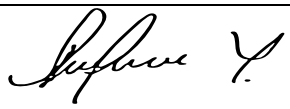
	Aprobación	**Revisión Técnica**
Firma:		
Nombre:	CARMEN ROSA MENDOZA SÚAREZ	ROBER ENRIQUE PALACIOS SIERRA
Cargo:	Directora Técnica.	Director Técnico (EF)
Dependencia:	Dirección de Tecnologías de la Información y las Comunicaciones.	Dirección de Planeación.
R.R. No. 016	**Fecha 10-08-2020**	

1. OBJETIVO

Establecer las actividades para 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), recolección de evidencias y termina con la documentación y solución 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.

NORMA	FECHA	DESCRIPCIÓN
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 103	20-ene-2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
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.
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.

NORMA	FECHA	DESCRIPCIÓN
Resolución 305 de la Secretaría General Alcaldía Mayor de Bogotá D.C. - Comisión Distrital de Sistemas - CDS	20-oct-2008	Por la cual se expiden las 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", la cual fue modificada por la Resolución 004 del 28 de noviembre de 2017.
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 27001:2013	11-dic-2013	Norma Técnica Colombiana - Requisitos del Sistema de Gestión de la Seguridad de la Información.
Norma GTC ISO/IECISO 27002	22-jul-2015	Guía Técnica Colombiana ISO - Tecnologías de la Información. Técnicas de Seguridad. Código de Práctica para Controles de Seguridad de la Información.
Guía No 3 de MINTIC	25-abr-2016	Procedimientos de Seguridad de la Información.

4. DEFINICIONES:

Activo (Inglés: Asset): cualquier cosa que tenga valor para un individuo, una organización o un gobierno[1] .

Activo de Información: conocimiento o datos que tienen valor para el individuo u organización[2]. 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[3].

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

[1] Tomado de la Norma ISO/IEC 27032:2012 (definición 4.6, traducida al español), disponible en Internet en: https://www.iso.org/obp/ui/#iso:std:isoiec:27032:ed-1:v1:en.
[2] Ibídem (definición 4.27, traducida español)
[3] Tomado del Portal de ISO 27001 en español, Gestión de Seguridad de la Información. En http://www.iso27000.es/glosario.html#section10a.

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.

Evidencia: información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información.

Incidente de Seguridad[4]: 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.

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.

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

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

5. DESCRIPCIÓN DEL PROCEDIMIENTO

5.1 Gestión de incidentes de seguridad la información.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Director de Tecnologías de la Información y las 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, Oficial de Seguridad de la Información, 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 responsable 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 D.C. Partes interesadas.	Reporta el evento a través del sistema de mesa de servicio; se activa el Procedimiento de registro y atención de requerimientos de soporte a los sistemas de información y equipos informáticos - PGTI-04. En caso que no se tenga acceso a la mesa de servicios, puede realizar el reporte a través de	Sistema de Mesa de Servicios por número de caso	**Observación:** Se deberá seguir lo establecido en el procedimiento PGTI-04, en lo referente a las actividades de los responsables de Atender Caso Nivel 1, 2, 3 o 4 según corresponda y aplique, hasta el cierre del caso.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		cualquier medio de comunicación (telefónico, escrito, correo electrónico, verbal) para que la Dirección de TIC lo registre en el sistema correspondiente.		
3	Profesional o Técnico responsable del Sistema de Mesa de Servicios.	Asigna la solicitud al Líder Seguridad de la Información para atender requerimiento.	Registro en el Sistema de Mesa de Servicios	
4	Profesional Líder Seguridad de la Información.	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. Si el caso no es catalogado como incidente de seguridad de la información, puede recategorizarlo para darle solución definitiva o reasignarlo y finaliza este procedimiento. De lo contrario informa al Oficial de Seguridad de la Información.	Sistema de Mesa de Servicios por número de caso	
5	Profesional Líder Seguridad de la Información y Oficial de Seguridad.	Recolectan la información del incidente e identifica las causas y consecuencias. Clasifican el Incidente tomando como referencia la tabla de clasificación de los incidentes y/o eventos de seguridad (Anexo No. 1).	Sistema de Mesa de Servicios por número de caso Correo electrónico institucional convocatoria sesión equipo	**Punto de control:** Verifica los activos de información que puedan ser afectados por el incidente de seguridad. Si el incidente es originado en la ejecución de un contrato, el

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		Documentan el Incidente y como resultado de la verificación convoca sesión de Equipo de Respuestas ante Incidentes de Seguridad de la Información (CSIRT) y les remite información documentada del caso.	CSIRT	supervisor del mismo, debe diligenciar la información requerida en el incidente, incluyendo el plan de actividades que va a ejecutar el proveedor.
6	Equipo de respuestas ante incidentes de seguridad de la Información (CSIRT).	Realizan análisis del incidente para lo cual: • Revisan la información presentada del incidente. • Determinan las acciones que se deben ejecutar para la gestión y atención del Incidente de Seguridad. • Definen si el incidente puede ser gestionado internamente o se hace necesario el apoyo de un proveedor o Entidad externa y determinan sí es necesario recurrir a una recolección de evidencias, se activa procedimiento 5.2 Recolección de evidencias en incidente de seguridad.	Acta CSIRT	**Observación:** Si es necesario el apoyo de un proveedor para el manejo, se activa del procedimiento PGAF08 - Gestión Contractual. **Punto de Control:** El Director de TIC, junto con los Subdirectores de acuerdo a la clasificación del Incidente, .evalúa y aprueban la realización de las actividades propuestas en la estrategia de atención al incidente.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
7	Profesional Líder Seguridad de la Información.	Asigna las tareas en la mesa de servicio a responsables de atención del incidente de seguridad.	Sistema de Mesa de Servicios por número de caso	
8	Profesional(es) responsable(s) de la ejecución de actividades para la atención del incidente de seguridad.	Ejecuta acciones y/o actividades necesarias para la: • Contención y mitigación inmediata, buscando minimizar su impacto y salvaguardar la información principal que está siendo afectada. • Erradicación de la causa raíz detectada del incidente de seguridad con el fin de controlar la vulnerabilidad explotada y la amenaza materializada. • Solución y remediación del incidente. • Recuperación o restauración según aplique. En caso de afectación de activo de información TI y de requerirse, activa el numeral 5.2 Restauración de copias de respaldo del Procedimiento para la Realización y Control de Copias de Respaldo (backups) – PGTI-03. Documentación en el	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 procesos y/o sistemas de información.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
		sistema de mesa de servicio las acciones ejecutadas.		
9	Profesional Especializado Líder Seguridad de la Información y Oficial de Seguridad.	Comprueban sí el incidente fue solucionado con las acciones ejecutadas. Documentan el caso en la mesa de servicio y en acta CSIRT. Informan a CSIRT que el incidente fue solucionado e indican recomendaciones. Sí la solución no es satisfactoria devuelve a la actividad 8.	Sistema de Mesa de Servicios por número de caso Acta CSIRT	**Observación:** Define la necesidad de convocar a sesión extraordinaria CSIRT según la complejidad de las acciones de atención y solución del incidente. El aprendizaje adquirido en el análisis y solución del incidente se gestionará de acuerdo a los lineamientos definidos por la Dirección de TIC con respecto a la gestión del conocimiento.

5.2 Recolección de evidencias en incidente de seguridad.

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
1	Director y/o Subdirector TIC	Comunica a Contralor y/o Contralor Auxiliar la necesidad de reportar el incidente de seguridad a entidad externa o autoridad competente.		

No.	RESPONSABLE	ACTIVIDAD	REGISTROS	PUNTOS DE CONTROL/ OBSERVACIONES
2	Oficial de Seguridad	Restringe acceso físico /lógico para evitar el acceso al área donde ocurrió el incidente y/o alteración de la posible evidencia. Acompaña a funcionario de entidad externa o autoridad competente en las actividades de recolección y entrega de evidencia. Documenta las acciones ejecutadas. Continúa con los protocolos y/o recomendaciones establecidos por entidad externa o autoridad competente para el trámite de la evidencia.	Acta	**Punto de control:** Las actividades ejecutadas se deben realizar en coordinación y acompañamiento de funcionario(s) responsable(s) de área(s) donde ocurrió el incidente y partes interesadas. **Observación:** Documenta los datos relacionados con la evidencia, entre otros aspectos la siguiente información: • ¿Dónde?, ¿cuándo? y ¿quién? descubrió, recolectó y manejó la evidencia. • ¿Quién ha custodiado la evidencia?, ¿cuánto tiempo?
3	Oficial de Seguridad	Entrega documentación o resultados de la actividad realizada a Comité CSIRT para continuar con procedimiento de gestión de incidentes de seguridad.	Acta y/o documentos soportes entregados por entidad externa o autoridad competente	**Observación:** El Líder de seguridad es el encargado de documentar en la mesa de servicio las acciones realizadas para atender el incidente de seguridad.

6. ANEXOS

ANEXO 1. Clasificación de Incidentes de Seguridad.

La clasificación de los incidentes de seguridad se debe realizar teniendo en cuenta los siguientes aspectos:

- **Impacto**: Establece la afectación del incidente seguridad a los activos de información, procesos, servicios y la importancia de los mismos para la organización.
- **Urgencia**: Define la celeridad de la atención según el retraso o bloqueo que se presente con el incidente de seguridad.
- **Prioridad:** Determina la importancia y los tiempos de respuesta según el impacto y la urgencia del incidente de seguridad.

IMPACTO	
Critico	Se considera crítico, cuando el incidente de seguridad presenta una o más de las siguientes afectaciones: • Afecta la integridad o disponibilidad o confidencialidad de los activos de información para la prestación de servicios al interior de la entidad o hacia la ciudadanía, que impida el cumplimiento de la misionalidad de la Entidad. • Daños a la imagen institucional por esta circunstancia. • Riesgo de demandas penales, económicas. • Riesgo de seguridad de la información. • Afecta la integridad humana.
Alto	Se considera alto, cuando el incidente de seguridad presenta una o más de las siguientes afectaciones: • Afecta la integridad o disponibilidad o confidencialidad de los activos de información para la prestación de servicios al interior de la entidad, que impida el cumplimiento de los objetivos de los procesos institucionales. • Daños a la imagen institucional por esta circunstancia. • Explotación de una vulnerabilidad sin materializar un riesgo de seguridad de la información. • Afecta el cumplimiento de los objetivos de los procesos institucionales.
Medio	Se considera medio, cuando el incidente de seguridad presenta una o más de las siguientes afectaciones: • Afecta la integridad o disponibilidad o confidencialidad de los activos de información no misionales que apoyan a los procesos de la entidad. • De alguna manera afecta los objetivo de los procesos institucionales.
Bajo	Se considera bajo, cuando el incidente de seguridad no afecta o afecta en mínima medida uno o más de los siguientes aspectos: • La integridad o disponibilidad o confidencialidad de los activos de información. • Cumplimiento de los objetivos institucionales. • Daños de imagen institucional. • La integridad humana. • Riesgo de demandas penales o económicas. • Explotación de vulnerabilidades o amenazas. • No hay materialización de riesgo de seguridad de la información.

Tabla No 1: Impacto

URGENCIA	
Inmediato	Presenta bloqueo total
Alto	Presenta bloqueo parcial
Medio	Presenta retraso que no implica bloqueo
Bajo	Mínimo retraso o no hay retraso

Tabla No 2: Urgencia

URGENCIA	IMPACTO			
	Bajo (1)	**Medio (2)**	**Alto (3)**	**Critico (4)**
Inmediato (4)	M	A	C	C
Alta (3)	B	M	A	C
Medio (2)	B	M	M	A
Baja (1)	B	B	B	M

Tabla No 3: Matriz de Prioridad

Prioridad	Tiempo de respuesta (solución) *horas laborales
Bajo (B)	<= 96 horas*
Medio (M)	Entre 32 – 48 horas*
Alto (A)	Entre 17 - 32 horas*
Critico (C)	Entre 0 – 16 horas consecutivas

Tabla No 4: Tiempo de atención según la prioridad

7. CONTROL DE CAMBIOS

Versión	R.R. No. Fecha Día mes año	Descripción de la modificación
1.0	RR No 047 28 Diciembre de 2018	Se ajustó el alcance incorporando la recolección de evidencias y se optimizaron las actividades del procedimiento, ajustando los responsables, observaciones y puntos de control, para dar mayor claridad al procedimiento. Se ajustaron las actividades para la evaluación, categorización y clasificación del incidente de seguridad y convocatoria de Equipo CSIRT. Unificación de actividades para atención del incidente. Se crea procedimiento 5.2 Recolección de evidencias en incidente de seguridad y se renumera el procedimiento de Gestión de Incidente de Seguridad. Se ajustó el Anexo No 1, determinando la clasificación del incidente de seguridad según el impacto y urgencia de atención.
2.0	**R.R. No. 016 Fecha 10-08-2020**	