1. OBJETIVO

Establecer las actividades necesarias para gestionar de manera correcta los cambios requeridos en sistemas de Información, servicios, dispositivos y, en general, la infraestructura tecnológica del Concejo de Bogotá D.C.

2. ALCANCE

Inicia con la solicitud de cambio y finaliza con las directrices para la implementación de La Gestión de Cambios.

3. DEFINICIONES

3.1 ADMINISTRACIÓN o GESTIÓN DE CAMBIOS: Comprende la planeación, programación, pruebas y despliegue de nuevas configuraciones sobre la plataforma tecnológica.

3.2 CAMBIO: Referente a cualquier adición, eliminación, modificación temporal o permanente realizada a uno o varios activos que conforman la infraestructura tecnológica del Concejo de Bogotá D.C.

3.3 CAMBIO ESTANDAR: Referente a un cambio programado.

3.4 CAMBIO DE EMERGENCIA: Referente a un cambio de emergencia.

3.5 INFRAESTRUCTURA TECNOLÓGICA: La infraestructura tecnológica se encuentra integrada por un conjunto de elementos de hardware (servidores, puestos de trabajo, redes, enlaces de telecomunicaciones, etc.), software (sistemas operativos, bases de datos, lenguajes de programación, herramientas de administración, etc.) y servicios (soporte técnico, seguros, comunicaciones, etc.) que en conjunto dan soporte a las aplicaciones (sistemas informáticos) de la Corporación.

3.6 LIDER DE CAMBIOS: Funcionario que concede el aval para realizar o rechazar un cambio.

3.7 RESPONSABLE DEL CAMBIO: Funcionario o contratista encargado de la ejecución del cambio. El responsable del cambio es designado por el Proceso de Sistemas y Seguridad de la Información.

4. APLICATIVOS, INSTRUCTIVOS, DOCUMENTOS Y FORMATOS UTILIZADOS

TIPO	TÍTULO DEL DOCUMENTO	CÓDIGO	No ACTIVIDAD	ORIGEN DEL DOCUMENTO	
				INTERNO	EXTERNO
Formato	Solicitud de Cambio	SSI-PR012-FO1	6.1, 6.2	x	

5. RELACIÓN DE EMPLEOS QUE INTERVIENEN EN EL PROCEDIMIENTO

EMPLEO	CÓDIGO	GRADO	PROCESO
Profesional Especializado	222	04	Sistemas
Profesional Universitario	219	03	Sistemas
Auxiliar Administrativo	407	11 09	Sistemas

6. DESCRIPCIÓN DE ACTIVIDADES (RESPONSABLES Y FORMATOS)

6.1 IDENTIFICACIÓN DE CAMBIO: Cuando se detecta un cambio que puede tener impacto en la infraestructura tecnológica del Concejo de Bogotá D.C., se debe realizar la solicitud de cambio por medio del formato SSI-PR012-FO1.

6.2 ASIGNAR LA SOLICITUD DE CAMBIO: El solicitante del cambio debe conceder la solicitud al Profesional Especializado mediante el formato SSI-PR012-FO1.

6.3 ACEPTAR O RECHAZAR LA SOLICITUD DE CAMBIO: El Profesional Especializado decide si acepta la solicitud de cambio o la rechaza considerando que el cambio no está justificado o que algunos aspectos de la misma son susceptibles de mejora o mayor definición. En caso de que la solicitud de cambio sea rechazada se devuelve a quien realizó la solicitud y termina el procedimiento.

NOTA: La aceptación del cambio no implica su posterior aprobación por parte del Proceso de Sistemas y Seguridad de la Información.

6.4 CLASIFICAR Y PRIORIZAR LA SOLICITUD DE CAMBIO: El Profesional Especializado clasifica el cambio teniendo en cuenta la urgencia y el impacto del mismo en el(los) proceso(s) y a nivel de seguridad de la información, teniendo en cuenta lo siguiente:

Cambio estándar
Cambios programados que en ocasiones se pueden realizar en conjunto con otros cambios. En esta categoría se encuentran los cambios relacionados con:

+ Mantenimiento de la infraestructura o las aplicaciones.
+ Actualización paquetes de software para corregir problemas funcionales o vulnerabilidades de criticidad media o baja.
+ Implementación de nuevos servicios de TI.

Cambio de emergencia
El Líder de Cambios debe verificar la información para determinar si se trata o no de una emergencia. Estos cambios no son programados y deben clasificarse como cambios de emergencia siempre que se ajusten a alguno de los criterios definidos a continuación:

+ Cambios que si no se realizan impiden la prestación del servicio y/o la operación del negocio.
+ Cambios que deben realizarse debido a la presencia de una vulnerabilidad crítica conocida en software o firmware de la entidad.
+ Cambios que deben realizarse porque de no hacerlo, el Concejo de Bogotá D.C. puede incurrir en multas o costos financieros, por incumplimientos legales o contractuales.

Los cambios de emergencia se llevan a cabo de acuerdo con las directrices de la actividad 6.10.

NOTA: Si una solicitud de cambio es urgente y no es posible coordinar una reunión extraordinaria del Proceso de Sistemas y Seguridad de la Información se puede efectuar el cambio con la Autorización del Responsable del Proceso de Sistemas y Seguridad de la Información. En caso tal de que el Responsable del Proceso de Sistemas no esté disponible, la autorización del cambio queda a cargo del Dirección Administrativa.

6.5 ANALIZAR EL CAMBIO: El Profesional Especializado o delegado de Sistemas y Seguridad de la Información analiza y, aprueba o rechaza las solicitudes de cambio pendientes, considerando:

+ Beneficios esperados del cambio propuesto.
+ Costos asociados al proceso de cambio.
+ Riesgos de seguridad de la información asociados.
+ Recursos necesarios para llevar a cabo el cambio con garantías de éxito.
+ Tiempo estimado de ejecución del cambio.
+ Impacto general sobre la infraestructura tecnológica.
+ Nivel de afectación de la seguridad de la información.
+ Responsable del cambio.

Si la solicitud de cambio es rechazada termina el procedimiento.

6.6 DIVULGAR EL(LOS) CAMBIO(S): El Proceso de Sistemas y Seguridad de la Información divulga el cambio a realizar a todos los procesos que podrían ser afectadas o que se encuentran relacionadas con el mismo.

6.7 IMPLEMENTAR Y MONITOREAR EL CAMBIO: El responsable del cambio coordina la ejecución del cambio con el personal competente. Asimismo, el responsable del cambio monitorea el proceso para asegurar que:

+ Se ajusta a las especificaciones predeterminadas.
+ Se cumplen los calendarios previstos y la asignación de recursos es la adecuada.
+ El entorno de pruebas es realista y realiza una simulación adecuada.
+ Se ejecute el plan de retorno (rollback) en caso de ser necesario.
+ Se tiene en cuenta las sugerencias, se aclaran dudas y se da soporte a funcionarios, contratistas, proveedores y demás partes interesadas, según se requiera.

6.8 EVALUAR EL CAMBIO: Antes de proceder al cierre del cambio es necesario que el oficial de seguridad o delegado realice una evaluación del impacto del mismo en el Concejo de Bogotá D.C., teniendo en cuenta la seguridad de la información. Los aspectos fundamentales a considerar son:

+ Cumplimiento de los objetivos previstos del cambio.
+ Incidentes o interrupciones imprevistas.
+ Ejecución de planes de retorno (rollback) y sus causas.
+ Percepción de los funcionarios, contratistas y demás involucrados respecto al cambio.
+ Verificación de que se han cumplido los requisitos de seguridad de la información.

6.9 CERRAR LA SOLICITUD DE CAMBIO: Si la evaluación final determina que el proceso y los resultados han sido satisfactorios se procede al cierre del cambio por parte del líder de cambios. Adicionalmente, se debe comunicar a las partes interesadas (involucradas en el cambio) la finalización del mismo.

6.10 IMPLEMENTAR Y DOCUMENTAR CAMBIOS DE EMERGENCIA: Para la ejecución de cambios de emergencia, después de la aprobación del cambio por parte del Proceso de Sistemas y Seguridad de la Información de Emergencia o por parte del funcionario autorizado, el responsable del procesos de sistemas y seguridad de la información o el Director Administrativo. asigna el cambio a quien corresponda. Después de ejecutado el cambio, este debe ser registrado siguiendo los lineamientos normales del procedimiento, con el fin de que se evalúe el impacto del mismo en el Concejo de Bogotá D.C. y la seguridad de la información.

7. BASE LEGAL

Ver Normograma de la Corporación.

8. POLÍTICAS DE OPERACIÓN

Ver Manual de Políticas de Seguridad de la Información

9. GESTIÓN DE VULNERABILIDADES TÉCNICAS

9.1 Como parte de la gestión de vulnerabilidades técnicas la membrecía en grupos o foros de interés especial es requerida para:

- Mejorar el conocimiento acerca de las buenas prácticas y permanecer al día con la información de seguridad pertinente.
- Asegurar que la comprensión del entorno de la seguridad de la información sea actual y esté completa.

- Recibir advertencias tempranas de las alertas, avisos y parches acerca de ataques y vulnerabilidades.

Por los motivos anteriores, el Proceso de Sistemas y Seguridad de la Información debe mantener contacto con los siguientes grupos de interés.

Descripción	Organización	Contacto
Boletines de Seguridad de Microsoft	Security Tech Center - Microsoft	https://portal.msrc.microsoft.com/en-us/
Avisos de Seguridad para Sistemas GNU/Linux	Linux Security	http://www.linuxsecurity.com/content/section/3/170/
Noticias de Seguridad de Ubuntu	Ubuntu	https://www.ubuntu.com/usn/
Actualizaciones del Departamento de Seguridad Nacional	Homeland Security	https://www.dhs.gov/subscribe
Boletines y noticias de seguridad	Security Focus	http://www.securityfocus.com/
Comunidad Colombiana de Seguridad de la Información	DragonJAR	http://www.dragonjar.org/
Publicaciones de la División de Seguridad Informática del NIST	NIST	http://csrc.nist.gov/publications/subscribe.html

Descripción	Organización	Contacto
Base de Datos Nacional de Vulnerabilidades de Estados Unidos	National Vulnerability Database	https://nvd.nist.gov/Home/Email-List
Noticias diarias e información sobre seguridad informática, virus, criptología y antivirus.	Hispasec	http://unaaldia.hispasec.com/
Sitio de Seguridad Informática de Argentina que conforma la comunidad más grande de habla hispana sobre Seguridad de la Información	Segu-Info	http://www.segu-info.com.ar/
En el Blog de Eleven Paths (Filial de Telefónica dedicada a la ciberseguridad) se publica información relacionada con nuevas tecnologías de seguridad de la información y ciberseguridad	Eleven Paths	http://blog.elevenpaths.com/
El Lado del Mal es el blog donde Chema Alonso (el hacker de habla hispana más reconocido a nivel mundial) y otros autores publican artículos relacionados con seguridad informática	El Lado del Mal (Chema Alonso)	http://www.elladodelmal.com/

Descripción	Organización	Contacto
Información sobre alertas de seguridad y eventos de Ciberseguridad publicada por el Grupo de Respuesta a Emergencias Cibernéticas de Colombia	ColCERT	http://www.colcert.gov.co/?q=tags/alertas-de-seguridad http://www.colcert.gov.co/?q=blog-categories/eventos-de-ciberseguridad
Boletines y noticias de seguridad informática publicados por el CSIRT de la Policía Nacional	CSIRT - PONAL	https://cc-csirt.policia.gov.co/Publicaciones/Tema/alertas_y_tips https://cc-csirt.policia.gov.co/Publicaciones/Tema/Noticias
Boletines de Seguridad de VMware	VMware	http://www.vmware.com/security/advisories.html
Boletines de Seguridad de Oracle	Oracle	http://www.oracle.com/technetwork/es/topics/security/alerts-086861.html
Boletines de Seguridad CISCO	Cisco	https://tools.cisco.com/security/center/publicationListing.x
PSIRT Advisories	Fortinet	https://fortiguard.com/psirt

9.2 El Proceso de Sistemas y Seguridad de la Información está conformado por:

+ Responsable del Proceso (Profesional Especializado 222-04)
+ Oficial de Seguridad
+ Administrador(es) de servidores y redes (Profesional Universitario 219-03)
+ Administrador(es) de bases de datos (en caso de ser requerido)

9.3 Las responsabilidades del Proceso de Sistemas y Seguridad de la Información son:

+ Revisar, aceptar, aprobar o rechazar las solicitudes de cambio según se requiera.
+ Participar en el análisis de la solicitud de cambio según se requiera.

+ Designar el personal que se requiera para el análisis de la solicitud de cambio.

9.4 Las responsabilidades del Oficial de Seguridad en materia de Cambios son:

+ Hacer la revisión inicial de la solicitud de cambio con el fin de validar que el cambio es justificado y está bien documentado.
+ Registrar las solicitudes de cambio para aprobación.
+ Participar en el análisis de la solicitud de cambio según se requiera.
+ Convocar reuniones requeridas para revisar solicitudes de cambio.
+ Comunicar a las partes interesadas acerca del cambio a realizar.

10. RIESGOS Y CONTROLES
Ver Mapa de Riesgos

11. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA
01	Elaboración de Documento.	27-Oct.-2017
02	Se modifica texto numerales: 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.8, 6.9, 8. Se incluyen numerales: 3.3, 3.4, 3.7 y título numeral 9. Se eliminan notas de los numerales 6.5 y 6.7.	26-Jul.-2018
03	Se modifica el punto 4.	11 DIC 2018

ELABORÓ:	REVISÓ:	APROBÓ:
Carlos Alberto Muñoz Torres Profesional Especializado 222-04 Oficina Sistemas y Seguridad de la Información	Diana Carolina Avila Pinzón Profesional Universitario 219-03 Oficina Asesora de Planeación	Efvanni Paola Palmariny Peñaranda Directora Administrativa (E)