APC-COLOMBIA / TODOS POR UN NUEVO PAÍS	PROCEDIMIENTO

PROCEDIMIENTO	Gestión de Seguridad y Continuidad de TI.	Código: A-PR-041	Versión: 4 Marzo 14 de 2017
OBJETIVO:	Asegurar la confidencialidad, integridad y disponibilidad de los activos de la información asi como su continuidad soportadas por los servicios de TI.		
ALCANCE	Inicia desde el autodiagnóstico de la situación actual de la Seguridad de la Informacion continua con la la elaboracion y ejecucion del Plan de Seguridad y Continuidad de TI y finaliza con el seguimiento y control de las actividades definidas en el Plan de Seguirdad y Continuidad de TI. Aplica a los activos de informacion soportadas por los servicios de TI en la APC-Colombia		
RESPONSABLE:	Director Administrativo y Financiero / Profesional Universitario Grado 8 con Funciones en Sistemas.		
PROCESO ASOCIADO:	Gestión de Tecnologías de la Información.		

No.	ACTIVIDAD	TAREA	AUTOCONTROL	RESPONSABLE	REGISTRO	TIEMPO
1	Realizar autodiagnóstico situación actual de la Seguridad de la Información.	Diligenciar el instrumento de Evaluación del Modelo de Seguridad de la información.	N.A.	Profesional Universitario Grado 8 con Funciones en Sistemas.	Formatos Auto-Evaluación de Seguridad de la Información - MINTIC	Definido en el Plan de Trabajo de Seguridad y Continuidad de TI que le aplique a la vigencia.
2	Elaborar o Actualizar el Plan de Seguridad y Continuidad de TI	Tarea 1. Elaborar o Actualizar el Plan de Seguridad y Continuidad de TI.	N.A.	Profesional Universitario Grado 8 con Funciones en Sistemas.	Plan de Seguridad y Continuidad de TI	Definido en el Plan de Trabajo de Seguridad y Continuidad de TI que le aplique a la vigencia.
		Tarea 2. Revisar la propuesta del Plan de Seguridad y Continuidad de TI para posibles correcciones y posterior aprobación	Si la propuesta no tiene correcciones continua con la tarea 3, de lo contrario se realiza la tarea 1.	Director Administrativo y Financiero	Plan de Seguridad y Continuidad de TI	Definido en el Plan de Trabajo de Seguridad y Continuidad de TI que le aplique a la vigencia.
		Tarea 3.Aprobar el Plan de Seguridad y Continuidad de TI por el Comité Institucional de Desarrollo Administrativo	Si la propuesta es aprobada continua con la tarea 4, de lo contrario se realiza la tarea 3.	Comité Institucional de Desarrollo Administrativo	Acta de Comité	Definido en el Plan de Trabajo de Seguridad y Continuidad de TI que le aplique a la vigencia.
		Tarea 4. Realizar divulgación formal del Plan de Seguridad y Continuidad de TI	N.A.	Profesional Universitario Grado 8 con Funciones en Sistemas.	Publicación Intranet Correo Electrónico	Definido en el Plan de Trabajo de Seguridad y Continuidad de TI que le aplique a la vigencia
		Tarea 1. Actualizar la Política de Seguridad de la Información.		Profesional Universitario Grado 8 con Funciones en Sistemas.	Política de Seguridad de la Información	Definido en el Plan de Trabajo de Seguridad y Continuidad de TI que le aplique a la vigencia
		Tarea 2. Revisar la Política de Seguridad de la Información para posibles correcciones y posterior aprobación.	Si la propuesta no tiene correcciones continua con la tarea 3, de lo contrario se realiza la tarea 1.	Director Administrativo y Financiero	Política de Seguridad de la Información	Definido en el Plan de Trabajo de Seguridad y Continuidad de TI que le aplique a la vigencia

PROCEDIMIENTO	Gestión de Seguridad y Continuidad de TI.	Código: A-PR-041	Versión: 4 Marzo 14 de 2017
OBJETIVO:	Asegurar la confidencialidad, integridad y disponibilidad de los activos de la información asi como su continuidad soportadas por los servicios de TI.		
ALCANCE	Inicia desde el autodiagnóstico de la situación actual de la Seguridad de la Informacion continua con la la elaboracion y ejecucion del Plan de Seguridad y Continuidad de TI y finaliza con el seguimiento y control de las actividades definidas en el Plan de Seguirdad y Continuidad de TI. Aplica a los activos de informacion soportadas por los servicios de TI en la APC-Colombia		
RESPONSABLE:	Director Administrativo y Financiero / Profesional Universitario Grado 8 con Funciones en Sistemas.		
PROCESO ASOCIADO:	Gestión de Tecnologías de la Información.		

3	Ejecutar el Plan de Seguridad y Continuidad de TI	Tarea 3.Aprobar la Política de Seguridad de la Información por el Comité Institucional de Desarrollo Administrativo.	Si la propuesta es aprobada continua con la tarea 4, de lo contrario se realiza la tarea 3.	Comité Institucional de Desarrollo Administrativo	Acta de Comité	Definido en el Plan de Trabajo de Seguridad y Continuidad de TI que le aplique a la vigencia
		Tarea 4. Realizar divulgación formal de la Política de Seguridad de la Información.	N.A.	Profesional Universitario Grado 8 con Funciones en Sistemas.	Publicación Intranet Correo Electrónico Lista de Asistencia	Anualmente, una vez ha sido aprobada la Política.
		Tarea 5. Realizar o actualizar el Inventario de Activos de Información soportados por TI.	N.A.	Profesional Universitario Grado 8 con Funciones en Sistemas.	Informe Inventario de Activo de la Información soportados por TI	Definido en el Plan de Trabajo de Seguridad y Continuidad de TI que le aplique a la vigencia
		Tarea 6.Realizar un análisis de riesgo e identificar amenazas y Vulnerabilidades asociados a los activos de información, soportados por TI.	N.A.	Profesional Universitario Grado 8 con Funciones en Sistemas.	Formato Gestión de Riesgos de TI- MINTIC	Definido en el Plan de Trabajo de Seguridad y Continuidad de TI que le aplique a la vigencia
		Tarea 7. Realizar el Análisis de Impacto de Negocios (BIA) teniendo en cuenta el carácter crítico del activo de información soportado por TI	N.A.	Profesional Universitario Grado 8 con Funciones en Sistemas.	Formato Análisis de Impacto de Negocios BIA - MINTIC	Definido en el Plan de Trabajo de Seguridad y Continuidad de TI que le aplique a la vigencia
		Tarea 8,Definir las estrategias de Seguridad y Continuidad de TI.	N.A.	Profesional Universitario Grado 8 con Funciones en Sistemas.	Plan de Seguridad y Continuidad de TI	Definido en el Plan de Trabajo de Seguridad y Continuidad de TI que le aplique a la vigencia
4	Hacer seguimiento y control a las actividades definidas en el Plan de seguridad y Continuidad de TI.	Hacer seguimiento a los mecanismos de defensa contra las amenazas internas y externas en APC-Colombia.	N.A.	Profesional Universitario Grado 8 con Funciones en Sistemas.	Reporte UTM Reporte Herramienta iTop Reporte Consola de Antivirus	Diariamente
		Hacer seguimiento a los mecanismos de copias y recuperación de respaldos para continuidad de los servicios definidos en el Catálogo de Servicio.	N.A.	Profesional Universitario Grado 8 con Funciones en Sistemas.	Logs de la herramienta de Backup EXEC y recuperación de la información A-FO-088 Soporte Backup Información	Diariamente

NORMOGRAMA

PROCEDIMIENTO	Gestión de Seguridad y Continuidad de TI.	Código: A-PR-041	Versión: 4 Marzo 14 de 2017
OBJETIVO:	Asegurar la confidencialidad, integridad y disponibilidad de los activos de la información asi como su continuidad soportadas por los servicios de TI.		
ALCANCE	Inicia desde el autodiagnóstico de la situación actual de la Seguridad de la Informacion continua con la la elaboracion y ejecucion del Plan de Seguridad y Continuidad de TI y finaliza con el seguimiento y control de las actividades definidas en el Plan de Seguirdad y Continuidad de TI. Aplica a los activos de informacion soportadas por los servicios de TI en la APC-Colombia		
RESPONSABLE:	Director Administrativo y Financiero / Profesional Universitario Grado 8 con Funciones en Sistemas.		
PROCESO ASOCIADO:	Gestión de Tecnologías de la Información.		

#	ACTO	No.	FECHA	DETALLE	EXPEDIDA POR	RESUMEN	VÍNCULO URL
1	Ley	1273	01/05/2009	Toda la Norma	Congreso de la República	De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492
2	Ley	1581	10/17/2012	Artículo 2	Congreso de la República	Se dictan disposiciones generales para la protección de datos personales	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981
3	Ley	1712	03/06/2014	Articulo 6	Congreso de la República	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882
4	Decreto	2573	12/12/2014	Toda el Decreto	Presidencia de la República	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60596

GLOSARIO DE TÉRMINOS Y SIGLAS
Activos de información: Es aquel elemento que contiene o manipula información. Por ejemplo, ficheros, base de datos, contratos, acuerdos, documentación del sistema, manuales de usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipos de comunicación, servicios informáticos y de comunicaciones, calefacción, iluminación, energía, y aire acondicionado y las personas, que son las que en últimas generan, transmiten y destruyen información
Amenazas: Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño sobre los elementos de un sistema de seguridad informática
Análisis de riesgos: Hace referencia al proceso necesario para responder a tres cuestiones básicas sobre la seguridad: Que queremos proteger, contra quien, como lo queremos proteger.
Backup Exec: Ofrece copias de seguridad y recuperación eficaces, flexibles y fáciles de usar para la infraestructura tecnológica independientemente de la plataforma: físicas o virtual.
Copia de respaldo: Copia de la información en un medio magnético que se almacena en un lugar seguro
Confidencialidad: Criterio que responde a la importancia que tendría que el activo se accediera de manejo no autorizado.
Disponibilidad: Criterio que responde a la pregunta de cuál sería la importancia o el trastorno que tendría el que el activo no estuviera disponible.
Estrategia de seguridad de TI: Vela por la seguridad de los sistemas y servicios de TI.
Estrategia de Continuidad de TI: Se preocupa de impedir que una imprevista y grave interrupción de los servicios de TI, debido a causa de fuerzas mayor tengan consecuencias catastróficas para la Entidad.
Gestión de riesgo: Es un programa de trabajo y estrategias para disminuir la vulnerabilidad y promover acciones de conservación, desarrollo de mitigación del riesgo utilizando recursos gerenciales.
Integridad: Criterio que responde que importancia tendría que el activo fuera alterado sin autorización ni control.
Inventario de activos: Es la base para la gestión de los mismos, ya que tiene que incluir toda la información necesaria para mantenerlos operativos e incluso poder recuperarse ante un desastre.
ITOP: Herramienta Open Source, permite la gestión del inventario, gestión de incidencias, gestión del cambio, gestión del servicio (SLAs, contratos con clientes y proveedores)
Plan de Seguridad y Continuidad de TI: Provee información sobre asuntos de Seguridad y de Continuidad de TI.
Política de seguridad de TI: Establece reglas vinculantes para el uso de servicios y de sistemas con miras a mejorar la seguridad de TI.

PROCEDIMIENTO	Gestión de Seguridad y Continuidad de TI.	Código: A-PR-041	Versión: 4 Marzo 14 de 2017
OBJETIVO:	Asegurar la confidencialidad, integridad y disponibilidad de los activos de la información asi como su continuidad soportadas por los servicios de TI.		
ALCANCE	Inicia desde el autodiagnóstico de la situación actual de la Seguridad de la Informacion continua con la la elaboracion y ejecucion del Plan de Seguridad y Continuidad de TI y finaliza con el seguimiento y control de las actividades definidas en el Plan de Seguirdad y Continuidad de TI. Aplica a los activos de informacion soportadas por los servicios de TI en la APC-Colombia		
RESPONSABLE:	Director Administrativo y Financiero / Profesional Universitario Grado 8 con Funciones en Sistemas.		
PROCESO ASOCIADO:	Gestión de Tecnologías de la Información.		

Riesgo: Es la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione, a las operaciones.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI (Sistema de Gestión de la Seguridad de la Información): Es un depósito virtual de todos los datos de gestión de la seguridad de TI.

UTM: Es un término que se refiere a un firewall de red con múltiples funciones añadidas, trabajando a nivel de aplicación. Realiza el proceso del tráfico a modo de proxy, analizando y dejando pasar el tráfico en función de la política implementada en el dispositivo

Vulnerabilidad: Es la capacidad, las condiciones y características del sistema mismo, que lo hace susceptible a amenazas, con el resultado de sufrir algún daño.

TRAZABILIDAD

VERSIÓN	CÓDIGO	NOMBRE DEL DOCUMENTO	ACTO	CONTROL DE CAMBIOS
1	A-PR-041	Gestión de Seguridad	Acta de Dic22/2015	Hace parte de los nuevos procedimientos (A-PR-036, A-P
2	A-PR-041	Gestión de Seguridad	Brújula Mayo 12 de 2016	Se actualizan tiempos, responsable, diagrama
3	A-PR-041	Gestión de Seguridad y de la Continuidad de TI	Brújula, Jul26/2016	Se fusiona los procedimientos Gestión de Seguridad y Gestion de Continuidad y se realiza cambios de lo siguientes item: 1. Se define un nuevo Objetivo. 2. Se define un nuevo Alcance. 3. Se cambian todas las actividades para fusionar los dos procedimientos. 4. Se hace cambio en el nombre del procedimiento
4	A-PR-041	Gestión de Seguridad y de la Continuidad de TI	Brújula, Marzo 14 de 2017	Se ajusta a la nueva imagen institucional.