colombia.

* 1. Desarrollo de las estrategias de Continuidad de TI

En esta fase se debe desarrollar las estrategias definidas en el anterior punto y documentar el plan de recuperación como respuesta a un incidente o evento de TI que genere interrupción de los servicios soportados por TI.

* 1. Plan de Capacitación, Comunicaciones y Sensibilización de Seguridad y Privacidad de la Información.

La Entidad debe definir un Plan de comunicación, sensibilización que incluya la estrategia para que la seguridad de la información se convierta en cultura institucional, al generar competencias y hábitos en toda APC-Colombia, para estructurar dicho plan se toma como base la Guía No 14 – Plan de Comunicación, Sensibilización y Capacitación[[4]](#footnote-4). Dicho plan se encontrará anexo al presente documento.

* 1. Plan de Transición de IPv4 a IPv6.

Para cumplir con los objetivos de innovación tecnológica que exige el país, las entidades del país deben entrar en el proceso de transición del protocolo IPv4 hacia el nuevo protocolo IPv6.

Para llevar a cabo esta actividad, se toma como base la Guía No 20 - Transición de IPv4 a IPv6[[5]](#footnote-5). (http://www.mintic.gov.co/gestionti/615/articles-5482\_Guia23\_Transicion\_IPV4\_IPV6.pdf)

* 1. Indicadores de Gestión para la Seguridad de la Información

Crear o actualizar los indicadores de gestión orientados a la medición de la efectividad, eficiencia y eficacia en el modelo de operación del marco de seguridad y privacidad de la información.

1. CRONOGRAMA DE ACTIVIDADES

Las fechas de las actividades descritas a continuación, se encuentran definidas en el Plan de Trabajo de Seguridad y Privacidad de la Información.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **COMPONENTE SEGURIDAD Y PRIACIDAD DE LA INFORMACIÓN** | **OBJETIVO** | **Documentos** | **Estado** | **Tareas** | **Fecha de Inicio** | **Fecha de Finalización** |
| **DEFINICIÓN DEL MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y DE LOS SISTEMAS DE INFORMACIÓN** | **Busca definir el estado actual del nivel de seguridad y privacidad y define las acciones a implementar** | | | | | | |
| Plan de Seguridad y privacidad de la Información | Busca generar un plan de seguridad y privacidad alineado con el propósito misional. | Plan de integración del MSPI y Sistema de Gestión Documental | No hay documento | a. Coordinar con el Proceso de Gestión Administrativa la integración del MSPI con la Gestión Documental b.Elaborar el Plan de Integración (Gestión de TI) | 2/04/2018 | 1/08/2018 |
| Informe de Análisis de Riesgos, | En construcción | a. Coordinar con Control Interno y planeación la revisión del Informe de Análisis de Riesgo. b. Solicitar la Aprobación del documento por la Alta Dirección (Gestión de TI) | 16/05/2018 | 1/08/2018 |
| Declaración de Aplicabilidad | En revisión | a. Coordinar con Control Interno, Planeación, Administrativa, Contractual, Talento Humano, Jurídica la revisión de la Declaración de Aplicabilidad. b. Solicitar la Aprobación del documento por la Alta Dirección (Gestión de TI) | 16/05/2018 | 1/08/2018 |
| Plan de comunicación, sensibilización y capacitación (Anexo al plan de Seguridad y Privacidad | En Aprobación | a. Desarrollar las actividades relacionadas en el Anexo del presente documento | 16/05/2018 | 31/12/2018 |
| **IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y DE LOS SISTEMAS DE INFORMACIÓN** | **Busca desarrollar las acciones definidas en el plan de seguridad y privacidad.** | | | | | | |
| Gestión de Riesgos de Seguridad y Privacidad de la Información | Busca proteger los derechos de los usuarios de la entidad y mejorar los niveles de confianza en los mismos a través de la identificación, valoración, tratamiento y mitigación de los riesgos de los sistemas de información. | Documento con la estrategia de planificación y control operacional | En revisión | 1. Elaborar la estrategia de planificación y control Operacional 2. Solicitar la Aprobación del documento por la Alta Dirección (Gestión de TI) | 2/04/2018 | 1/08/2018 |
| Informe de la ejecución del plan de tratamiento de riesgos | En construcción | 1. Realizar informes trimestrales de la ejecución del Plan luego de aprobado el Plan de Tratamiento de Riesgos. | 2/05/2018 | 1/08/2018 |
| Indicadores de gestión del MSPI | En revisión | 1. Elaborar los Indicadores de Gestión. 2. Solicitar la Aprobación de los Indicadores por la Alta Dirección (Gestión de TI) | 2/04/2018 | 1/08/2018 |
| Plan de Control Operacional | En revisión | 1. Elaborar el Plan de Control Operacional 2. Solicitar la Aprobación del documento por la Alta Dirección (Gestión de TI) | 2/04/2018 | 1/08/2018 |
| **MONITOREO Y MEJORAMIENTO CONTINUO** | **Busca desarrollar actividades para la evaluación y mejora de los niveles de seguridad y privacidad de la información y los sistemas de información** | | | | | | | |
| Evaluación del Desempeño | Busca hacer las mediciones necesarias para calificar la operación y efectividad de Ios controles, estableciendo niveles de cumplimiento y de protección de los principios de seguridad y privacidad de la información. | Plan de seguimiento, evaluación, análisis y resultados del MSPI, | No hay documento | 1. Elaborar el Plan de seguimiento, evaluación, análisis y resultados MSPI | Realizar a partir del segundo semestre |  |
| Plan de Auditorías Internas y resultados, de acuerdo a lo establecido en el plan de auditorías | No hay documento | 1. Ejecutar el Plan de Auditorias establecido por Control Interno   (Control Interno) | Realizar a partir del segundo semestre |  |
| Resultados de la auditoría interna al MSPI, de acuerdo a lo establecido en el plan de auditoría | No hay documento | 1. Generar los resultados de la auditoría interna conforme a lo establecido en el plan de auditoría.   (Control Interno ) | Realizar a partir del segundo semestre |  |
| Documento con el plan de mejoramiento | No hay documento | 1. Generar el Plan de Mejoramiento conforme a los resultados de la auditoría.   (Proceso de TI) | Realizar a partir del segundo semestre |  |
| Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías | No hay documento | 1. Elaborar el documento consolidado con las auditorías realizadas de acuerdo al plan de auditorías. | Realizar a partir del segundo semestre |  |

1. EVALUACIÓN Y SEGUIMIENTO

Una vez implementadas las anteriores actividades, el Plan de Seguridad y Privacidad de la Información y Continuidad de TI, se debe evaluar anualmente durante el primer trimestre de la vigencia para medir la efectividad de las acciones tomadas a través de los indicadores definidos anteriormente, que permitan evaluar la interacción entre el modelo de seguridad y privacidad de la información y la aplicación de la Ley de Transparencia y Acceso a la Información Pública.

**ANEXOS**

DESCRIPCIÓN GENERAL DEL PLAN DE CAPACITACIÓN, SENSIBILIZACION Y COMUNICACIÓN

APC- Colombia ha estructurado el plan de Sensibilización de Seguridad y Privacidad de la Información que busca que todos los funcionarios y colaboradores cumplan con la Política de Seguridad y privacidad de la Información mediante actividades, capacitaciones, talleres y socializaciones.

El plan será diseñado e implementado para seguir los requerimientos exigidos por Gobierno en Línea.

DISEÑO DEL PLAN DE CAPACITACIÓN, SENSIBILIZACION Y COMUNICACIÓN.

Para el diseño del plan se detallan los medios y herramientas de comunicación que se tendrán en cuenta para la ejecución del plan:

|  |  |
| --- | --- |
| **No** | **Medios y Herramientas** |
| 1 | Folletos |
| 2 | Correo Masivo |
| 3 | Protector de Pantalla |
| 4 | Publicaciones en Intranet |
| 5 | Charlas con los temas correspondientes a la seguridad de la información |
| 6 | Audiovisuales (Videos) |

Todos los funcionarios deben ver la información entregada de sensibilización como una responsabilidad compartida, en la actual vigencia algunos temas serán los siguientes:

* Administración de Contraseñas.
* Política de Seguridad de la Información
* Seguridad de la Información en el puesto de Trabajo
* Seguridad para los dispositivos USB
* Medidas de seguridad para la información clasificada y reservada
* Gestión de Incidentes (como reportar, que puedo reportar)
* Amenazas y Vulnerabilidades Comunes.
* Talleres prácticos para desarrollar habilidades en la Seguridad de la Información.

Las fuentes de información puedes ser de conferencias de seguridad, boletines de CSIRT-PONAL, organizaciones relacionada con seguridad de la información, todos estos temas serán presentados a través de los medios descritos anteriormente.

## Materiales para el plan de capacitación, sensibilización y comunicación.

* Infraestructura: Las actividades de capacitación y socialización se desarrollarán en las instalaciones de APC-Colombia y en el auditorio del primer piso del Edificio Trade Center.
* Equipo y otros: conformado por los equipos multimedia, video beam, etc.
* Documento Técnico – Educativo: entre ellos tenemos encuestas de evaluación, listas de asistencias, material de estudio, etc.

## Instrumentos de sensibilización

Con el apoyo de comunicaciones internas se requiere diseñar una estrategia de comunicación para sensibilizar a APC-Colombia en temas de seguridad de la información y dar cumplimiento a la estrategia de Gobierno en Línea, para lograr este fin se requiere de las siguientes actividades

* Identificar con una imagen y nombre que represente los temas de seguridad y privacidad de la información.
* Captar la atención de los funcionarios y colaboradores de APC-Colombia para que participen con las actividades de seguridad y privacidad de la información.
* Entrega de folletos para los casos que se requieran.
* Boletines informativos con temas de seguridad en la intranet.
* Socializar los videos de seguridad de la información disponibles en la página de enticconfio.gov.co.

ACCIONES PARA LA COMUNICACIÓN Y SENSIBILIZACIÓN.

* 1. Temario: Política de Seguridad y Privacidad de la Información
  2. Responsables: Gestión de TI
  3. Metodología a utilizar: Correos masivos, charlas

ACCIONES PARA LAS CAPACITACIONES.

* 1. Capacitación preventiva: orientada a preparar a los funcionarios y colaboradores para enfrentar las nuevas amenazas informáticas.
  2. Capacitación correctiva: orientada a solucionar problemas identificados mediante los incidentes de seguridad.

Las capacitaciones anteriores se realizarán a través de exposiciones con enfoque teórico- práctico.

LOGROS ESPERADOS.

* Comprometer a todos los funcionarios y colaboradores con la seguridad de la información.

INSTRUMENTOS DE MEDICIÓN

Para medir la percepción de la Seguridad y Privacidad de la Información, se diseñarán encuestas que se aplicarán por lo menos dos veces al año con el fin de determinar que se debe mejorar en el plan.

CRONOGRAMA DE ACTIVIDADES

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No.** | **Actividad** | **Objetivos** | **Medios** | **Fecha de Ejecución** | **Frecuencia** |
| 1 | Diseñar la estrategia para la campaña de sensibilización y comunicación con el apoyo de comunicaciones internas | Generar una campaña efectiva en donde los funcionarios participen activamente | Definido por comunicaciones internas | Segundo semestre 2018 |  |
| 2 | Socialización Política de Seguridad de la Información, | Lograr que todos en APC-Colombia conozca sus responsabilidades de seguridad de la información | Correo, Intranet | Segundo semestre 2018 | 1 vez al año o cuando se requiera |
| 3 | Talleres Teórico- Práctico para desarrollar habilidades en seguridad de la información | Generar una cultura preventiva ante posibles perdida de información | Charlas | Segundo semestre 2018 | De acuerdo al PIC |
| 4 | Boletines informativos | Informar acerca de las últimas amenazas informáticas y la forma de contrarrestar | Correo, intranet | Primer- Segundo semestre 2018 | Mensual |
| 5 | Encuestas de Seguridad de la Información | Conocer el grado de conocimiento adquirido de acuerdo a las actividades realizadas en seguridad de la información | Correo Masivo (Formulario de Google) | Segundo semestre 2018 | Mínimo una vez al año |

CONTROL DE CAMBIOS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VERSIÓN** | **CÓDIGO** | **NOMBRE DEL DOCUMENTO** | **ACTO** | **CONTROL DE CAMBIOS** |
| 1 | A-OT-030 | Plan de Seguridad y Continuidad de TI | Brújula, septiembre 28 de 2016 | Nuevo |
| 2 | A-OT-030 | Plan de Seguridad y Continuidad de TI | Brújula, marzo 14 de 2017 | Se ajusta a la nueva imagen institucional. |
| 3 | A-OT-030 | Plan de Seguridad y Continuidad de TI | Brújula, agosto 02 de 2017 | Se hace referencia a la Política, Lineamientos y Metodología de Identificación y Administración del Riesgo en el numeral 7.5  Se actualiza la estructura del plan de acuerdo a las guías de MINTIC  Se actualiza el cronograma de actividades. |
| 4 | A-OT-030 | Plan de Seguridad y Privacidad de la Información y Continuidad de TI | Acta Comité Institucional de Gestión y Desempeño (16-05/2018) | Se cambia el nombre del documento, ya que se incorporan los elementos de privacidad de la información  Se actualiza el cronograma para la ejecución del plan.  Se incluye el plan de sensibilización, capacitación y comunicación. |

1. MINTIC. Modelo de Seguridad y Privacidad. Recuperado http://www.mintic.gov.co/gestionti/615/articles-5482\_Modelo\_Seguridad.pdf [↑](#footnote-ref-1)
2. DNP. Plan Nacional de Desarrollo 2014- 2018https://colaboracion.dnp.gov.co/CDT/Prensa/PND%202014-2018%20Bases%20Final.pdf [↑](#footnote-ref-2)
3. [↑](#footnote-ref-3)
4. MINTIC PLAN DE COMUNICACIONES <http://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf> [↑](#footnote-ref-4)
5. MINTIC IPV6 <http://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf> [↑](#footnote-ref-5)