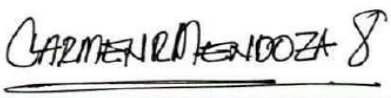
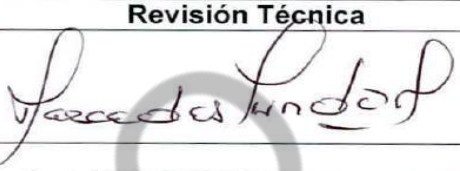
	Aprobación	Revisión Técnica
Firma:		
Nombre:	CARMEN ROSA MENDOZA SUÁREZ	**Nombre:** MERCEDES YUNDA MONROY
Cargo:	Director Técnico	**Cargo:** Director Técnico
Dependencia:	Dirección de Tecnologías de la Información y las Comunicaciones	**Dependencia:** Dirección de Planeación
R.R. No. 047	**Fecha**	28 DIC. 2018

1. OBJETIVO

Gestionar los incidentes y/o eventos de seguridad que se presenten en los activos de información de la Contraloría de Bogotá D.C., y que atenten contra sus características de Confidencialidad, Integridad y Disponibilidad, así como la atención eficaz y oportuna de éstos.

2. ALCANCE

El procedimiento inicia con la creación del Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT) y termina con la documentación y cierre del incidente.

3. BASE LEGAL

NORMA	FECHA	DESCRIPCIÓN
Ley 1273	5-ene-2009	Por medio de la cual se modifica el Código Penal. Título VII Bis "De la protección de la información y de los datos". Artículos 269A a 269J.
Ley 1581	17-oct-2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712	06-mar-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.
Decreto 1377	27-jun-2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 886	13-may-2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Decreto 2573	12-dic-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 103	20-ene-2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1078	26-may-2015	Por medio del cual se expide el Decreto Único

NORMA	FECHA	DESCRIPCIÓN
		Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Capítulo 1, Título 9, Libro 2, Parte 2 subrogado por el Decreto 1008 de 2018.
Decreto 1081	26-may-2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector Presidencia de la República. Parte 1, Titulo 1.
Decreto 1008	14-jun-2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. Política de Gobierno Digital.
Acuerdo 658	21-dic-2016	Por el cual se dictan normas sobre organización y funcionamiento de la Contraloría de Bogotá, D.C., se modifica su estructura orgánica e interna, se fijan las funciones de sus dependencias, se modifica la planta de personal, y se dictan otras disposiciones.
Acuerdo 664	28-mar-2017	Por el cual se modifica parcialmente el Acuerdo 658 del 21 de diciembre de 2016, por el cual se dictan normas sobre organización y funcionamiento de la Contraloría de Bogotá, D.C., se modifica su estructura orgánica e interna, se fijan las funciones de sus dependencias, se modifica la planta de personal, y se dictan otras disposiciones.
Resolución 305	20-oct-2008	Comisión Distrital de Sistemas. Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.
Resolución 004	28-nov-2017	Por la cual se modifica la Resolución 305 de 2008 de la CDS
CONPES 3701-2011	14-jul-2018	Lineamientos de Política para Ciberseguridad y Ciberdefensa.
CONPES 3854 - 2016	11-Abr-2016	Política Nacional de Seguridad Digital.
NTC-ISO/IEC COLOMBIANA 20000-1:2011	abr-2011	Norma Técnica Colombiana NTC-ISO/IEC 27001 Colombiana. Tecnología de la Información.Gestión de Servicio. Parte 1: Requisitos del Sistema de Gestión del Servicio.
NTC-ISO/IEC COLOMBIANA 27001:2013	11-dic-2013	Norma Técnica Colombiana NTC-ISO-IEC 27001.Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información.Requisitos.

NORMA	FECHA	DESCRIPCIÓN
Guía No 3	25-abr-2016	Procedimientos de Seguridad de la Información, MINTIC.

4. DEFINICIONES

Clasificación y priorización de servicios expuestos: Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.

Código malicioso: Es un tipo de código informático o script web dañino diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Contención: Son aquellas acciones tendientes a evitar la propagación de la amenaza que ocasiono el incidente de seguridad de la información detectado.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT): Es un grupo de profesionales que buscan restituir las actividades con el impacto mínimo aceptable para la entidad, así mismo brindan apoyo al funcionario u área afectada en la respuesta rápida para contener un incidente de seguridad de la información de igual manera recibe los informes sobre incidentes de seguridad, analiza las situaciones y responde a las amenazas.

Erradicación: Una vez el incidente de seguridad de la información es contenido, este debe erradicarse, es decir, eliminar cualquier tipo de rastro que pudiera existir con ocasión de comportamiento inusual sobre los activos de información y/o infraestructura de TI.

Incidente de Seguridad[1]: Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de Seguridad de la Información de la entidad.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Log (Registro): es un archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado.

[1] http://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

Mesa de servicios: Sistema manual o automatizado donde los funcionarios o entes externos registran las solicitudes e incidencias sobre los servicios que presta la Dirección de TIC.

Recolección y Análisis de Evidencia: Actividad referente a la toma, preservación, documentación y análisis de evidencia.

Vulnerabilidad: Debilidad de un activo o control que pueda ser explotado por una o más amenazas.

5. DESCRIPCIÓN DEL PROCEDIMIENTO

N°	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Director de Tecnologías de la Información y la comunicaciones	Crea el Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT), el cual estará conformado por el Director, los Subdirectores de la Dirección de TIC, el líder de seguridad de la Información y los administradores y/o gestores de infraestructura y/o servicios de TI según el incidente a considerar.	Comunicación Oficial	**Observación:** Al Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT), deben ser convocados funcionarios con funciones asignadas relativas al incidente a atender, así como el dueño funcional del servicio que está afectado (Si aplica). Los integrantes del Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT) tienen derecho a voz y voto, mientras que los invitados solo podrán ejercer el derecho de voz.
2	Servidores públicos de la Contraloría de Bogotá.	Reporta el evento, siguiendo las actividades del numeral 5.1. del procedimiento PGTI-04 - “Registro y	Sistema de Mesa de Servicios por número de caso.	

N°	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		atención de requerimientos de soporte a los sistemas de información y equipos informáticos".		
3	Profesional Especializado, Profesional Universitario o Técnico responsable del Sistema de Mesa de Servicios.	Evalúa si el evento y/o incidente reportado es una falsa alarma o es un incidente de seguridad que afecta la disponibilidad, integridad y/o confidencialidad de la información. En caso de que el incidente no sea catalogado como de seguridad de la información, se continuará el numeral 5.1. Del procedimiento PGTI-04 - "Registro y atención de requerimientos de soporte a los sistemas de información y equipos informáticos".	Sistema de Mesa de Servicios por número de caso.	
4	Profesional Especializado, Profesional Universitario o Técnico responsable del Sistema de Mesa de Servicios.	Clasifica el Incidente tomando como referencia la tabla de clasificación de los incidentes y/o eventos de seguridad (Ver. ANEXO No.1 - Clasificación de Incidentes de Seguridad).	Sistema de Mesa de Servicios por número de caso.	**Observación:** El incidente deberá ser estimado estableciendo el impacto causado a cualquier activo de Información de la Contraloría de Bogotá y a los tiempos de respuesta por parte de la Dirección de TIC. Todo esto, deberá ser documentado en el registro de la Mesa de Servicio.

N°	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
5	Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT)	Verifica la situación actual del incidente (finalizó, está en proceso, ya se tiene bajo control), obteniendo la mayor cantidad de información del incidente, complementando el registro del Incidente, como resultado de la verificación puede reclasificar y reasignar el incidente.	Sistema de Mesa de Servicios por número de caso.	**Observación:** Se deberá validar la situación reportada realizando visita en sitio de ser necesario y se da inicio al análisis del incidente, posibles causas, daños, y demás datos necesarios para realizar el análisis. Es necesario que se recoja la mayor cantidad de información de lo ocurrido o de lo que llevó al reporte teniendo en cuenta el antes, durante y después de cada acción o comportamiento para identificar la causa de manera rápida y apropiada. Así como analizar el material complementario como logs, archivos, código malicioso entre otros. Determina si es necesario reportar el caso la Oficina de Asuntos Disciplinarios en caso de existir una presunta conducta disciplinaria.

N°	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
6	Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT)	Verifica si el incidente puede ser manejado por los responsables de la actividad o se hace necesario el apoyo de un proveedor o Entidad externa. Si es necesario el apoyo de un proveedor para el manejo, se continúa con las actividades del procedimiento PGAF-08 - Gestión Contractual.	Sistema de Mesa de Servicios por número de caso.	**Punto de Control:** Si el incidente es originado en la ejecución de un contrato, el supervisor del mismo, debe diligenciar la información requerida en el incidente, incluyendo el plan de actividades que va a ejecutar el proveedor.
7	Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT)	Planea las estrategias a seguir las actividades que se deben ejecutar para la gestión del Incidente de Seguridad y posteriormente, si es necesario recurrir a una recolección de evidencias. Identifica las causas del incidente, las plataformas afectadas y el detalle técnico de los activos afectados.	Documento de la estrategia para de atención del incidente	**Punto de Control**: El Director de las TIC, junto con los Subdirectores de acuerdo a la clasificación del Incidente, evalúan y aprueban la realización de las actividades propuestas en la estrategia de atención al incidente. **Observación:** Dentro de la planeación para la atención del incidente y/o evento de seguridad, deberá tener en cuenta los tiempos, así como aquellas necesidades de recursos logísticos, humanos, áreas que deben involucrarse, entre otros aspectos.

N°	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
8	Asesor y/o Profesional Especializado con funciones de Oficial de Seguridad de la Información y Profesionales de la Dirección TIC – con roles de Administradores de infraestructura y/o servicios de TI.	Ejecuta las acciones orientadas a la contención y corrección inmediata buscando salvaguardar la información principal que está siendo afectada.	Sistema de Mesa de Servicios por número de caso.	**Observación**: Los esfuerzos se deben enfocar en detener el incidente de seguridad, evitando la propagación de la amenaza que lo causo y teniendo en cuenta las siguientes prioridades: • Proteger la vida y la seguridad de las personas. • Proteger la información confidencial o del ámbito directivo. • Proteger el hardware y software contra el ataque. • Minimizar la interrupción de los sistemas de información (incluidos los procesos).
9	Asesor y/o Profesional Especializado con funciones de Oficial de Seguridad de la Información y Profesionales de la Dirección TIC – con roles de Administradores de infraestructura y/o servicios de TI.	Ejecuta actividades de mitigación y remediación del incidente que se plantearon en el documento de la estrategia de atención al incidente con el fin de controlar la vulnerabilidad explotada y activando o implementado controles y/o eliminando o contralando la amenaza.	Sistema de Mesa de Servicios por número de caso.	**Observación:** Dentro de las actividades de remediación, se deberán tener en cuenta actividades de inspección, si es el caso, a todos aquellos activos de información que pudieron estar impactados, con la finalidad de poder cerrar las vulnerabilidades detectadas.

N°	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
10	Asesor y/o Profesional Especializado con funciones de Oficial de Seguridad de la Información y Profesional Especializado, Profesional Universitario de la Dirección TIC con roles de Administradores de infraestructura y/o servicios de TI.	Ejecuta actividades de recuperación de sistemas de información, de información o restauración, para lo cual, si se requiere cargar la copia de respaldo actualizada del sistema de información, configuración y/o base de datos, se ejecuta el numeral 5.2 Restauración de copias de respaldo del procedimiento Realización y Control de Copias de Respaldo (backups) – PGTI-03.	Sistema de Mesa de Servicios por número de caso.	**Observación:** Dentro de las actividades de recuperación se puede contemplar: • Creación nuevamente de la información digital o física, configuración de sistemas operativos, sistemas de información y carga manual de la información. • Actualización o instalación de parches de seguridad a los sistemas que se vieron comprometidos. • Actualización en lote del antivirus.
11	Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT)	Comprueba la eficacia y oportunidad de la solución al incidente de seguridad de la información.	Sistema de Mesa de Servicios por número de caso.	**Observación:** Como parte de la comprobación, se debe realizar un análisis que ocasionó la no disponibilidad de los servicios, o el daño de los activos de información afectados por el incidente de seguridad, teniendo en cuenta la criticidad que estos representan para la entidad.
12	Asesor y/o Profesional Especializado	Documenta y cierra el incidente con indicación del análisis	Sistema de Mesa de Servicios por número de caso.	

N°	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
	con funciones de Oficial de Seguridad de la Información	de sitio, fecha, descripción del hecho y cuáles fueron las causas, la estrategia de atención, las acciones preventivas, acciones correctivas, conclusiones y recomendaciones.		

6. ANEXOS

ANEXO No.1 - Clasificación de Incidentes de Seguridad

La clasificación de los incidentes de seguridad se debe realizar teniendo en cuenta la siguiente tabla:

Tabla 1 - Niveles de criticidad de los incidentes y/o eventos de Seguridad

NIVEL	NOMBRE	TIEMPO DE ATENCIÓN
1	BAJO	1 SEMANA
2	MEDIO	2 DÍAS
3	ALTO	12 HORAS
4	CRÍTICO	1 HORA

Fuente: Elaboración propia – con base en el catálogo de servicios de la Dirección de TIC de la Contraloría de Bogotá.

La ponderación para la clasificación de estos niveles es la siguiente:

Bajo o Nulo: Este nivel de criticidad se da para aquellos incidentes o eventos que son detectados y/o denunciados como posibles amenazas para los activos de información, es decir, que pueden impactar sus características de integridad y/o confidencialidad y/o disponibilidad, sin embargo, los controles de seguridad resultan efectivos anulando cualquier impacto para la Contraloría de Bogotá.

Medio: Este nivel de criticidad se da para aquellos incidentes o eventos que son detectados y/o denunciados como posibles amenazas, que pueden afectar los activos de información de la entidad, impactando de modo limitado sus características de integridad y/o confidencialidad y/o disponibilidad frente a un activo no crítico para la Contraloría de Bogotá.

Alto: Este nivel de criticidad se da para aquellos incidentes o eventos que son detectados y/o denunciados, porque en ellos, es posible establecer una amenaza sobre los activos de información capaz de impactar de manera considerable las características de integridad y/o confidencialidad y/o disponibilidad de un activo no crítico o critico para la Contraloría de Bogotá.

Crítico: Este nivel de criticidad se da para aquellos incidentes o eventos que son detectados y/o denunciados, porque en ellos, es posible establecer una amenaza sobre los activos de información capaz de impactar de manera considerable las características de integridad y/o confidencialidad y/o disponibilidad de un activo crítico la Contraloría de Bogotá.

7. CONTROL DE CAMBIOS

Versión	R.R. No. Fecha Día mes año	Descripción de la modificación
1.0		Versión Inicial