PLAN DE CAPACITACIÓN, SENSIBILIZACIÓN Y COMUNICACIÓN DE SEGURIDAD DE LA INFORMACIÓN

PROCESO GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES

FECHA DE APROBACIÓN

(Mediante Acta No. 13 del 08/04/2025 de Comité Institucional de Gestión y Desempeño con radicado No.20251700195103)

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Tabla de Contenido

1. Introducción 3
2. Alineación Estratégica 3
3. Diagnóstico 4
4. Objetivo General 5
5. Objetivos Específicos 6
6. Vigencia 6
7. Beneficiarios 6
8. Responsables 6
9. Definiciones 7
10. Línea de acción o componente 8
11. Seguimiento 9
12. Instancia que aprueba 10
13. Cronograma de actividades 10
14. Anexos 11
15. Control de Cambios 11
16. Responsables de elaboración, revisión y aprobación 12

1. Introducción

La resolución 1978 de 2023 del Ministerio de Tecnologías de la Información y las Comunicaciones por la cual se adopta la Versión 3 del Marco de Referencia de Arquitectura Empresarial para el Estado Colombiano como el instrumento para implementar el habilitador de arquitectura de la Política de Gobierno Digital y se dictan otras disposiciones, establece los lineamientos generales de la Política de Gobierno Digital que deberán adoptar las entidades pertenecientes a la administración pública, encaminados hacia la transformación digital y el mejoramiento de las capacidades TIC. Dentro de la política se detalla el Habilitador de Arquitectura, el cual contiene todas las temáticas y productos que deberán desarrollar las entidades en el marco del fortalecimiento de las capacidades internas de gestión de las tecnologías, así mismo el Marco de Arquitectura Empresarial V 3.0 que es uno de los pilares de este habilitador.

Por lo tanto este plan busca establecer la estrategia y actividades enfocadas a fortalecer la cultura organizacional en Seguridad y Privacidad de la Información de la Secretaría de Cultura Recreación y Deporte, en adelante identificada con la sigla SCRD, mediante la divulgación de buenas prácticas para el adecuado tratamiento de la información, con el fin que los funcionarios y contratistas generen conciencia y se apropien de la importancia de contar con información segura y confiable para el cumplimiento y desarrollo de los objetivos misionales de la Entidad.

2. Alineación Estratégica

Misión

Liderar la formulación e implementación concertada de políticas públicas en arte, cultura, patrimonio, recreación y deporte, así como la transformación y sostenibilidad cultural y deportiva de la ciudad, garantizando los derechos culturales, reconociendo a los habitantes de Bogotá como creadores, agentes de cambio y el centro de todas nuestras acciones en la construcción de una ciudad creadora, cuidadora, consciente e incluyente.

Visión

En el 2030, la Secretaría de Cultura, Recreación y Deporte será reconocida como líder en la transformación cultural de la ciudad, con capacidad de adaptación a las dinámicas de la ciudad, la democracia cultural, la inclusión de la dimensión recreo-deportiva y cultural, consolidando la internacionalización cultural y deportiva con la participación de creadores y gestores del sector, donde la cultura, el arte, el patrimonio, la recreación y el deporte seguirán siendo fundamentales en la calidad de vida de los habitantes de Bogotá, forjando una ciudad más consciente, incluyente y cuidadora.

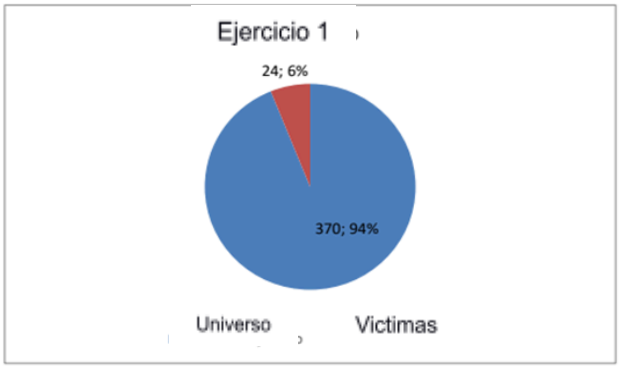
Objetivo Estratégico

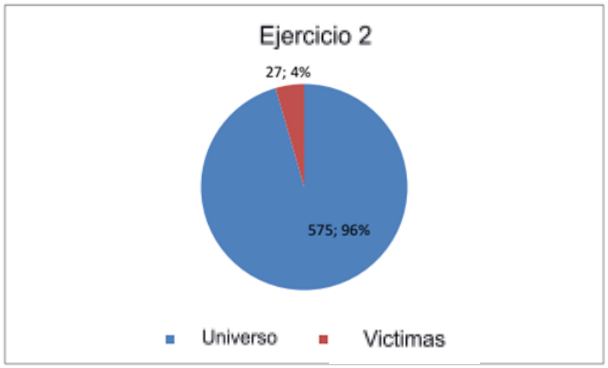
Objetivo estratégico No. 3. Generar una cultura inteligente institucional y sectorial, centrada en el uso de las tecnologías de la información y las comunicaciones y, la mejora continua de saberes, conocimientos y habilidades del talento humano de las entidades, para comprender las necesidades de la ciudadanía, adaptándose a las transformaciones de la sociedad para la toma de decisiones informadas, creativas e innovadoras.

3. Diagnóstico

En esta fase se identifican necesidades y prioridades para la formulación del presente Plan, teniendo en cuenta los resultados de dos ejercicios de Phishing que se realizaron durante la vigencia 2024 en la entidad, con los cuales mediante el envío de correo electrónico con simulación de Phishing se obtuvo como resultado que de un universo de 370 personas en el primer ejercicio y de 575 en el segundo, hubo un porcentaje en ambos ejercicios de 5% posible de víctimas potenciales en la SCRD, lo cual puede llegar a incidir en fuga de información de la entidad y/o ingreso de archivos maliciosos.

Imagen No. 1 Resultados ejercicios Phishing 2024





Fuente elaboración propia SCRD

La problemática central que se estableció fue la necesidad de reforzar las capacitaciones, sensibilizaciones y comunicaciones al personal de la entidad sobre seguridad de la información para evitar que se ponga en riesgo la información de la SCRD.

Lo anterior es importante abordarlo a través de actividades que contengan temas como phishing, protección de datos personales, descarga de software, copias de seguridad, contraseñas seguras entre otros, para con ello contribuir a disminuir los riesgos relacionados con Confidencialidad (divulgación de información no autorizada), Integridad (información que no es precisa, coherente y completa) y Disponibilidad (falta de acceso a la información cuando se requiera por parte de quien esté habilitado para ello).

4. Objetivo General

Diseñar, planificar y ejecutar actividades que contribuyan a concientizar a la comunidad institucional acerca de la importancia y aplicación de lineamientos relacionados con la Seguridad de la información dentro de la SCRD.

5. Objetivos Específicos

- Realizar mínimo 6 capacitaciones y/o sensibilizaciones a los funcionarios públicos y contratistas de la SCRD sobre seguridad de la Información.
- Realizar mínimo un ejercicio de Phishing o suplantación de identidad.
- Llevar a cabo una prueba de caso a toda la comunidad Institucional sobre la seguridad de la Información en la SCRD.
- Divulgar a la comunidad institucional tips de seguridad de la información y/o los boletines que sean recibidos por parte del CSIRT, mínimo en 6 ocasiones.

6. Vigencia

El presente Plan será implementado durante la vigencia 2025, con plazo de 15 de diciembre.

7. Beneficiarios

El Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información está dirigido a todos los funcionarios y contratistas de la SCRD.

8. Responsables

El encargado de la verificación de la ejecución del Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información de la SCRD es el jefe de la Oficina de la OTI.

9. Definiciones

Apropiación: Es el ejercicio consciente y permanente de las personas para proteger los activos de información que tiene a su cargo. Lograr este nivel de interiorización, pasa por aceptar e incorporar dentro de las creencias personales y de la entidad que la información es tan valiosa como los elementos visibles de la misma y que marcan la diferencia, frente al ejercicio estratégico y su relación con sus grupos de interés.

Concienciación: Busca que las personas en el contexto de la entidad se hagan conscientes de los riesgos y amenazas frente a la protección de la información, que entiendan los impactos y beneficios de su papel en la protección de esta.

Confidencialidad: Es la propiedad que determina que la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Cultura de Seguridad de la Información: Se define como la totalidad de los atributos humanos tales como comportamientos, actitudes y valores, además establece tres elementos claves que la constituyen: la concienciación, la apropiación y el cumplimiento; los cuales están constituidos por comportamientos que motivan la protección de la información.

Cumplimiento: Está relacionado con la adherencia a las políticas, procedimientos y prácticas de seguridad de la información. Es el entendimiento práctico de los comportamientos esperados por la entidad respecto de la protección de la información, los cuales son sujetos de auditoría y verificación con el fin de conocer el nivel de observancia de los individuos al cuerpo normativo, así como la forma de mantenerse sintonizado con la mejores prácticas nacionales e internacionales en los temas de seguridad de la información.

Disponibilidad: Es la propiedad de acceso y utilización de la información por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Integridad: Es la propiedad de la información de mantenerse precisa, coherente y completa desde su creación hasta su destrucción.

PCSCSI: Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información.

CSIRT: Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad Informáticas, es el equipo que provee las capacidades de gestión de incidentes a una organización/sector en especial.

10. Línea de acción o componente

El presente plan de capacitación, sensibilización y comunicación de seguridad de la información, será implementado bajo los siguientes lineamientos:

10.1. Capacitaciones y/o sensibilizaciones

Serán dictadas por los Ingenieros de la OTI y/o por entes externos, y se realizará divulgación mediante correos electrónicos y banners publicados en la Cultunet con el apoyo de la Oficina de Comunicaciones.

10.2. Ejercicio de Phishing o suplantación de identidad

Estará a cargo de la OTI y se realizará mediante el envío de correo electrónico a toda la comunidad institucional.

10.3. Encuesta de percepción

Estará a cargo de la OTI. Se realizará el diseño y envío de un formulario de Google forms, mediante el cual se solicitará a la comunidad institucional su diligenciamiento con el fin de saber y obtener la percepción de la Seguridad de la información en la SCRD.

Luego de la tabulación de la información recolectada se realizará mejora continua en las estrategias de capacitación y socialización.

10.4 Divulgación Tips de seguridad y/o boletines CSIRT

Estará a cargo de la OTI. Se realizará el diseño y envío de tips mediante correo electrónico, banners y noticias de actualidad publicados en la Cultunet con el apoyo de la Oficina de Comunicaciones.

Los boletines de seguridad recibidos por parte del CSIRT se socializarán a través de correo electrónico a toda la comunidad institucional.

11. Seguimiento

El seguimiento a la ejecución del Plan se realizará cuatrimestralmente, tal como se indica en el cronograma de actividades.

- **Seguimiento Estratégico**

El seguimiento estratégico será realizado como mínimo de manera cuatrimestral para el seguimiento de la segunda línea de defensa, a través de los formatos DES-PR-11-FR-01 V1 Formulación, seguimiento y monitoreo de los planes institucionales y estratégicos y DES-PR-11-FR-02 “INFORME EJECUTIVO DE GESTIÓN DEL PLAN”, de acuerdo con lo establecido en la “GUÍA PARA LA FORMULACIÓN, SEGUIMIENTO Y EVALUACIÓN DE PLANES INSTITUCIONALES”.

- **Seguimiento Operativo**

El seguimiento de este plan se realizará cuatrimestralmente (a mediados de abril, agosto y diciembre de 2025) , de lo cual se dejará acta de reunión, verificando los avances de las actividades formuladas en el plan, para lo cual el indicador será: (No. de actividades realizadas/No. de actividades programadas)*100.

12. Instancia que aprueba

La Instancia que aprueba el Plan de Seguridad y Privacidad de la información es el Comité Institucional de Gestión y Desempeño.

13. Cronograma de actividades

Tabla No. 1 Cronograma de Actividades

Actividad	Fecha Inicio	Fecha Fin	Responsable
Realizar mínimo 2 capacitaciones y/o sensibilizaciones por cuatrimestre a los funcionarios públicos y contratistas de la SCRD sobre seguridad de la Información	01/04/2025	15/12/2025	OTI
Realizar mínimo 1 ejercicio de Phishing o suplantación de identidad.	02/05/2025	30/08/2025	OTI
Llevar a cabo una prueba de caso a toda la comunidad Institucional sobre la seguridad de la Información en la SCRD.	1/11/2025	30/11/2025	OTI

Actividad	Fecha Inicio	Fecha Fin	Responsable
Divulgar a la comunidad institucional tips de seguridad de la información y/o los boletines que sean recibidos por parte del CSIRT, mínimo en 6 ocasiones.	1/04/2025	15/12/2025	OTI

Fuente: Elaboración propia SCRD

14. Anexos

Anexo 1. Formato para la formulación, seguimiento y monitoreo de los planes institucionales y estratégicos DES-PR-11-FR-01

15. Control de cambios

Versión	Fecha de Emisión	Cambios realizados
1	**27/10/2021**	Versión inicial del documento GOT-PN-01 v1 con radicado 20211600328203 del 27/10/2021
2	**28/06/2022**	Ver Solicitud de elaboración, modificación o eliminación de documento / Radicado: 20221600227283: Fecha: 21/06/2022
3	**08/04/2025**	Ver Solicitud de creación, modificación o eliminación de documento radicada en GLPI con el caso número 118649 del 18/03/2025. Las principales modificaciones tuvieron que ver con la inclusión de los ítems: Alineación estratégica, Diagnóstico, Vigencia, Beneficiarios, Líneas de acción, Instancia que aprueba y Anexos, debido a la actualización de la plantilla para formulación de planes. También se actualizó el cronograma de actividades teniendo en cuenta lo programado para la vigencia 2025.

16. **Responsables de elaboración, revisión y aprobación**

ELABORÓ	APROBÓ	VALIDÓ	AVALÓ
NOMBRE: Nidia Patricia Rodríguez	NOMBRE: Javier Mariño navarro	NOMBRE: Nelsón Velandia	NOMBRE: Comité Institucional de Gestión y Desempeño
CARGO: Contratistas OTI	CARGO: Jefe OTI	CARGO: Profesional Oficina de Planeación	CARGO: Comité Institucional de Gestión y Desempeño
FIRMA: Firmado Electrónicamente	FIRMA: Firmado Electrónicamente	FIRMA: Firmado Electrónicamente	FIRMA: Firmado Electrónicamente

Radicado: **20251600205013**
Fecha 29-04-2025 13:01

El Documento 20251600205013 fue firmado electrónicamente por:	
Luis Fernando Mejia Castro	**Jefe Oficina Asesora de Planeación**, Oficina Asesora de Planeación, ID: 79558456, luis.mejia@scrd.gov.co, Fecha de Firma: 07-05-2025 15:09:42
Nelson Javier Velandia Castro	**Profesional Universitario**, Oficina Asesora de Planeación, ID: 79905104, nelson.velandia@scrd.gov.co, Fecha de Firma: 07-05-2025 12:35:59
Javier Enrique Mariño Navarro	**Jefe Oficina de Tecnologías de la Información**, Oficina de Tecnologías de la Información, ID: 91474000, javier.marino@scrd.gov.co, Fecha de Firma: 29-04-2025 16:14:40
Nidia Patricia Rodriguez Rodriguez	**Contratista**, Oficina de Tecnologías de la Información, ID: 51930241, nidia.rodriguez@scrd.gov.co, Fecha de Firma: 29-04-2025 13:28:29
a9f987a872e20a64a3e8a05d1b882347fc4151899d3617ef11d9d0049d9ca5a8 Codigo de Verificación CV: 3c855	