

PLAN INSTITUCIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2022

TC-PL-03

Oficina de Tecnologías de la Información
y las Comunicaciones

24/01/2022

Versión 1

Contenido

1. OBJETIVO PRINCIPAL DEL PLAN	5
2. RESULTADOS AUTODIAGNOSTICO	5
3. RESPONSABLE DE LA EJECUCIÓN DEL PLAN	7
4. RESPONSABLE DEL MONITOREO DEL PLAN	7
5. RESPONSABLE DEL SEGUIMIENTO DEL PLAN	7
6. DETALLE DEL PLAN	7
7. CONTROL DE CAMBIOS.....	8
8. PRESUPUESTO	8

Tablas

Tabla 1 - Evaluación efectividad de controles	6
Tabla 2 - Control de Cambios	8

Ilustraciones

Ilustración 1 - Diagnostico del MSPI	6
--	---

1.OBJETIVO PRINCIPAL DEL PLAN

Elaborar el Plan de Seguridad y Privacidad de la Información del Instituto Distrital de Gestión de Riesgos y Cambio Climático – IDIGER, dando cumplimiento al Decreto 612 de 2018 para trazar y planificar la manera como la entidad continuará con la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

2.RESULTADOS AUTODIAGNOSTICO

Se realiza una actualización al diagnóstico al Modelo de Seguridad y Privacidad de la Información (MSPI) durante el mes de diciembre de 2021, la herramienta contempla los 114 controles de los 14 dominios que componen la Norma ISO 27001:2013.

De acuerdo con los resultados se evidencia que en la entidad se requiere una identificación de los riesgos de seguridad de la información que permitan identificar las zonas de riesgos asociadas a los activos de información.

Existen documentos como políticas y guías que deben ser actualizados, igualmente para los activos de información, se requiere su actualización y publicación.

Actualmente no se cuentan con métricas y mediciones que den cuenta de los avances del plan de Seguridad de la Información.

Se requiere la implementación del Sistema de Gestión de Seguridad de la Información con el fin de establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información en la entidad para asegurar el cumplimiento de sus objetivos.

Debido a que el Sistema de Gestión de Seguridad de la Información (SGSI) afecta a los objetivos de la entidad, se requiere que todas las acciones futuras y las decisiones que se tomen sólo puedan ser desarrolladas por la alta dirección de la organización.

Es un error común que el SGSI sea considerado como una cuestión netamente tecnológica o técnica de los niveles operativos de la entidad. Por eso es muy importante el compromiso de la alta dirección en la implementación, establecimiento, operación, monitorización, mantenimiento, revisión y mejora del SGSI a través de las siguientes iniciativas:

- Mantener actualizada una política de seguridad de la información.
- Garantizar el cumplimiento de planes y objetivos del SGSI.
- Identificar los roles y responsabilidades de seguridad de la información.
- Divulgar en la entidad la importancia de alcanzar los objetivos de seguridad de la información y de cumplir con la política de seguridad.
- Designar todos los recursos necesarios para llevar a cabo el SGSI.
- Determinar todos los criterios de aceptación de riesgos y sus correspondientes niveles.
- Asignar los recursos suficientes para todas las fases del SGSI.
- Garantizar que se realicen todas las auditorías internas.

A continuación, se resumen las calificaciones por cada uno de los dominios de la norma ISO 27001:2013:

Tabla 1 - Evaluación efectividad de controles

DOMINIO	Calificación Actual
POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	30
SEGURIDAD DE LOS RECURSOS HUMANOS	26
GESTIÓN DE ACTIVOS	28
CONTROL DE ACCESO	14
CRIPTOGRAFÍA	10
SEGURIDAD FÍSICA Y DEL ENTORNO	15
SEGURIDAD DE LAS OPERACIONES	56
SEGURIDAD DE LAS COMUNICACIONES	49
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	36
RELACIONES CON LOS PROVEEDORES	60
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	63
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	37
CUMPLIMIENTO	66
PROMEDIO	36

Adicionalmente se muestra gráficamente como están los dominios de seguridad de la información.

Ilustración 1 - Diagnostico del MSPI



3. RESPONSABLE DE LA EJECUCIÓN DEL PLAN

Para la ejecución del presente plan el responsable será como primera línea de defensa la Oficina de Tecnologías de la Información y las Comunicaciones. En el archivo en formato Excel *TIC-Plan de Seguridad y Privacidad de la Información.xlsx* en la hoja "Seguimiento Trimestral" se reportará el avance de la ejecución de este plan.

4. RESPONSABLE DEL MONITOREO DEL PLAN

Para el monitoreo del presente plan el responsable será la segunda línea de defensa la Oficina Asesora de Planeación. En el archivo en formato Excel *TIC-Plan de Seguridad y Privacidad de la Información.xlsx* en la hoja "Seguimiento Trimestral" se reportará el monitoreo de este plan.

5. RESPONSABLE DEL SEGUIMIENTO DEL PLAN

Para el seguimiento del presente plan el responsable será la tercera línea de defensa la Oficina de Control Interno. En el anexo en formato Excel *TIC-Plan de Seguridad y Privacidad de la Información.xlsx* en la hoja "Seguimiento Trimestral" se reportará el seguimiento de este plan.

6. DETALLE DEL PLAN

El detalle del Plan Institucional el cual contiene: vigencia, responsable principal de la ejecución del plan, objetivo del plan, actividades, producto o entregable, dependencia responsable de ejecutar la actividad, política MIPG que aplica, cronograma semanal para incluir las magnitudes a ejecutar por actividad, total de actividades programadas y una segunda hoja para reportar el avance trimestral de la primera línea de defensa, el monitoreo de la segunda línea de defensa y el seguimiento de la tercera línea de defensa. Se encuentra en el anexo en formato Excel *TIC-Plan de Seguridad y Privacidad de la Información.xlsx* en la hoja "Plan 2022" se reportará el seguimiento de este plan.

7.CONTROL DE CAMBIOS

Tabla 2 - Control de Cambios

Control de Cambios		
Versión	Fecha	Descripción de la Modificación
1	24/01/2021	Versión Inicial

8.PRESUPUESTO

Los recursos disponibles para el desarrollo de este plan están definidos en el proyecto de inversión “7558- FORTALECIMIENTO Y MODERNIZACIÓN DE LA GESTIÓN INSTITUCIONAL DEL IDIGER EN BOGOTÁ” aprobado en el Plan Anual de Adquisiciones 2022.

Elaboró	Revisó	Aprobó
Andrés Daza Cardona Contratista Oficina TICS	María Eugenia Tovar Rojas Jefe Oficina Asesora de Planeación	Comité de Gestión y Desempeño