 CONTADURÍA <small>GENERAL DE LA NACIÓN</small>	SEGURIDAD DE LA INFORMACIÓN			
	PROCESO	GESTIÓN TICS		
	FECHA DE APROBACIÓN: 16-11-2018	CÓDIGO: GTI-PRC010	VERSIÓN:	PAG. 3

1. OBJETIVO

Establecer y ejecutar las actividades propias para asegurar y mantener la seguridad de la información, de la plataforma tecnológica, en lo referente a la red de datos y comunicaciones, sistemas operativos, bases de datos, y aplicativos utilizados, brindando un acompañamiento en cuanto al aseguramiento de la disponibilidad y continuidad de los servicios y sistemas de información de la Contaduría General de la Nación.

Basándose en la Política, las normas de seguridad definen qué hay que proteger y los niveles de protección deseados. El conjunto de todas las normas de seguridad debe cubrir la protección de todos los entornos de los sistemas de información de la organización; y establecer un conjunto de expectativas y requisitos que deben ser alcanzados para poder satisfacer y cumplir cada uno de los objetivos de seguridad establecidos en la política de seguridad de la información.

2. DEFINICIONES

ACTIVO DE INFORMACIÓN: Un activo de información es cualquier cosa que tenga valor para la organización y en consecuencia deba ser protegido. No obstante este concepto es bastante amplio y debe ser limitado por una serie de consideraciones el impacto que para la institución supone la pérdida de confidencialidad integridad o disponibilidad de cada activo el tipo de información que maneja en términos de su sensibilidad y criticidad y sus productores y consumidores. Los activos de información se traducen en dispositivos tecnológicos archivos bases de datos documentación física personas sistemas de información entre otros.


APLICATIVO: Es un tipo de programa informático diseñado para facilitar al usuario la realización de un determinado tipo de trabajo.

BORRADO SEGURO: Es la medida de seguridad mediante la cual se establecen métodos y técnicas para la eliminación definitiva de los datos personales de modo que la probabilidad de recuperarlos sea mínima.

CONFIABILIDAD: Es la capacidad de un producto de realizar su función de la manera prevista. De otra forma la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

CONFIDENCIALIDAD: Es la garantía de que la información no está disponible o divulgada a personas entidades o procesos no autorizados.

CONTINUIDAD: Práctica que relaciona la organización para recuperarse ante cualquier

 CONTADURÍA <small>GENERAL DE LA NACIÓN</small>	SEGURIDAD DE LA INFORMACIÓN			
	PROCESO	GESTIÓN TICS		
	FECHA DE APROBACIÓN: 16-11-2018	CÓDIGO: GTI-PRC010	VERSIÓN: 3	PAG. 2 de 2

inconveniente o desastre con el fin de restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

COPIA DE RESPALDO: Copia adicional o duplicado que generamos del contenido de cada uno de los equipos de cómputo de la entidad servidores configuraciones se deben realizar con cierta periodicidad teniendo en cuenta siempre la importancia de la información que manejamos y la cantidad de cambios que realicemos.

CUSTODIA DEL ACTIVO DE INFORMACIÓN: Es la unidad organizacional o proceso designado por los propietarios encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

DISPONIBILIDAD: Calidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella ya sean personas procesos o aplicaciones. A groso modo la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

EVENTOS: Es un cambio de estado importante para un elemento de configuración (CI) o para la gestión de servicios de TI es una alerta o notificación creada por cualquier servicio TI CI o herramienta de supervisión.

FORMATO A BAJO NIVEL: Reiniciación de un disco a su configuración de fábrica.


INCIDENTE: Una interrupción no planificada de un Servicio de TI o una reducción de la Calidad de un Servicio de TI.comportamiento no esperado en el sistema que puede impedir la continuidad del mismo.

INFORMACIÓN: Está constituida por un grupo de datos ya supervisados y ordenados que sirven para construir un mensaje basado en cada una de las actividades que se realizan en la entidad. La información permite resolver problemas y tomar decisiones ya que su aprovechamiento racional es la base del conocimiento. // Es lo que se obtiene del procesamiento de datos es el resultado final de interés para entidades usuarios y servidores públicos entre otros.

LOGS: Registro o datos de quién qué cuándo dónde y por qué un evento ocurre para un dispositivo o sistema en particular.

PROBLEMA: Causa conocida o desconocida que generó el incidente.

POLÍTICA DE SEGURIDAD: Conjunto de normas y procedimientos establecidos por una

 CONTADURÍA <small>GENERAL DE LA NACIÓN</small>	SEGURIDAD DE LA INFORMACIÓN			
	PROCESO	GESTIÓN TICS		
	FECHA DE APROBACIÓN: 16-11-2018	CÓDIGO: GTI-PRC010	VERSIÓN: 3	PAG. 3 de 3

organización para regular el uso de la información y de los sistemas que la tratan con el fin de mitigar el riesgo de pérdida deterioro o acceso no autorizado a la CGN.

RACK: Gabinete destinado a alojar equipamiento electrónico informático y de comunicaciones. Las medidas para la anchura están estandarizadas para sea compatible con equipamiento de cualquier fabricante.

RECURSOS TECNOLÓGICOS: Son aquellos componentes de hardware y software tales como servidores (De aplicaciones y de servicios de red) estaciones de trabajo equipos portátiles dispositivos de comunicaciones y de seguridad equipos de radio servicios de red de datos y bases de datos entre otros los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la institución.

RED DE DATOS: Es la infraestructura cuyo diseño posibilita la transmisión de información a través del intercambio de datos. Cada una de estas redes ha sido diseñada específicamente para satisfacer los objetivos de la entidad con una arquitectura determinada para facilitar el intercambio de los contenidos.

Red LAN: Local Área Network Red de área local es una red que conecta los equipos de cómputo en un área relativamente pequeña y predeterminada (como una habitación un edificio o un conjunto de edificios).


RESPALDO: Copia de seguridad o backup de información realizada con el fin de utilizarse para restaurar la original después de una eventual pérdida de datos.

SEGURIDAD: Se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y especialmente la información contenida o circulante. Para ello existen una serie de estándares protocolos métodos reglas herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

SISTEMA DE INFORMACIÓN: Es un conjunto organizado de elementos que pueden ser personas datos actividades o recursos materiales en general. Estos elementos interactúan entre sí para procesar información y distribuirla de manera adecuada en función de los objetivos de una organización.

SISTEMA OPERATIVO (S.O.): Es un conjunto de programas de computación destinados a realizar múltiples tareas entre ellas se destaca la administración eficaz de los recursos de hardware del sistema y la ejecución de diversas aplicaciones.

SOFTWARE MALICIOSO: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o danacutear los recursos tecnológicos sistemas

 CONTADURÍA <small>GENERAL DE LA NACIÓN</small>	SEGURIDAD DE LA INFORMACIÓN			
	PROCESO	GESTIÓN TICS		
	FECHA DE APROBACIÓN: 16-11-2018	CÓDIGO: GTI-PRC010	VERSIÓN: 3	PAG. 4 de 4

operativos redes de datos o sistemas de información.

TERCEROS O PARTES EXTERNAS: Personas o entidades que brindan servicios a la CGN o que interactúan de alguna manera con la información de entidad.

UPS: Suministro redundante de energía ininterrumpible dispositivo que permite suministrar energía a los dispositivos que están conectados a él después de un apagado durante un tiempo prudencial para realizar un apagado seguro de dichos dispositivos.

VULNERABILIDAD: Propiedades intrínsecas de algo que resulta en la susceptibilidades a una fuente de riesgo que puede ocasionar un evento con una consecuencia. // GTI. Son las debilidades hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la institución (amenazas) las cuales se constituyen en fuentes de riesgo.

3. MARCO LEGAL

[Ley 1712 del 6 de Marzo de 2014.](#) 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.

[Ley 1581 del 17 de octubre de 2012.](#) Por la cual se dictan disposiciones generales para la protección de datos personales.


[Ley 1753 de 09 de junio de 2015.](#) Por la cual se expide el plan nacional de desarrollo 2014-2018 todos por un nuevo país

[Ley 1341 de 30 julio de 2009.](#) Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones -tic-, se crea la agencia nacional de espectro y se dictan otras disposiciones.

[Ley 1273 de 05 de enero de 2009.](#) Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

[Ley Estatutaria 1266 de 31 de diciembre 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, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

[Decreto 1499 de 11 de septiembre de 2017.](#) Por medio del cual se modifica el Decreto 1083

 CONTADURÍA <small>GENERAL DE LA NACIÓN</small>	SEGURIDAD DE LA INFORMACIÓN			
	PROCESO	GESTIÓN TICS		
	FECHA DE APROBACIÓN: 16-11-2018	CÓDIGO: GTI-PRC010	VERSIÓN: 3	PAG. 5 de 5

[de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015](#)

[Decreto 1078 de 26 de mayo de 2015.](#) Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

[Decreto 2573 de 12 de diciembre de 2014.](#) 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.

[Decreto 1377 de 27 de junio de 2013.](#) Por el cual se reglamenta parcialmente la Ley 1581 de 2012 Ley de Habeas Data

[Decreto 2693 de 21 de diciembre de 2012.](#) Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, Y se dictan otras disposiciones

[Resolución 364 de 28 de agosto de 2017.](#) Por el cual se actualiza el Sistema Integrado de Gestión Institucional (SIGI) en la Unidad administrativa Especial Contaduría General de la Nación y se dictan otras disposiciones.

[Norma Técnica Norma Técnica Colombiana ISO 45001-2018.](#) Sistemas de Gestión de la Seguridad y Salud en el Trabajo

[Norma Técnica Colombiana ISO 9001-2015.](#) Sistema de Gestión de la Calidad

[Norma Técnica Colombiana ISO 14001- 2015.](#) Sistema de Gestión Ambiental

[Norma Técnica Colombiana ISO IEC 27001-2013.](#) Sistemas de Gestión de la Seguridad de la Información

4. DOCUMENTOS RELACIONADOS

[CHECK LIST GTI03-FOR01](#)


[BITACORA PLATAFORMA TECNOLOGICA GTI02-FOR01](#)

[SOLICITUD DE CUENTAS DE USUARIO INSTITUCIONAL GTI010-FOR02](#)

[REGISTRO INCIDENTES SEGURIDAD DE LA INFORMACIÓN GTI010-FOR01](#)

[POLITICA DE ADMINISTRACION DE USUARIOS Y/O CONTRASEÑAS GTI02-POL01](#)

[TRASLADO DE ELEMENTOS ENTRE SERVIDORES PÚBLICOS Y/O CONTRATISTAS GAD-](#)

 CONTADURÍA <small>GENERAL DE LA NACIÓN</small>	SEGURIDAD DE LA INFORMACIÓN			
	PROCESO	GESTIÓN TICS		
	FECHA DE APROBACIÓN: 16-11-2018	CÓDIGO: GTI-PRC010	VERSIÓN:	PAG. 3

PRC02

- [ACTA DE RECIBO A SATISFACCIÓN GTI06-FOR02](#)
- [ACTA DE CERTIFICACIÓN DE VERSIÓN GTI06-FOR03](#)
- [ADMINISTRACION DE CAMBIOS DE TI GTI02-FOR04](#)
- [PROCEDIMIENTO OPERACIÓN CENTRO DE COMPUTO GTI-PRC03](#)
- [FORMATO DE PAZ Y SALVO POR DESVINCULACIÓN O TERMINACIÓN DE CONTRATO GAD05-FOR01](#)
- [CREACIÓN DE USUARIOS APLICATIVO CHIP GTI010-FOR03](#)
- [SOLICITUD DE CUENTAS DE USUARIO INSTITUCIONAL - VPN GTI010-FOR04](#)
- [MANUAL DE SEGURIDAD DE LA INFORMACION GTI-MAN01](#)
- [NO CONFORMIDADES, ACCION CORRECTIVA, PREVENTIVA Y PLANES DE MEJORAMIENTO PI-PRC16](#)
- [DIAGNÓSTICO DE NECESIDADES DE APRENDIZAJE POR GIT - DNAG GTH01-FOR11](#)
- [ORDEN DE CAMBIO GTI01-FOR02](#)
- [INSTRUCTIVO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. GTI010-INS04](#)
- [INSTRUCTIVO GESTIÓN DE LA CAPACIDAD GTI010-INS02](#)
- [INSTRUCTIVO PARA LA RECOLECCIÓN Y PRESERVACIÓN DE EVIDENCIA GTI010-INS03](#)
- [INSTRUCTIVO PARA LA GESTIÓN DE CAMBIOS TECNOLÓGICOS GTI010-INS05](#)
- [FORMATO EXTRACCIÓN IMAGÉNES FORENSES GTI010-FOR05](#)
- [RÓTULO ELEMENTO MATERIA DE PRUEBA O EVIDENCIA FÍSICA. GTI010-FOR06](#)

5. DOCUMENTOS ANEXOS
No plaica

6. PROCEDIMIENTO
Se anexan Flujogramas del procedimiento de seguridad de la informacion.

- [FLUJOGRAMA COPIAS DE RESPALDO DE LA INFORMACIÓN.xls](#)
- [FLUJOGRAMA SEGURIDAD DE LA INFORMACIÓN.xls](#)
- [FLUJOGRAMA SEGURIDAD DE REDES, COMUNICACIONES Y SERVICIOS DE TI.xls](#)
- [FLUJOGRAMA SEGURIDAD EN EL DESARROLLO Y MANTENIMIENTO DE SOFTWARE.xls](#)
- [FLUJOGRAMA ACTUALIZACIÓN DE SOFTWARE Y HARDWARE.xls](#)
- [FLUJOGRAMA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN.xls](#)
- [FLUJOGRAMA CONTROL DE ACCESO A SISTEMAS DE INFORMACIÓN Y ADMINISTRACIÓN DE USUARIOS Y CONTRASEÑAS.xls](#)
- [FLUJOGRAMA DE GESTIÓN DE CAMBIOS TECNOLÓGICOS.xlsx](#)
- [FLUJOGRAMA DERECHO DE PROPIEDAD INTELECTUAL.xls](#)

 CONTADURÍA <small>GENERAL DE LA NACIÓN</small>	SEGURIDAD DE LA INFORMACIÓN			
	PROCESO	GESTIÓN TICS		
	FECHA DE APROBACIÓN: 16-11-2018	CÓDIGO: GTI-PRC010	VERSIÓN:	PAG. 3

[FLUJOGRAMA GESTIÓN DE INCIDENTES, AMENAZAS Y DEBILIDADES DE SEGURIDAD.xls](#)

[FLUJOGRAMA GESTIÓN DE LA CAPACIDAD.xls](#)

[FLUJOGRAMA GESTION DE MEDIOS REMOVIBLES.xls](#)

[FLUJOGRAMA OPERACIÓN DEL CENTRO DE DATOS.xls](#)

[FLUJOGRAMA SEGURIDAD FÍSICA Y ENTORNO.xls](#)

Nota: La totalidad de la ejecución de las actividades descritas deben ser alineadas a las Políticas del Sistema Integrado de Gestión Institucional (Política de la calidad, Política Ambiental, Política de la SST, Política de la Seguridad de la Información, Políticas de Gestión y desempeño institucional - MIPG) lo que contribuirá al cumplimiento misional, la satisfacción de las partes interesadas, la mejora del desempeño ambiental, proporcionar un lugar seguro y saludable previniendo lesiones y deterioro de la salud, asegurar la integridad, disponibilidad y confiabilidad de la información recibida y generada y el éxito sostenido de la CGN.

Revisado por:	Aprobado por:
LIDER DEL PROCESO GESTIÓN TICS	REPRESENTANTE DE LA DIRECCIÓN LÍDER DE PROCESO DE PLANEACIÓN INTEGRAL