1. OBJETIVO

Establecer actividades, criterios y condiciones necesarias para la prevención, detección, identificación, atención y aprendizaje de eventos e incidentes relacionados con la seguridad de la información.

2. ALCANCE

El procedimiento inicia con la identificación y reporte de eventos de seguridad de la información y finaliza con la actualización de bases de conocimiento y las lecciones aprendidas tras la ocurrencia de un incidente grave de seguridad de la Información o reuniones periódicas del equipo de gestión de incidentes

3. DEFINICIONES Y NIVELES DE SOPORTE

3.1 COLCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia.

3.2 CONSECUENCIA: Resultado de un evento que afecta a los objetivos [ISO/IEC 27000: 2014].

3.3 CRITERIOS DE DECISIÓN: Umbrales, objetivos, o patrones utilizados para determinar la necesidad de una acción o de una mayor investigación, o para describir el nivel de confianza en un resultado determinado. [ISO/IEC 27000: 2014]

3.4 ERISI: Equipo de Respuesta a Incidentes de Seguridad de la Información del Concejo de Bogotá.

3.5 EVENTO: Aparición o cambio de un conjunto particular de circunstancias. [ISO/IEC 27000: 2014]

3.6 EVENTOS EN SEGURIDAD DE LA INFORMACIÓN: Ocurrencia identificada de un sistema, servicio o estado de la red que indica una posible violación de la política de seguridad de la información o el fracaso de los controles, o una situación previamente desconocida que puede ser la pertinente a seguridad. [ISO/IEC 27000: 2014].

3.7 INCIDENTE EN SEGURIDAD DE LA INFORMACIÓN: Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de la organización y amenaza la seguridad de la información. [ISO/IEC 27000: 2014].

3.8 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: Procesos para detectar, informar, evaluar, responder, tratar, y aprender de los incidentes de seguridad de la información. [ISO/IEC 27000: 2014].

3.9 INVESTIGACIÓN FORENSE DE SEGURIDAD DE LA INFORMACIÓN: Aplicación de técnicas de investigación y análisis para recolectar registrar y analizar información de incidentes de seguridad de la información [ISO/IEC 27035: 2012].

3.10 PHISHING: suplantación de identidad, clonación de una página o abuso informático para adquirir información.

3.11 SNNIFER: Es un analizador de paquetes. Un programa de captura las tramas de una red de computadoras.

3.12 VIRUS TROYANO: Virus informático que ingresa al sistema a través de otro archivo.

3.13 GUSANO: Un gusano es un programa que se reproduce por sí mismo, que puede viajar a través de redes y difundirse a través de estas.

3.14 CONTENCIÓN: Acciones necesarias para garantizar la contención del incidente mientras se realiza un análisis más detallado y se definen las acciones necesarias para remediar el incidente.

3.15 REGISTRO: Documento que presenta resultados obtenidos o proporciona evidencia del desarrollo de las actividades desempeñadas.

3.16 NIVELES DE SOPORTE

- Nivel I: Equipo de mesa de ayuda.
- Nivel II: Oficial de seguridad.

4. APLICATIVOS, INSTRUCTIVOS, DOCUMENTOS Y FORMATOS UTILIZADOS

TIPO	TÍTULO DEL DOCUMENTO	CÓDIGO	No ACTIVIDAD	ORIGEN DEL DOCUMENTO	
				EXTERNO	INTERNO
Aplicativo	Aranda - Mesa de Ayuda	Electrónico	6.1, 6.9		X
Formato	Plan de Mejoramiento y Acciones Correctivas	GD-PR001-FO2	6.7		X
Formato	Eventos de Seguridad de la Información	SSI-PR007-FO1	6.1		X
Formato	Incidentes de Seguridad de la Información	SSI-PR007-FO2	6.2		X
Guía	Guía Gestión de Incidentes	SSI-GU002	6.4		X
Guía	Guía de Análisis Forense	SSI-GU003	6.6		X

5. RELACIÓN DE EMPLEOS QUE INTERVIENEN EN EL PROCEDIMIENTO

EMPLEO	CÓDIGO	GRADO	ÁREA
Profesional Especializado	222	04	Sistemas y Seguridad de la Información
Profesional Universitario	219	03	Sistemas y Seguridad de la Información
Auxiliar Administrativo	407	11 09	Sistemas y Seguridad de la Información
Todos servidores públicos, contratistas, visitantes y aquellos con acceso a la información del Concejo de Bogotá D.C.			

6. DESCRIPCIÓN DE ACTIVIDADES (RESPONSABLES Y FORMATOS)

6.1. IDENTIFICAR Y REPORTAR EVENTOS DE SEGURIDAD: Los servidores públicos, contratistas, visitantes y todo aquel que tenga acceso a la información del Concejo de Bogotá D.C. debe reportar eventos [SSI-PR007-FO1] técnicos o físicos que afecten la confidencialidad, integridad y/o disponibilidad de la información a través del aplicativo Aranda- Mesa de ayuda.

Nota 1: Si el evento de seguridad es detectado por visitantes o terceros que no tienen acceso al software de mesa de ayuda, se debe informar al servidor público que autoriza el ingreso o realiza el acompañamiento durante la estadía en las instalaciones del Concejo de Bogotá D.C. Asimismo, el evento podrá ser reportado mediante llamada telefónica al número (1) 2088210 extensión 884 o al número 018000112448.

Nota 2: Si el evento de seguridad impide el uso del software de mesa de ayuda, por ejemplo, por pérdida de conexión a Internet o por daños en la estación de trabajo, el evento podrá ser reportado autenticándose en la estación de trabajo de un compañero o mediante llamada telefónica al número (1) 2088210 extensión 884.

Nota 3: Es importante que el reporte sea lo más detallado posible y que incluya, de ser posible, evidencias tales como capturas de pantallas.

Al presentarse un evento en el que esté involucrado el equipo de cómputo, tener en cuenta las siguientes condiciones:

- No reiniciar el equipo.
- No apagar el equipo.
- Informar sobre los eventos ocurridos.
- Hacer capturas de pantallas de mensajes o errores de sistema desplegados en pantalla.

Nota 4: El proceso de Sistemas y Seguridad de la Información debe tener en cuenta que los siguientes componentes son fuentes generadoras de eventos de seguridad de la información:

- Alertas en sistemas de seguridad
- Caídas de servidores
- Logs de servidores, aplicaciones y herramientas de seguridad

6.2. EVALUAR EL EVENTO DE SEGURIDAD DE LA INFORMACIÓN: El equipo de soporte nivel I evalúa el evento reportado con el fin de decidir si corresponde a un incidente de seguridad de la

información. Si se determina que el evento no corresponde a un incidente de seguridad de la información, este será atendido de acuerdo con el procedimiento de atención de soporte tecnológico (SSI-PR003). Si el evento es catalogado como un incidente de seguridad de la información este deberá ser asignado al oficial de seguridad o delegado quien a su vez deberá asignar una categoría teniendo en cuenta las siguientes directrices y el formato Incidentes de Seguridad de la Información (SSI-PR007-FO2):

- **Denegación de servicio:** Pérdida de disponibilidad de sistemas, redes u otros servicios.
- **Ingeniería social:** Método de ataque en el que se engaña a un usuario para obtener acceso a sistemas de información y a información del Concejo de Bogotá D.C., mediante técnicas tales como phishing, llamadas telefónicas fraudulentas, mensajes de texto, entre otras.
- **Uso inadecuado de activos:** Violaciones a las políticas de uso aceptable de los activos.
- **Código malicioso:** Programas utilizados por usuarios malintencionados para obtener acceso no autorizado y control de equipos de cómputo, servidores, sistemas de información; capturar contraseñas o información confidencial tecleada por el usuario; secuestrar la información de equipos de cómputo, servidores, dispositivos móviles; entre otros. Esta categoría incluye virus informáticos, gusanos informáticos, ransomware, keyloggers, entre otros.
- **Acceso físico no autorizado:** Acceso no autorizado a las instalaciones del Concejo de Bogotá D.C.
- **Acceso lógico no autorizado:** Acceso no autorizado a sistemas de información, servidores, equipos de cómputo o dispositivos de red del Concejo de Bogotá D.C.
- **Datos personales:** Involucra la pérdida de confidencialidad, integridad y/o disponibilidad de activos relacionados con datos personales y su información asociada.
- **Escaneos, pruebas o intentos de obtener la información:** Técnicas utilizadas para la obtención de información privilegiada.

6.3. DETERMINAR EL NIVEL DE PRIORIDAD DEL INCIDENTE: Se debe determinar el nivel de prioridad del incidente, siguiendo las directrices de la guía de gestión de incidentes (SSI-GU002). El responsable de determinar el nivel de prioridad del incidente es el servidor público encargado de las funciones del Oficial de Seguridad.

6.4. ESCALAR EL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: En primera instancia se examina el incidente con ayuda de la base de conocimiento (incidentes resueltos anteriormente) y así aplicar la solución adecuada. Si la resolución del incidente se escapa de las posibilidades del equipo de soporte nivel I de la mesa de ayuda, ésta re-direcciona el caso a un nivel superior para su investigación, teniendo en cuenta el numeral 6.3 de la guía de gestión de incidentes (SSI-GU002).

6.5. PLANEAR LA RESPUESTA AL INCIDENTE: En caso de que el equipo de soporte no pueda atender el incidente, el plan de respuesta a incidentes debe considerar:

- La reunión y toma de decisiones del Equipo de Respuesta a Incidentes de Seguridad de la Información (ERISI), en caso de que el incidente se escape del alcance del personal de soporte o del oficial de seguridad de la información.
- Revisión de incidentes similares que se hayan presentado anteriormente para determinar si se pueden tomar las mismas acciones.
- El canal de comunicación con las partes interesadas involucradas en el incidente.

- Revisión de los procedimientos, planes de contingencia o protocolos que sean aplicables, para solucionar el incidente.
- Medidas de corrección para resolver el incidente.
- Acciones correctivas en caso de ser necesario.

Las estrategias para la resolución de incidentes pueden ser de tres tipos:

- **Contención:** Busca la detección del incidente con el fin de que no se propague y pueda generar más daños a la información o a la arquitectura de TI. Algunos ejemplos de actividades de contención son: bloqueo de cuenta después de sucesivos intentos de acceso o la desconexión de la red de un equipo infectado con malware.
- **Erradicación:** Busca eliminar cualquier rastro dejado por el incidente con acciones tales como: Reparación del sitio web después de un defacement, borrado seguro y restauración de un backup en un equipo infectado por malware, reinstalación del equipo y recuperación de datos cuando se detecta un rootkit.
- **Recuperación:** Restauración de los sistemas y/o servicios afectados para restablecer la funcionalidad de los mismos, y realizar un endurecimiento (hardening) del sistema que permita prevenir incidentes similares en el futuro.

NOTA: Durante todo el ciclo de vida del incidente se debe actualizar la información almacenada en las bases de datos correspondientes para que los implicados dispongan de información sobre el estado del mismo.

Si fuera necesario se puede emitir una solicitud de cambio, siguiendo las directrices del procedimiento de gestión de cambios [SSI-PR001].

6.5. COMUNICAR EL INCIDENTE: Es importante comunicar el incidente a las partes interesadas y, en caso de ser necesario, al Comité Directivo del SIG o a la Presidencia con el fin de que se tomen decisiones que se escapen del alcance del ERISI. El objetivo de esta actividad puede ser:

- Informar a los funcionarios y contratistas acerca de un ataque que esté ocurriendo en el Concejo de Bogotá D.C. y las precauciones que se deben tener.
- Informar a la Superintendencia de Industria y Comercio (SIC) acerca de incidentes que involucren datos personales.
- Promover la toma de decisiones que se escapan del alcance del ERISI.
- Informar a las partes interesadas acerca de la pérdida de disponibilidad de un servicio y el tiempo que tomará restaurarlo.

6.6. RECOLECTAR Y ANALIZAR LA EVIDENCIA DEL INCIDENTE: Para la resolución del incidente es necesaria la recolección de evidencia. Estas evidencias pueden provenir de diferentes fuentes, tales como:

- **Información basada en la red:** Logs de IDS o IPS, logs de monitoreo, logs de routers, logs de firewalls, información recolectada mediante Sniffers de red, información de servidores de autenticación.
- **Información Basada en el Equipo:**

- Live data collection: Volcado (dump) de la memoria RAM, fecha y hora del sistema, procesos activos, conexiones de red establecidas, puertos abiertos, aplicaciones escuchando en dichos puertos, estado de la tarjeta de red.
- Otra información: Testimonio de funcionario, contratista o tercero que reporta el evento.

NOTA 1: En caso de que se requiera hacer denuncias penales, se debe tener en cuenta el Directorio Contacto con Autoridades y Grupos de Interés el cual se encuentra documentado en el numeral 6.4 de la Guía de Gestión de Incidentes (SSI-GU002). Adicionalmente, es importante hacer una recolección y manejo adecuado de la evidencia; para ello, la entidad puede contactar al ColCERT, contratar un experto en el tema, o en caso de que se decida que personal de del proceso de Sistemas y Seguridad de la Información recolecte la evidencia se deberían tener en cuenta las directrices de la Guía de Análisis Forense (SSI-GU003).

NOTA 2: En caso de que se decida contactar al ColCERT porque algún componente de la infraestructura tecnológica (sitios Web, aplicaciones, servicios en línea, sistemas de información, entre otros) de la Entidad, haya sido vulnerado o comprometido, los datos para contactar al ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia) son: correo electrónico contacto@colcert.gov.co o al teléfono (+571) 2959897.

NOTA 3: Cuando se tenga evidencia de un incidente informático, contactar con el Cai Virtual de la Policía Nacional www.ccp.gov.co, Centro Cibernético Policial de la Policía Nacional al teléfono 4266900 ext. 104092, para recibir asesoría del caso en particular y posterior judicialización.

6.7. TRATAR EL INCIDENTE: Ejecutar las acciones definidas para tratar el incidente. Asegurarse de que todas las actividades de respuesta involucradas se registren en el software de mesa de ayuda para análisis posterior y registralos como hallazgo en un Plan de Mejoramiento [GD-PR001-FO2].

6.8. HACER SEGUIMIENTO AL INCIDENTE: El responsable del aplicativo de mesa de ayuda estará en contacto con las áreas involucradas y con el equipo de respuesta a incidentes de seguridad de la información (ERISI), para conocer y actualizar el estado del incidente.

6.9. CERRAR EL INCIDENTE: Antes de proceder a cerrar el caso, es necesario confirmar con el(los) usuario(s) la solución satisfactoria del mismo. Adicionalmente, se deben registrar, en el software de mesa de ayuda, los procedimientos aplicados para resolver el incidente. Adicionalmente, es importante verificar que se haya documentado por completo el tratamiento del mismo.

6.10. REGISTRAR LAS LECCIONES APRENDIDAS: Es necesario mantener un proceso de lecciones aprendidas después de un incidente grave, y semestralmente para analizar los incidentes menores, en el cual participen el ERISI y las demás partes interesadas que se considere deben asistir.

Se debe mantener un adecuado registro, en el software de mesa de ayuda, de lecciones aprendidas con el fin de conocer:

- Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
- Cuál sería la gestión de personal y qué debería hacerse la próxima vez que ocurra un incidente similar.
- Actualización de la matriz de riesgos.

- Acciones correctivas para prevenir incidentes similares en el futuro.
- Cuales herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.

7. BASE LEGAL

Ver Normograma de la Corporación (NTC-ISO/IEC 27001:2013 y Manual de Políticas de Seguridad de la Información).

8. POLÍTICAS DE OPERACIÓN

Ver manual de políticas de seguridad de la información

9. RESPONSABILIDADES OPERACIONALES

9.1. Es responsabilidad de los funcionarios, contratistas y todo aquel que tenga acceso a la información del Concejo de Bogotá D.C., reportar el incumplimiento de las políticas de seguridad de la información y cualquier otro evento que pueda atentar contra la confidencialidad, integridad y disponibilidad de la información.

9.2. Es responsabilidad de todos los funcionarios y contratistas que usan los servicios y sistemas de información de la Entidad, reportar cualquier debilidad de seguridad de la información observada o sospechada.

9.3. El equipo de respuesta a incidentes de seguridad de la información (ERISI) está conformado por:

- Oficial de seguridad de la información (Líder de equipo de atención a incidentes de seguridad de la información)
- Responsable del proceso de Sistemas y Seguridad de la Información.
- Administrador de servidores.
- Administrador de redes.

9.4. La primera medida para la gestión de incidentes es la prevención de los mismos mediante actividades tales como:

- Análisis periódico de riesgos.
- Auditorías periódicas.
- Aplicar las lecciones aprendidas de los eventos e incidentes de seguridad de la información para reducir la posibilidad o impacto de incidentes futuros.
- Realizar campañas periódicas de sensibilización a funcionarios y contratistas acerca de las políticas de seguridad de la información, procedimientos de seguridad de la información y lecciones aprendidas producto de la gestión de incidentes de seguridad de la información.
- Administración de actualizaciones.
- Aseguramiento (hardening) de servidores expuestos hacia internet.
- Seguridad en la red.
- Protección contra código malicioso.
- Gestión de vulnerabilidades técnicas.

10. RIESGOS Y CONTROLES
Ver Mapa de Riesgos

11. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA
01	Elaboración de Documento.	29-Sep.-2015
02	Modificación de las secciones 1 (Objetivo), 2 (alcance) y 3 (definiciones) del procedimiento. Reestructuración de la sección 6 (Actividades) del procedimiento. Modificación de la sección 8 (políticas de operación) del procedimiento.	27-Oct.-2017
03	Modificación título numeral 3 Modificación texto numerales 6.2 y 6.8. Se incluye texto en numerales 3.1, 3.4, 3.7, 3.16, 4, 6.2, 6.4, 6.6 y 9. Se elimina texto en numeral: 6.2 y 6.7	26-Jul.-2018

ELABORÓ:	REVISÓ:	APROBÓ:
Carlos Alberto Muñoz Torres Profesional Especializado 222-04 Jheisson Adrián Montaño Álvarez Profesional Universitario 219-03 Sistemas y Seguridad de la Información	Reynaldo Roa Parra Profesional Especializado 222-05 Oficina Asesora de Planeación	Jorge Luis Peñuela Ramos Director Administrativo