PROCEDIMIENTO		
Macroproceso - Proceso: Gestión Técnica y Tecnológica – Gestión de Seguridad de la Información	**Página:** 1 **de** 10	
Procedimiento: Emisión de Conceptos de Seguridad de la Información.	**Código:** FT0424P	**Versión:** 1

Objetivo del Procedimiento

Hacer que la Política de Seguridad de la Información de la Empresa de Acueducto se cumpla en todos los proyectos y contratos que gestionen información de la Empresa como sigue:

- Proyecto en formación,
- proceso en contratación,
- contrato en ejecución,

Normas que Rigen el Procedimiento

- Artículo octavo "Todos los procesos y proyectos que se desarrollen en el Acueducto de Bogotá, que involucren el manejo de información deberán incluir la revisión expresa y cumplimiento de los requisitos de seguridad de la información con el fin que se incorporen las acciones pertinentes para minimizar los riesgos asociados durante el ciclo de vida a la incorporación y cambios derivados de los nuevos proyectos." de la resolución 1127 de 2009 Políticas Generales de Seguridad de la Información de la Empresa de Acueducto y Alcantarillado de Bogotá.

Políticas Generales y Operación

1. El dueño del procedimiento es Líder de Servicios de Informática de la EAAB.
2. Cada proyecto que implique tratamiento de Información de la EAAB interno o externo, debe gestionar los riesgos de seguridad de la información orientados a lograr un nivel aceptable de mitigación, acatando la evaluación del Grupo de Seguridad de la Información – GSI y en concordancia con la gestión de riesgos establecida por MECI.
3. El promotor del proyecto / contrato es responsable por la elaboración y presentación a consideración del GSI el documento de especificaciones técnicas o el documento de gestión de riesgos de seguridad de la información según aplique.
4. El promotor del proyecto / contrato es responsable por la omisión de los documentos, de especificaciones técnicas de seguridad o de gestión de riesgos de seguridad, en el ciclo de vida de la solución.
5. Cada proyecto / contrato que involucre tratamiento de Información de la EAAB debe contar con un documento de gestión de riesgos expresamente aprobado por el GSI.
6. El GSI podrá solicitar las reuniones técnicas o ampliación escrita que considere necesarias para la evaluación del documento de gestión de riesgos de seguridad de la información.
7. Dependiendo del estado de evolución, de ejecución o de funcionamiento de proyectos que involucren gestión de información del Acueducto, se deben tomar en cuenta las siguientes instancias:
    - Los términos de referencia de la solicitud de contratación de los proyectos o procesos a contratar, deben incluir un capítulo o sección con los "requerimientos técnicos de seguridad" o en caso contrario debe figurar una nota expresa indicando que no aplica con el siguiente texto: "*El objeto del contrato no incluye el tratamiento de información de la Empresa de Acueducto*

o sus suscriptores o empleados o terceras partes y por lo tanto no aplica la política de seguridad de la información contenida en la resolución 1127/2009"

- Los contratos deben incluir en el plan de calidad el capítulo o sección presentando las actividades y sus resultados, referentes a la gestión de riesgo de seguridad de la información.
- Para la puesta en marcha y entrega de los productos o soluciones el contrato debe entregar al GSI un documento, clasificado como documento privado, que demuestre la evaluación y gestión de los riesgos de la información tratada en el contrato.
- Si el contrato / proyecto no consideró el presente procedimiento, el GSI deberá ser informado en el mismo instante en que se detecte la omisión, para proceder a cumplir con el presente procedimiento como requisito para entrar/ continuar en operación. Durante este tiempo, junto con el GSI, se analizarán los riesgos en el uso de la información para tomar las acciones conducentes a la mitigación del riesgo a niveles aceptables por la empresa. El GSI dispondrá de por lo menos un mes para el análisis y aprobación del documento. El Interventor / promotor será responsable por la elaboración del documento "evaluación y gestión de los riesgos de la información".
- Cada proyecto que entre en producción debe contar con un documento de riesgos gestionados con la aprobación de GSI, requerido dentro del proceso de control de cambios, la no existencia de este documento causará el rechazo del cambio por parte del GSI.
- Las áreas que traten información del Acueducto en el proyecto / contrato serán responsables de la gestión de riesgos durante el ciclo de vida de la solución implantada, de acuerdo con el procedimiento de gestión de riesgos del Acueducto.

Entradas

- Correo de solicitud de concepto.
- Inventario de nuevos proyectos, procesos en contratación y contratos en ejecución de TI con:
  - Cronograma.
  - Objetivo del proyecto/contrato
  - Descripción detallada del proyecto/contrato
  - Diagramas de red
  - Diagramas de flujo de información / casos de uso.
  - Diagramas de infraestructura actual con nombres de servidor o elementos de la infraestructura.
  - Diagramas de infraestructura propuesta con nombres de servidor o elementos de infraestructura.
  - Mapa de procesos afectados
  - Información de contactos técnicos
  - Documento de gestión de riesgos (no aplica para términos de referencia)
  - Lista de requerimientos de seguridad (no aplica para contratos ya ejecutados o en ejecución).

Documentos Relacionados

- FT0424F01 - Formato Conceptos de Seguridad

ACTIVIDADES	Parámetro de Control/ plazos máximos	Responsable	Documentos Relacionados
Caso 1: proyectos en formación o por iniciar trámites de contratación			**"Especificación técnica de seguridad a ser incluida en los términos de referencia"**
1.1 Solicitud de concepto		Promotor del proyecto o proceso de contratación	
1.2 El solicitante envía mediante correo electrónico dirigido al Líder de Seguridad de la Información, la solicitud de revisión por parte del GSI del documento de especificaciones técnicas relacionadas con las actividades de gestión de información del proyecto. Se debe anexar el cronograma propuesto detallando las tareas específicas esperadas, las fechas y los recursos a utilizar en la elaboración de la especificación técnica de seguridad que debe ser incluida en los términos de referencia.	Mínimo 1 mes antes de la radicación del proceso de contratación.	Líder de Seguridad de la Información	
1.3 El responsable del caso - GSI valida si el proyecto involucra Gestión de Información de propiedad del Acueducto. El Líder de Seguridad de la Información aprueba la solicitud y coordinará su inclusión en el cronograma interno y la fecha compromiso de entrega. El Líder de Seguridad de la Información responderá mediante correo informando el nombre de la persona responsable. Si no se aprueba la solicitud se da respuesta expresa y termina el procedimiento.	1 semana	Líder de Seguridad de la Información , El responsable del caso – GSI	

1.4 El responsable del caso - GSI podrá solicitar al Promotor la información técnica que requiera (Entradas) como requisito del cumplimiento del compromiso. Dejará constancia, con el Promotor, que el caso queda cerrado si no se ha recibido la información solicitada dentro del plazo establecido para la atención por parte del GSI. También será el responsable de mantener el registro de los casos y de la respuesta en el repositorio definido para ello.	1 semana para el Promotor	El responsable del caso – GSI	
1.5 El representante del GSI selecciona de la especificación técnica de seguridad vigente los ítems a incluir en los términos de referencia en función de los riesgos, referida en este procedimiento.	1 semana	El responsable del caso – GSI	
1.6 La lista de requerimientos redactada como texto constituirá el capítulo de seguridad del proyecto o proceso de contratación, que se deberá publicar por el promotor como fue aprobado por el GSI sin disminuciones ni cambios.		Promotor del proyecto o proceso de contratación	**"Especificación técnica de seguridad a ser incluida en los términos de referencia"**
1.7 Una vez se propongan los términos de referencia, el proyecto se contrate y pase a ejecución, el Promotor / Interventor debe hacer el seguimiento periódico, mantener y enviar copia del cumplimiento del capítulo de seguridad en los términos de referencia al GSI según lo establecido en la Actividad 2 a partir del numeral 2.5 como requisito para entrada en producción. El Interventor es responsable de mantener evidencia que ha informado y se han gestionado los riesgos en seguridad de la información.	Informe final: 1 semana antes de la entrada en producción o entrega de producto. Informes de seguimiento: con la frecuencia definida en el plan de calidad.	Promotor del proyecto o proceso de contratación	
1.8 Ir a caso 5.			

Caso 2: contratos en ejecución			**"evaluación y gestión de riesgos de la información"**
Solicitud de concepto		Interventor del contrato.	
2.1 El solicitante envía correo de solicitud de concepto del GSI en el contrato, dirigido al Líder de Seguridad de la Información. Se debe anexar el cronograma propuesto detallando las tareas específicas esperadas, las fechas y los recursos a utilizar.		Interventor del contrato.	
2.2 El responsable del caso - GSI evalúa si el proyecto involucra Gestión de Información de propiedad del Acueducto. El Líder de Seguridad de la Información aprueba la solicitud y coordinará su inclusión en el cronograma interno y la fecha compromiso de entrega. El Líder de Seguridad de la Información responderá mediante correo informando el nombre de la persona responsable. Si no se aprueba la solicitud se da respuesta expresa y termina el procedimiento.	1 semana	Líder de Seguridad de la Información , El responsable del caso – GSI	
2.3 El responsable del caso - GSI podrá solicitar al Interventor la información técnica que requiera (Entradas), como requerimiento del cumplimiento del compromiso. Dejará constancia, con el Promotor, que el caso queda cerrado si no se ha recibido la información solicitada dentro del plazo establecido para la atención por parte del GSI.	1 semana para el Interventor	El responsable del caso – GSI	
2.4 El responsable del caso - GSI evalúa el contrato y le presta asesoría al Interventor en la elaboración del documento "evaluación y gestión de riesgos de la información", en caso de que este documento no esté desarrollado mostrando la aplicación en el contrato. El responsable	1 semana	El responsable del caso – GSI	"evaluación y gestión de riesgos de la información"

del GSI con el Interventor lo revisa y actualiza / desarrolla a la luz de los objetivos del proyecto y la documentación técnica en función del riesgo y emite su concepto expreso.			
2.5 El Interventor del contrato debe hacer seguimiento de la ejecución con el fin de determinar si se implementaron los requerimientos de seguridad y es el responsable por la documentación y gestión de riesgos y por el balance y registro de los riesgos al momento de entrada en producción o puesta en marcha o de recibo final, y de entrega del documento como anexo de handover. Es decir, el Interventor debe emitir un documento tipo privado y oficial de gestión de riesgo de la información dirigido al GSI, a la Dirección del área interventora y al responsable de la operación del producto o servicio, donde se muestren el estado de los riesgos de seguridad a que está expuesto la información como resultado de la ejecución del contrato.	Informe final: 1 semana antes de la entrada en producción o entrega de producto. Informes de seguimiento: con la frecuencia definida en el plan de calidad.	Interventor del contrato.	
2.6 El Interventor del contrato es responsable por la gestión de riesgos de seguridad de la información de la solución que se haga hasta la entrega en producción según el procedimiento de gestión de riesgos de la EAAB.		Interventor del contrato.	
2.7 Ir a caso 6.			
Caso 3: contratos o proyectos implementados		Dueño de la solución implementada.	**"evaluación y gestión de riesgos de la información"**
3.1 Si el contrato se terminó de ejecutar y el producto o servicio resultante está implementado, y se detecta que no tiene desarrollado el documento "evaluación y gestión de riesgos de la información", el		El responsable del caso – GSI	

GSI debe rechazar cualquier cambio en la solución que afecte la seguridad de la información hasta que se desarrolle y complete con documento anexo el "handover" del cambio. Si el documento existe, el GSI debe analizarlo, emitir su concepto y terminar esta actividad.			
3.2 Si el documento no existe, el dueño envía correo al Líder de Seguridad de la Información, al dueño de la solución, al dueño del cambio y al Gestor de Cambios informando sobre la ausencia del documento. El dueño debe gestionar su elaboración y entrega al GSI.		El responsable del caso – GSI, Dueño de la solución implementada.	
3.3 El dueño de la solución desarrolla el documento de "evaluación y gestión de riesgos de la información" y lo adjunta al documento de cambio – RFC y vuelve a enviar la solicitud de cambio.	2 semanas	Dueño de la solución implementada.	"evaluación y gestión de riesgos de la información"
3.4 El dueño de la solución debe hacer seguimiento cercano con el fin de determinar si se implementaron los requerimientos de seguridad y es el responsable por la documentación y gestión de riesgos y por el balance final de los riesgos. Es decir, el Interventor debe emitir un documento tipo privado y oficial de gestión de riesgo de la información dirigido al GSI, a la Dirección del área interventora y al responsable de la operación del producto o servicio, donde se muestren el estado de los riesgos de seguridad a que está expuesto la información como resultado de la ejecución del contrato o proyecto.	RFC ajustado con matriz de riesgo: 1 semana	Dueño de la solución implementada.	
3.5 El dueño de la solución es responsable por la gestión de riesgos de seguridad de la información de la solución que se haga hasta su eliminación según el procedimiento de gestión de riesgos de la EAAB.		Dueño de la solución implementada.	

3.6 Ir a caso 6.			
Caso 4: proyectos internos en ejecución			**"evaluación y gestión de riesgos de la información"**
4.1 Solicitud de concepto		Promotor del proyecto.	
4.2 El solicitante envía correo de solicitud de concepto del GSI en el proyecto, dirigido al Líder de Seguridad de la Información. Se debe anexar el cronograma propuesto detallando las tareas específicas esperadas, las fechas y los recursos a utilizar.		Promotor del proyecto.	
4.3 El responsable del caso - GSI evalúa si el proyecto involucra gestión de Información de propiedad del Acueducto. El Líder de Seguridad de la Información aprueba la solicitud y coordinará su inclusión en el cronograma interno y la fecha compromiso de entrega. El Líder de Seguridad de la Información responderá mediante correo informando el nombre de la persona responsable. Si no se aprueba la solicitud se da respuesta expresa y termina el procedimiento.	1 semana	El Líder de Seguridad de la Información , El responsable del caso - GSI	
4.4 El responsable del caso - GSI podrá solicitar al solicitante la información técnica que requiera (Entradas), como requerimiento del cumplimiento del compromiso. Dejará constancia, con el Promotor, que el caso queda cerrado si no se ha recibido la información solicitada dentro del plazo establecido para la atención por parte del GSI.	1 semana para el Promotor	El responsable del caso - GSI	
4.5 El responsable del caso - GSI evalúa el proyecto y le presta asesoría al Interventor en la elaboración del documento "evaluación y gestión de riesgos de la	1 semana	El responsable del caso – GSI	

información", en caso de que este documento no esté desarrollado mostrando la aplicación en el contrato. El responsable del GSI con el Interventor lo revisa y actualiza / desarrolla a la luz de los objetivos del proyecto y la documentación técnica en función del riesgo y emite su concepto expreso.			
4.6 El solicitante debe hacer seguimiento de la ejecución con el fin de determinar si se implementaron los requerimientos de seguridad y es el responsable por la documentación y gestión de riesgos y por el balance y registro de los riesgos al momento de entrada en producción o puesta en marcha o de recibo final, y de entrega del documento como anexo de handover. Es decir, el Interventor debe emitir un documento tipo privado y oficial de gestión de riesgo de la información dirigido al GSI, a la Dirección del área interventora y al responsable de la operación del producto o servicio, donde se muestren el estado de los riesgos de seguridad a que está expuesto la información como resultado de la ejecución del proyecto.	Informe final: 1 semana antes de la entrada en producción o entrega de producto. Informes de seguimiento: con la frecuencia definida en el plan de calidad.	Promotor del proyecto.	
4.7 El Solicitante es responsable por la gestión de riesgos de seguridad de la información de la solución que se haga hasta la entrega en producción según el procedimiento de gestión de riesgos de la EAAB.		Promotor del proyecto.	
4.8 Ir a caso 6.			
Caso 5: proyectos en formación o contratación. Documenta y cierra procedimiento.			
5.1 El responsable del GSI dejará constancia en el repositorio de evaluaciones de seguridad de la entrega y del documento "especificaciones técnicas de seguridad"	2 semanas	El responsable del GSI	FT0424F01 - Formato Conceptos de Seguridad

para el caso de proyectos en formación o en contratación. También mantendrá actualizado el registro de casos atendidos			
Caso 6: contratos o proyectos en ejecución o ya ejecutados. Documenta y cierra procedimiento.			
6.1 El responsable del GSI asigna un consecutivo, sustenta y almacena en los repositorios oficiales todos los documentos relacionados con el documento emitido "evaluación y gestión de riesgos de la información" que entrega al dueño o responsable el documento e informa al GSI sobre el cambio en el repositorio.	2 semanas	El responsable del GSI	
6.2 El responsable del GSI actualiza la matriz de riesgos de la información de Acueducto en el repositorio con los riesgos residuales resultantes de la gestión de riesgos de seguridad de la información.		El responsable del GSI	FT0424F01 - Formato Conceptos de Seguridad