Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (Documento "Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información")

Objetivos

1. DEI - (Detección Electrónica de Infracciones)
2. REGISTRO_BICI_BOGOTÁ
1. SIMUR PORTAL - (Portal Sistema de Información)
2. SIRC
3. Todas las Aplicaciones - (DATACENTER CALLE 13)
4. Todas las Aplicaciones - (REDES).

Estrategias

1. Análisis de Vulnerabilidades sobre las aplicaciones y servidores de la Entidad
2. Aplicación de Política de WSUS servidores Registrobicibogota y SIRC
3. Campañas de Sensibilización y Cultura de Seguridad
4. Definición de complementación de Guías de Hardening SO (De acuerdo a Alcance)
5. Implementar Cifrado de Información, (Contraseñas, Datos PC)
6. Plan de Contingencia PRT Registrobicibogota y SIRC
7. Plan de continuidad
8. Política protección de puestos desatendidos.
9. Políticas de Backup y Restauración
10. Remediación de Vulnerabilidades RegistrobiciBogota y SIRC
11. Revisión de Lista Blanca SIRC
12. Sistemas de acceso seguro a aplicaciones.
13. Validación e Instalación de antivirus Servidores Registrobicibogota y SIRC
14. Verificación de Accesos Registro Bici Bogota y SIRC
15. Verificación de Información
16. Verificación e implementación de WAF Registrobicibogota y SIRC

Proyectos y Metas

CÓDIGO RUBRO PRESUPUESTAL Y/O PROYECTO	OBJETO	VALOR TOTAL ESTIMADO (APROPIACIÓN VIGENTE ACTUAL) PREDIS	META
3-3-1-15-07-44-0967-192	PRESTAR LOS SERVICIOS PROFESIONALES ESPECIALIZADOS A LA OFICINA DE INFORMACIÓN SECTORIAL PARA APOYAR LAS ACTIVIDADES DE PLANIFICACIÓN, CONTROL, SEGUIMIENTO Y ESTRUCTURACIÓN DE LA IMPLEMENTACIÓN DE CONTROLES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	89.413.000	17. Implementar el 100 % de la estrategia anual para la sostenibilidad del Subsistema de Gestión Seguridad de la Información.

Acciones /Actividades

1. Campañas de concientización puestos desatendidos, escritorio limpio, uso de dispositivos externos.
2. Definición del modelo de Gestión e Continuidad SDM.
3. Definir PRT para las aplicaciones de negocio Registrobicibogota y SIRC
4. Realizar Plan de pruebas
5. Definir guías de aseguramiento para los SO más utilizados en la SDM.
6. Aplicar Guía de Aseguramiento Aplicaciones Registro Bicibogota y SIRC (Servidores que aplique)
7. Definir pan de Remediación para cerra las brechas de seguridad identificada a nivel de SO y Aplicación de registro Bicibogota y SIRC.
8. Pasar RFC para actividades de remediación de vulnerabilidades Registrobicibogota y SIRC
17. Definir política de gestión y actualización del WSUS, frente a servidores Registro Bicibogota y SIRC
18. Implementar actualización en esquema defino para los servidores Bicibogota y SIRC
19. Diseñar - plantear e implementar brigadas de Puestos de trabajo Seguro Colaboradores
20. Definir y solicitar espacios de fortalecimiento de cultura de seguridad en las inducciones de personal nuevo de la SDM
21. Documentar el plan de continuidad para eventos menores e intermedios.
22. Levantamiento de Información de IP autorizadas.
23. Plan de revisión configuración de roles y usuarios aplicaciones críticas SDM.
24. Realizar Análisis de Riesgos.
25. Definir y realizar seguimiento a los planes de mitigación
26. Realizar validación de inspección de tráfico de la aplicación registrobicibogota, por medio de un WAF.

27. Realizar validación y mitigación de vulnerabilidades de Denegación de servicio identificadas sobre las aplicaciones de registrobicibogota y SIRC
28. Realizar Validación de Políticas y/o Ejecución de backup sobre aplicación RegistroBicibogota y SIRC
29. Documentar e implementar procedimiento de restauración de copias de respaldo aplicación RegistroBicibogota y SIRC
30. Realizar validación equipos e información que requiere cifrado bajo el servicio de Registrobiciboogta.
31. Implementar procedimientos de cifrado.
32. Realizar Verificación de Usuarios locales (Servidores, aplicaciones, BD),
33. Realizar Verificación y/o levantamiento de matriz de accesos usuarios aplicación Registro_bici_Bogotá
34. Validación e instalación de antivirus Sophos Servidores entorno productivo (Aplicación y base de datos), registrobicibogota y SIRC
35. Verificación y/o creación de Manuales de administración de capa Media y Servidores sobre la aplicación Registrobicibogota

Productos

1. Cumplimiento de actividad de la fase de implementación del Modelo de Seguridad y Privacidad de la Información para el 2019

Responsables

1. Oficina de Tecnologías de la Información y comunicaciones / Operador tecnológico

Cronogramas

objetivo	Estrategia	Acción
DEI - (Detección Electrónica de Infracciones)	Análisis de Vulnerabilidades sobre las aplicaciones y servidores de la Entidad	1. Realizar Análisis de Riesgos. 2 Definir y realizar seguimiento a los planes de mitigación
	Total Análisis de Vulnerabilidades sobre las aplicaciones y servidores de la Entidad	
	Plan de continuidad	1. Documentar el plan de continuidad para eventos menores e intermedios.
	Total Plan de continuidad	
Total DEI - (Detección Electrónica de Infracciones)		
REGISTRO_BICI_BOGOTÁ	Aplicación de Política de WSUS servidores Registrobicibogota y SIRC	1. Definir política de gestión y actualización del WSUS, frente a servidores Registro Bicibogota y SIRC 2. Implementar actualización en esquema defino para los servidores Bicibogota y SIRC
	Total Aplicación de Política de WSUS servidores Registrobicibogota y SIRC	
	Campañas de Sensibilización y Cultura de Seguridad	1. Diseñar - plantear e implementar brigadas de Puestos de trabajo Seguro Colaboradores 2. Definir y solicitar espacios de fortalecimiento de cultura de seguridad en las inducciones de personal nuevo de la SDM
	Total Campañas de Sensibilización y Cultura de Seguridad	
	Definición e complementación de Guías de Hardening SO (De acuerdo a Alcance)	1. Definir guías de aseguramiento para los SO más utilizados en la SDM. 2. Aplicar Guía de Aseguramiento Aplicaciones Registro Bicibogota y SIRC (Servidores que aplique).
	Total Definición e complementación de Guías de Hardening SO (De acuerdo a Alcance)	
	Implementar Cifrado de Información, (Contraseñas, Datos PC)	1. Realizar validación equipos e información que requiere cifrado bajo el servicio de Registrobicibogota. 2. Implementar procedimientos de cifrado.
	Total Implementar Cifrado de Información, (Contraseñas, Datos PC)	
	Plan de Contingencia PRT Registrobicibogota y SIRC	
	Total Plan de Contingencia PRT Registrobicibogota y SIRC	
	Políticas de Backup y Restauración	1. Realizar Validación de Políticas y/o Ejecución de backup sobre aplicación RegistroBicibogota y SIRC 2. Documentar e implementar procedimiento de restauración de copias de respaldo aplicación RegistroBicibogota y SIRC
	Total Políticas de Backup y Restauración	
	Remediación de Vulnerabilidades RegistrobiciBogota y SIRC	1. Definir pan de Remediación para cerra las brechas de seguridad identificada a nivel de SO y Aplicación de registro Bicibogota y SIRC. 2. Pasar RFC para actividades de remediación de vulnerabilidades Registrobicibogota y SIRC 3. Realizar actividades de
	Total Remediación de Vulnerabilidades RegistrobiciBogota y SIRC	
	Validación e Instalación de antivirus Servidores Registrobicibogota y SIRC	1. Validación e instalación de antivirus Sophos Servidores entorno productivo (Aplicación y base de datos), registrobicibogota y SIRC
	Total Validación e Instalación de antivirus Servidores Registrobicibogota y SIRC	
	Verificación de Accesos Registro Bici Bogota y SIRC	1. Realizar Verificación de Usuarios locales (Servidores, aplicaciones, BD), Aplicación Registro_Bici_Bogot. 2. Realizar Verificación y/o levantamiento de matriz de accesos usuarios aplicación Registro_bici_Bogotá
	Total Verificación de Accesos Registro Bici Bogota y SIRC	
	Verificación de Información	1. Verificación y/o creación de Manuales de administración de capa Media y Servidores sobre la aplicación Registrobicibogota
	Total Verificación de Información	
	Verificación e implementación de WAF Registrobicibogota y SIRC	1. Realizar validación de inspección de trafico de la aplicación registrobicibogota, por medio de un WAF. 2. Realizar validación y mitigación de vulnerabilidades de Denegación de servicio identificadas sobre las aplicaciones de registrobicibogota y SIRC
	Total Verificación e implementación de WAF Registrobicibogota y SIRC	
Total REGISTRO_BICI_BOGOTÁ		
SIMUR_PORTAL - (Portal Sistema de Información)	Política protección de puestos desatendidos.	1. Campañas de cocientización puestos desatendidos, escritorio limpio, uso de dispositivos externos.
	Total Política protección de puestos desatendidos.	
	Sistemas de acceso seguro a aplicaciones.	1. Plan de revisión configuración de roles y usuarios aplicaciones críticas SDM.
	Total Sistemas de acceso seguro a aplicaciones.	
Total SIMUR_PORTAL - (Portal Sistema de Información)		
SIRC	Aplicación de Política de WSUS servidores Registrobicibogota y SIRC	1. Definir política de gestión y actualización del WSUS, frente a servidores Registro Bicibogota y SIRC 2. Implementar actualización en esquema defino para los servidores Bicibogota y SIRC
	Total Aplicación de Política de WSUS servidores Registrobicibogota y SIRC	
	Campañas de Sensibilización y Cultura de Seguridad	1. Diseñar - plantear e implementar brigadas de Puestos de trabajo Seguro Colaboradores 2. Definir y solicitar espacios de fortalecimiento de cultura de seguridad en las inducciones de personal nuevo de la SDM
	Total Campañas de Sensibilización y Cultura de Seguridad	
	Definición e complementación de Guías de Hardening SO (De acuerdo a Alcance)	1. Definir guías de aseguramiento para los SO más utilizados en la SDM. 2. Aplicar Guía de Aseguramiento Aplicaciones Registro Bicibogota y SIRC (Servidores que aplique).
	Total Definición e complementación de Guías de Hardening SO (De acuerdo a Alcance)	
	Implementar Cifrado de Información, (Contraseñas, Datos PC)	1. Realizar validación equipos e información que requiere cifrado bajo el servicio de Registrobicibogota. 2. Implementar procedimientos de cifrado.
	Total Implementar Cifrado de Información, (Contraseñas, Datos PC)	
	Plan de Contingencia PRT Registrobicibogota y SIRC	
	Total Plan de Contingencia PRT Registrobicibogota y SIRC	
	Políticas de Backup y Restauración	1. Realizar Validación de Políticas y/o Ejecución de backup sobre aplicación RegistroBicibogota y SIRC 2. Documentar e implementar procedimiento de restauración de copias de respaldo aplicación RegistroBicibogota y SIRC
	Total Políticas de Backup y Restauración	
	Remediación de Vulnerabilidades RegistrobiciBogota y SIRC	1. Definir pan de Remediación para cerra las brechas de seguridad identificada a nivel de SO y Aplicación de registro Bicibogota y SIRC. 2. Pasar RFC para actividades de remediación de vulnerabilidades Registrobicibogota y SIRC 3. Realizar actividades de
	Total Remediación de Vulnerabilidades RegistrobiciBogota y SIRC	
	Revisión de Lista Blanca SIRC	1. Levantamiento de Información de IP autorizadas. 2. Revisión con SDM, sobre las IP autorizadas (Diego Armando Torres y Maria Alendra pardo)
	Total Revisión de Lista Blanca SIRC	
	Validación e Instalación de antivirus Servidores Registrobicibogota y SIRC	1. Validación e instalación de antivirus Sophos Servidores entorno productivo (Aplicación y base de datos), registrobicibogota y SIRC
	Total Validación e Instalación de antivirus Servidores Registrobicibogota y SIRC	
	Verificación de Accesos Registro Bici Bogota y SIRC	1. Realizar Verificación de Usuarios locales (Servidores, aplicaciones, BD), Aplicación Registro_Bici_Bogot. 2. Realizar Verificación y/o levantamiento de matriz de accesos usuarios aplicación Registro_bici_Bogotá
	Total Verificación de Accesos Registro Bici Bogota y SIRC	
	Verificación de Información	1. Verificación y/o creación de Manuales de administración de capa Media y Servidores sobre la aplicación Registrobicibogota
	Total Verificación de Información	
	Verificación e implementación de WAF Registrobicibogota y SIRC	1. Realizar validación de inspección de trafico de la aplicación registrobicibogota, por medio de un WAF. 2. Realizar validación y mitigación de vulnerabilidades de Denegación de servicio identificadas sobre las aplicaciones de registrobicibogota y SIRC
	Total Verificación e implementación de WAF Registrobicibogota y SIRC	
Total SIRC		
Todas las Aplicaciones - (DATACENTER CALLE 13)	Campañas de Sensibilización y Cultura de Seguridad	1. Diseñar - plantear e implementar brigadas de Puestos de trabajo Seguro Colaboradores 2. Definir y solicitar espacios de fortalecimiento de cultura de seguridad en las inducciones de personal nuevo de la SDM
	Total Campañas de Sensibilización y Cultura de Seguridad	
	Plan de continuidad	1. Documentar el plan de continuidad para eventos menores e intermedios.
	Total Plan de continuidad	
Total Todas las Aplicaciones - (DATACENTER CALLE 13)		
Todas las Aplicaciones - (REDES)	Plan de continuidad	1. Documentar el plan de continuidad para eventos menores e intermedios.
	Total Plan de continuidad	
	Política protección de puestos desatendidos.	1. Campañas de cocientización puestos desatendidos, escritorio limpio, uso de dispositivos externos.
	Total Política protección de puestos desatendidos.	
Total Todas las Aplicaciones - (REDES)		
(en blanco)	(en blanco)	(en blanco)
	Total (en blanco)	

Planes de compras con fuentes de financiación

Código Fuente Financiación	DESCRIPCIÓN	VALOR INICIAL PROGRAMADO Desde Anteproyecto 2019
118-MULTAS	PRESTAR LOS SERVICIOS PROFESIONALES ESPECIALIZADOS A LA OFICINA DE INFORMACIÓN SECTORIAL PARA APOYAR LAS ACTIVIDADES DE PLANIFICACIÓN, CONTROL, SEGUIMIENTO Y ESTRUCTURACIÓN DE LA IMPLEMENTACIÓN DE CONTROLES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	89.413.000

Distribución presupuestal de los proyectos de inversión

LINEA PAA CLASIFICADA SUBSECRETARÍAS (CDPs)	Código Rubro Presupuestal y/o Proyecto	DESCRIPCIÓN	VALOR INICIAL PROGRAMADO Desde Anteproyecto 2019
SGC-148	3-3-1-15-07-44-0967-192	PRESTAR LOS SERVICIOS PROFESIONALES ESPECIALIZADOS A LA OFICINA DE INFORMACIÓN SECTORIAL PARA APOYAR LAS ACTIVIDADES DE PLANIFICACIÓN, CONTROL, SEGUIMIENTO Y ESTRUCTURACIÓN DE LA IMPLEMENTACIÓN DE CONTROLES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	89.413.000

Indicadores

Sección No. 1: PROGRAMACIÓN VIGENCIA _2018_						
1. NÚMERO	2. ACTIVIDADES PRIMARIAS	3. PONDERACIÓN ACTIVIDAD PRIMARIA	4. No.	5. ACTIVIDADES SECUNDARIAS	6. PONDERACIÓN ACTIVIDAD SECUNDARIA	7. FECHA ESTIMADA DE EJECUCIÓN
1	CONSOLIDAR EQUIPO TÉCNICO	30%	1	Contratación equipo de trabajo trimestre II	30%	abr-19
TOTAL MAGNITUD VIGENCIA		100,00%	TOTAL		30%	

Mapas de riesgos

ESTABLECIMIENTO DEL CONTEXTO	VALORACIÓN DEL RIESGO									
OBJETIVOS INSTITUCIONALES	IDENTIFICACIÓN DEL RIESGO				ANÁLISIS DEL RIESGO INHERENTE					EVALUACIÓN DEL RIESGO INHERENTE
	CAUSA(S) RAÍZ	EVENTO POTENCIAL	CONSECUENCIAS	TIPOLOGÍA (Gestión o Corrupción)	PROBABILIDAD (Consulte la tabla de probabilidad)	IMPACTO (Consulte las tablas de impacto corrupción/gestión)	NP	NI	NPR	ZONA DE RIESGO (Consulte la matriz de calificación)
	1: Deficiencia en la metodología y el control para recopilación y consolidación de la información. 2: Manipulación de la información 3: Bajos estándares éticos	**6. Efectuar la rendición de cuentas sin contar con la información pertinente y veraz buscando un beneficio particular.**	1: Ciudadanía insatisfecha 2: Investigaciones disciplinarias, administrativas, fiscales y penales. 3: Sanciones	Corrupción-Visibilidad	RARA VEZ	MAYOR	1	10	10	BAJA
6EST. Proveer un ecosistema adecuado para la innovación y adopción de tecnologías de movilidad y de información y comunicación.	1: Falta de planeación presupuestal 2: Inadecuada identificación de la arquitectura empresarial de TICs, acorde con las necesidades de la Entidad. 3: Falta de liderazgo y continua rotación de la alta dirección 4: Existencia de tecnología obsoleta de difícil integración	**13. Adopción de tecnologías obsoletas, inadecuadas o incompatibles para las necesidades de la movilidad de la ciudad.**	1: Afectación negativa del servicio y de la gestión de la Entidad. 2: Detrimento patrimonial. 3: Incompatibilidad con nuevas tecnologías, inconvenientes para realizar integraciones. 4. Pérdida de imagen institucional 5. Investigaciones disciplinarias, administrativas, fiscales y penales.	Gestión	POSIBLE	MAYOR	3	10	30	ALTA
6SIG. Establecer e implementar estándares que contribuyan a la seguridad de la información de la Secretaría Distrital de Movilidad.	1: Falta de liderazgo y compromiso en la Alta Dirección 2: Insuficiencia en recursos humanos, tecnológicos, económicos 3: Deficiencia en controles para garantizar el cumplimiento de la política 4: Falta de divulgación de la política y estándares.	**20. Implementación de la Política de Seguridad de la Información deficiente e ineficaz para las características y condiciones de la Entidad.**	1: Perdida de información 2: Vulneración de la confidencialidad, disponibilidad e integridad de la información 3: Investigaciones y sanciones 4: Pérdida de imagen institucional 5: Detrimento patrimonial	Gestión	IMPROBABLE	CATASTRÓFICO	2	20	40	ALTA