Servicio Público de Empleo

UNIDAD ADMINISTRATIVA ESPECIAL DEL SERVICIO PÚBLICO DE EMPLEO

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C
2026

Nombre del documento	Política de Seguridad y Privacidad de la Información	
Estado del documento	Versión liberada	
Responsables	**Nombre y Cargo**	**Entidad**
	Elaboró: Jorge Iván Alexis Díaz Bernal - Profesional Especializado **Aprobó:** Libertad Cordoba Varón – Subdirectora de Desarrollo y Tecnología	Unidad Administrativa Especial del Servicio Público de Empleo -SPE

Control de Versiones del Documento

Versión	Creación/ modificación	Liberación	Descripción Cambio
1.0	Diciembre 2018	Enero 2019	Versión inicial
2.0	Enero 2020	Enero 2020	Actualización
3.0	Enero 2021	Enero 2021	Actualización
4.0	Enero 2022	Enero 2022	Actualización
5.0	Enero 2023	Enero 2023	Actualización
6.0	Junio 2024	Junio 2024	Actualización general de forma y fondo del documento, conforme a la normatividad técnica vigente y las mejores prácticas.
7.0	Enero 2025	Enero 2025	Actualización de los documentos técnicos, el estado actual, la estrategia y las actividades de seguridad de la información.
8.0	Enero 2026	Enero 2026	Actualización de actividades 2026

Servicio Público de Empleo

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

La transformación digital del Estado colombiano constituye un eje estratégico para el fortalecimiento de la relación entre las entidades públicas y la ciudadanía, orientado a la generación de valor público, la mejora en la prestación de servicios y el incremento de la confianza digital. En este contexto, el Plan Nacional de Desarrollo 2022–2026 establece la necesidad de consolidar un Estado moderno, eficiente y confiable, soportado en el uso responsable, seguro y estratégico de las tecnologías de la información y las comunicaciones.

En desarrollo de lo anterior, el Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la Política de Gobierno Digital, define los lineamientos para que las entidades públicas adopten modelos de gestión que integren la gobernanza, la innovación pública digital y los habilitadores transversales, dentro de los cuales la seguridad y privacidad de la información se reconoce como un componente esencial para garantizar servicios digitales confiables, decisiones basadas en datos y la protección de los derechos de los ciudadanos en el entorno digital.

La seguridad y privacidad de la información se implementa como habilitador transversal de la Política de Gobierno Digital, en articulación con el Marco de Referencia de Arquitectura Empresarial y el Modelo de Seguridad y Privacidad de la Información, los cuales proporcionan un marco estructurado para la gestión integral de los activos de información, la mitigación de riesgos, la continuidad de los servicios y el fortalecimiento de las capacidades institucionales. Este enfoque permite que la seguridad de la información trascienda el ámbito técnico y se consolide como un elemento de gobierno, gestión y control al servicio de los objetivos misionales de la entidad.

En concordancia con los lineamientos establecidos en la Resolución 500 de 2021 y demás normativa aplicable, la Unidad Administrativa Especial del Servicio Público de Empleo adopta el presente Plan Estratégico de Seguridad de la Información como instrumento de planeación institucional, orientado a articular políticas, procedimientos, controles, responsabilidades y actividades que permitan proteger la confidencialidad, integridad, disponibilidad y trazabilidad de los activos de información, tanto digitales como físicos, bajo un enfoque de gestión del riesgo y mejora continua.

El presente documento establece el marco estratégico que orienta la implementación de la seguridad y privacidad de la información en la entidad, alineando las acciones institucionales con la arquitectura empresarial, la gobernanza de tecnologías de la información y los objetivos de la Política de Gobierno Digital. De esta manera, el plan contribuye al fortalecimiento de la confianza digital, la continuidad operativa, la protección de datos personales y la generación de valor público, asegurando que la seguridad de la información se consolide como un habilitador clave para el cumplimiento de la misión institucional y la prestación de servicios a los ciudadanos.

2. OBJETIVO

Fortalecer de manera progresiva y sostenible la seguridad y privacidad de la información de la Unidad Administrativa Especial del Servicio Público de Empleo, garantizando la confidencialidad, integridad, disponibilidad y trazabilidad de los activos de información, mediante la gestión integral del riesgo, la

implementación de controles técnicos, organizacionales y procedimentales, y la consolidación de capacidades institucionales, en concordancia con la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información y el Marco de Referencia de Arquitectura Empresarial del MinTIC, con el fin de habilitar servicios digitales confiables, apoyar la toma de decisiones basadas en datos y generar valor público durante la vigencia del plan estratégico.

3. ALCANCE

El Plan Estratégico de Seguridad de la Información aplica a todos los procesos, áreas, funcionarios, contratistas y terceros que gestionen, administren o utilicen activos de información de la Unidad Administrativa Especial del Servicio Público de Empleo, independientemente de su formato, medio o soporte, incluyendo información digital, física y verbal.

El alcance del plan comprende la identificación, clasificación, protección y tratamiento de los activos de información, los sistemas de información, las infraestructuras tecnológicas, los servicios digitales institucionales y los datos personales bajo custodia de la entidad, así como la gestión de riesgos, incidentes de seguridad, continuidad y recuperación ante desastres.

De igual manera, el plan se articula con los dominios de la Arquitectura Empresarial definidos en el Marco de Referencia de Arquitectura Empresarial del MinTIC —arquitectura de negocio, información, aplicaciones y tecnología— y actúa como habilitador transversal de la Política de Gobierno Digital, apoyando el cumplimiento normativo, el fortalecimiento de la gobernanza institucional, la confianza digital y la mejora continua de los servicios orientados a los ciudadanos y grupos de valor.

4. NORMATIVIDAD APLICABLE

A continuación, se relaciona normativa aplicable para la estructuración del Plan Estratégico de Seguridad de la Información:

Tabla 1. Normatividad Técnica Vigente, Fuente: Modificado de *(Guía, s.f.)*

NORMATIVA	DESCRIPCIÓN
Constitución Política de Colombia de 1991	Artículo 15. Derecho a su intimidad personal (Datos Personales).
Constitución Política de Colombia de 1991	Artículo 20. Difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial.
Ley 527 del Congreso de Colombia de 1999	Comercio Electrónico y Firma Electrónica.
Ley 1955 de 2019	Establece que las entidades del orden nacional deberán incluir en su plan de acción el componente de transformación digital, siguiendo los estándares que para tal efecto defina el Ministerio de Tecnologías de la Información y las Comunicaciones.
Ley 693 Congreso de Colombia de 2000	Derechos de Autor.

NORMATIVA	DESCRIPCIÓN
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado *"de la protección de la información y de los datos"* y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712 de 2014	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
Decreto 1413 de 2017	En el Capítulo 2 Características de los Servicios Ciudadanos Digitales, Sección 1 Generalidades de los Servicios Ciudadanos Digitales
Decreto 2150 de 1995	Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.
Decreto 235 de 2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
Decreto 2364 de 2012	Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012" o Ley de Datos Personales.
Decreto 2433 de 2015	Por el cual se reglamenta el registro de TIC y se subroga el título 1 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las Comunicaciones.
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Decreto 2106 del 2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública. Cap. II Transformación Digital Para Una Gestión Publica Efectiva
Decreto 620 de 2020	Establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Decreto 767 de 2022	Por medio del cual se actualiza la Política de Gobierno Digital.
Resolución 500 de 2021	Lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital
Resolución 2710 de 2017	Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.

NORMATIVA	DESCRIPCIÓN
Resolución 3564 de 2015	Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
Resolución 3564 de 2015	Reglamenta algunos artículos y parágrafos del Decreto número 1081 de 2015 (Lineamientos para publicación de la Información para discapacitados).
Norma Técnica Colombiana NTC 5854 de 2012	Accesibilidad a páginas web El objeto de la Norma Técnica Colombiana - NTC 5854 es establecer los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en los niveles de conformidad: A, AA, y AAA.
CONPES 3292 de 2004	Señala la necesidad de eliminar, racionalizar y estandarizar trámites a partir de asociaciones comunes sectoriales e intersectoriales (cadenas de trámites), enfatizando en el flujo de información entre los eslabones que componen la cadena de procesos administrativos y soportados en desarrollos tecnológicos que permitan mayor eficiencia y transparencia en la prestación de servicios a los ciudadanos.
CONPES 3920 de Big Data de 2018	Política de Big Data.
CONPES 3854 Política Nacional de Seguridad Digital de Colombia de 2016	Política Nacional de Seguridad Digital.
CONPES 3975	Política Nacional de Transformación Digital e Inteligencia Artificial.
Circular 02 de 2019	Avanzar en la transformación digital del Estado e impactar positivamente la calidad de vida de los ciudadanos generando valor público en cada una de las interacciones digitales entre ciudadano y Estado y mejorar la provisión de servicios digitales de confianza y calidad.
Directiva 02 de 2019	Moderniza el sector de las TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.
Resolución No 500 de 2021	Lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad como habilitador de la Política de Gobierno Digital.

5. DOCUMENTOS TÉCNICOS DE SEGURIDAD DE LA INFORMACIÓN

La Unidad Administrativa Especial del Servicio Público de Empleo dispone de un conjunto de documentos técnicos que soportan la gestión integral de la seguridad y privacidad de la información, los cuales se articulan con el Sistema Integrado de Gestión y constituyen el marco operativo para la implementación del presente Plan Estratégico de Seguridad de la Información.

Estos documentos establecen políticas, procedimientos, formatos y planes que permiten operacionalizar la estrategia de seguridad de la información, asegurando la identificación, protección y uso adecuado de los activos de información, la gestión de riesgos, la atención de incidentes y la continuidad de los servicios institucionales. Asimismo, facilitan la trazabilidad, el control y la mejora continua de las prácticas de seguridad de la información en la entidad.

El conjunto documental se encuentra alineado con los lineamientos de la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información y el Marco de Referencia de Arquitectura Empresarial del MinTIC, y actúa como un habilitador transversal de los procesos misionales,

estratégicos y de apoyo de la entidad. En este sentido, los documentos técnicos no se conciben como instrumentos aislados, sino como componentes integrados de la arquitectura institucional de información, aplicaciones y tecnología.

La actualización, divulgación y aplicación de estos documentos es responsabilidad compartida entre la Subdirección de Desarrollo y Tecnología y los líderes de proceso, en concordancia con el modelo de gobernanza institucional definido, garantizando que la seguridad y privacidad de la información se incorporen de manera efectiva en la operación diaria de la entidad y en la prestación de servicios a los ciudadanos.

Los documentos técnicos que respaldan la gestión de la seguridad y privacidad de la información se encuentran publicados en la intranet institucional y comprenden, entre otros, los relacionados en la Tabla 2 del presente documento.

Tabla 2. Documentos Técnicos de Seguridad de la Información, Fuente: Unidad SPE

TIPO DE DOCUMENTO	NOMBRE
Procedimiento	GS-Pr-04 Procedimiento Asociados con Tecnología
Procedimiento	GS-Pr-08 Procedimiento gestión de copias de seguridad
Procedimiento	GS-Pr-09 Procedimiento gestión de eventos de servicios TIC
Procedimiento	GS-Pr-09 Procedimiento de gestión de incidentes de seguridad informática
Procedimiento	GS-Pr-12 Procedimiento para Solicitudes de Información a la Subdirección de Desarrollo y Tecnología
Procedimiento	GS-Pr-14 Procedimiento Clasificación de Activos
Procedimiento	GS-Pr-15 Procedimiento de análisis, valoración y tratamiento de riesgos de SI
Procedimiento	GS-Pr-16 Procedimiento Control de Accesos
Procedimiento	GS-Pr-18 Procedimiento de las acciones de mitigación
Procedimiento	GS-Pr-19 Procedimiento Conexiones Seguras.
Procedimiento	GS-Pr-20 Procedimiento Copias de seguridad para paz y salvo
Procedimiento	GS-Pr-21 Procedimiento Copias de Seguridad de Servidores y Base de Datos Nube Privada
Procedimiento	GS-Pr-22 Procedimiento Copias de archivos de trabajo y correo electrónico de usuario final.
Procedimiento	GS-Pr-23 Procedimiento Copias de seguridad de servidores locales en sitio.

TIPO DE DOCUMENTO	NOMBRE
Documento	Mapa de Riesgos Proceso Gestión de Tecnologías de Información de la Unidad del SPE.
Manual	GS-M-02 Manual de Políticas de seguridad y privacidad de la información
Política	GS-P-01 Política de Seguridad y privacidad de la información.
Política	DE-P-02- Política de Tratamiento de Datos Personales
Planes	GS-PL-01 Plan Estratégico de Seguridad de la Información
Documentos	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
Formato	GS-Ft-10 Formato de documentación de incidentes de seguridad de la información
Formato	GS-Ft-19 Formato Tratamiento de Riesgos
Formato	GS-Ft-20 Formato del registro de riesgos de seguridad de la información
Formato	GS-Ft-21 Formato Inventario de activos de información
Formato	GS-Ft-23 Formato Registros de Incidentes de Seguridad de la Información

6. ESTADO ACTUAL DE SEGURIDAD DE LA INFORMACIÓN

El estado actual de la seguridad y privacidad de la información en la Unidad Administrativa Especial del Servicio Público de Empleo se analiza a partir de los resultados del Formulario Único de Reporte de Avances de la Gestión (FURAG), los cuales constituyen el principal instrumento de medición del desempeño institucional en el marco del Modelo Integrado de Planeación y Gestión, así como de la Política de Gobierno Digital y la Política de Seguridad Digital.

En lo correspondiente a la Política de Seguridad Digital, los resultados obtenidos para la vigencia evaluada reflejan un puntaje global del 76,8 %, evidenciando un nivel de avance intermedio en la implementación de los lineamientos establecidos por el Gobierno Nacional. Tal como se presenta en la Tabla 3, se destacan fortalezas significativas en el despliegue de controles, con un cumplimiento del 100 %, así como en la implementación de los lineamientos de política, con un resultado del 83,3 %. No obstante, se identifican oportunidades de mejora en el componente de asignación de recursos, el cual presenta un nivel de avance inferior, lo que evidencia la necesidad de fortalecer la planeación, priorización y sostenibilidad de las iniciativas de seguridad de la información.

Tabla 3. Función Pública, Fuente: *(Función_Pública, 2024)*

POLITICA SEGURIDAD DIGITAL	PUNTAJE TOTAL:76,8%
Asignación de Recursos	50
Implementación Lineamientos de Política	83,3
Despliegue de Controles	100

Estos resultados permiten concluir que la entidad cuenta con controles de seguridad implementados y en operación; sin embargo, requiere consolidar capacidades institucionales, recursos y mecanismos de gobernanza que garanticen la permanencia, madurez y evolución de la seguridad de la información como habilitador estratégico.

Por su parte, los resultados asociados a la Política de Gobierno Digital, presentados en la Tabla 4, evidencian un desempeño global favorable, con un puntaje total del 89,8 %, lo cual refleja un nivel avanzado de adopción de los lineamientos de política pública en materia de transformación digital. Se destacan particularmente los componentes de gobernanza, innovación pública digital, cultura y apropiación, estado abierto y proyectos de transformación digital, los cuales presentan niveles de cumplimiento superiores al promedio institucional.

No obstante, el análisis de la Tabla 4 también permite identificar brechas relevantes en componentes directamente relacionados con la seguridad y confiabilidad de los servicios digitales, tales como servicios ciudadanos digitales y servicios y procesos inteligentes, cuyos resultados evidencian la necesidad de fortalecer la protección de la información, la continuidad operativa y la integración de la seguridad desde el diseño de los servicios y procesos institucionales.

Tabla 4 Actividades Plan Estratégico de Seguridad de la Información, *Fuente: Unidad SPE*

POLITICA GOBIERNO DIGITAL	PUNTAJE TOTAL: 89,8
Gobernanza	94,5
Innovación pública digital	94,5
Arquitectura	89,2
Seguridad y privacidad de la información	84,6
Servicios ciudadanos digitales	41,8
Cultura y apropiación	100
Servicios y procesos inteligentes	55,6
Estado abierto	97,6
Decisiones basadas en datos	82,8
Proyectos de transformación digital	100
Estrategias de ciudades y territorios inteligentes	NA

En conjunto, el análisis de las Tablas 3 y 4 pone de manifiesto que la entidad dispone de una base sólida en materia de gobernanza y despliegue de controles de seguridad; sin embargo, enfrenta retos asociados a la articulación estratégica de la seguridad de la información con la arquitectura empresarial, la gestión integral del riesgo y la provisión de servicios digitales confiables y centrados en el ciudadano.

Este diagnóstico constituye un insumo fundamental para la formulación del presente Plan Estratégico de Seguridad de la Información, orientando la definición de estrategias y actividades hacia el cierre de

brechas identificadas, el fortalecimiento progresivo de las capacidades institucionales y la consolidación de la seguridad y privacidad de la información como un habilitador transversal del gobierno institucional, la toma de decisiones basadas en datos y la generación de valor público.

7. ESTRATEGIA DE SEGURIDAD DE LA INFORMACIÓN

La Unidad Administrativa Especial del Servicio Público de Empleo adoptará una estrategia integral de seguridad y privacidad de la información concebida como un habilitador transversal de la Política de Gobierno Digital, orientada a fortalecer la gobernanza institucional, la gestión del riesgo y la confiabilidad de los servicios digitales, en articulación con el Marco de Referencia de Arquitectura Empresarial y el Modelo de Seguridad y Privacidad de la Información definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones.

La estrategia reconoce que la seguridad de la información es un proceso de madurez progresiva, que debe implementarse de manera gradual, planificada y sostenible, considerando el contexto institucional, las capacidades existentes y los resultados de las evaluaciones de desempeño como el FURAG. En este sentido, las iniciativas de seguridad de la información se estructuran por fases, permitiendo avanzar desde un enfoque normativo y procedimental hacia un nivel de mayor integración, efectividad y generación de valor público.

Figura 1. Estrategia Seguridad de la Información, Fuente: Modificada de *(PGD, s.f.)*

Desde el enfoque de arquitectura empresarial, la estrategia integra la seguridad de la información como un componente estructural que soporta los dominios de negocio, información, aplicaciones y tecnología, asegurando que los controles y prácticas de seguridad se incorporen desde el diseño de los procesos, sistemas y servicios institucionales, y no únicamente como mecanismos reactivos.

La estrategia se fundamenta en un enfoque de gestión integral del riesgo, articulando políticas, procedimientos, controles, roles y responsabilidades, con el propósito de identificar, analizar, evaluar y tratar los riesgos asociados a los activos de información, bajo un esquema de mejora continua alineado con el ciclo Planear–Hacer–Verificar–Actuar (PHVA).

De igual manera, promueve la corresponsabilidad institucional en materia de seguridad y privacidad de la información, involucrando a la alta dirección, los líderes de proceso, las áreas misionales y de apoyo, así como a funcionarios, contratistas y terceros, de acuerdo con sus responsabilidades en la gestión y uso de la información.

En coherencia con los resultados del FURAG y los lineamientos de la Política de Gobierno Digital, la estrategia orienta la priorización de iniciativas y actividades hacia el fortalecimiento de capacidades institucionales, el despliegue progresivo de controles, la gestión de incidentes, la continuidad de los servicios y la consolidación de una cultura organizacional orientada a la seguridad digital, asegurando su sostenibilidad en el tiempo.

8. DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS

Las estrategias específicas de seguridad de la información constituyen los ejes operativos mediante los cuales la Unidad Administrativa Especial del Servicio Público de Empleo materializa la estrategia general definida en el presente plan. Estas estrategias se encuentran alineadas con los dominios del Marco de Referencia de Arquitectura Empresarial, el Modelo de Seguridad y Privacidad de la Información y la Política de Gobierno Digital, y permiten integrar la seguridad de la información en la gestión institucional de manera estructurada, coherente y sostenible.

Cada estrategia específica se concibe como un habilitador transversal que articula aspectos de gobernanza, gestión del riesgo, arquitectura institucional y cultura organizacional, asegurando que la seguridad de la información se incorpore desde el diseño de los procesos, sistemas y servicios, y no únicamente como un mecanismo reactivo o correctivo.

8.1 Liderazgo y Gobernanza de la Seguridad de la Información

Esta estrategia tiene como propósito fortalecer el liderazgo institucional y la gobernanza de la seguridad de la información, garantizando el compromiso de la alta dirección y de los líderes de proceso en la definición, aprobación, implementación y seguimiento de las políticas, lineamientos y controles de seguridad. Desde el enfoque de arquitectura empresarial, esta estrategia se articula principalmente con la arquitectura de negocio, asegurando que la seguridad de la información se integre en los procesos misionales, estratégicos y de apoyo, y que cuente con los recursos, responsabilidades y mecanismos de control necesarios para su sostenibilidad.

8.2 Gestión de Riesgos y Análisis de Vulnerabilidades

Esta estrategia se orienta a identificar, analizar, evaluar y tratar los riesgos asociados a los activos de información, considerando amenazas internas y externas, dependencias tecnológicas y riesgos derivados del uso de servicios digitales y terceros. Su implementación se articula con los dominios de

arquitectura de información y arquitectura tecnológica, permitiendo priorizar controles de seguridad, definir planes de tratamiento de riesgos y fortalecer la toma de decisiones institucional basada en criterios técnicos y de riesgo aceptable.

8.3 Clasificación y Gestión de Activos de Información

Esta estrategia busca asegurar la identificación, clasificación, actualización y uso adecuado de los activos de información de la entidad, definiendo roles, responsabilidades y niveles de clasificación acordes con su criticidad y sensibilidad. Desde el enfoque de arquitectura empresarial, se relaciona directamente con la arquitectura de información y constituye un insumo fundamental para la protección de datos personales, la transparencia, el acceso a la información y la gestión de riesgos.

8.4 Gestión de Incidentes de Seguridad de la Información

Esta estrategia tiene como finalidad fortalecer la capacidad institucional para prevenir, detectar, analizar, responder y aprender de los incidentes de seguridad de la información, minimizando su impacto en los servicios, procesos y la confianza de los ciudadanos. Se articula con la arquitectura de aplicaciones y tecnología, así como con los procesos de gobierno y control, permitiendo una respuesta coordinada, trazable y alineada con los lineamientos nacionales en materia de seguridad digital.

8.5 Continuidad y Recuperación ante Desastres

Esta estrategia está orientada a fortalecer progresivamente la capacidad institucional de la Unidad Administrativa Especial del Servicio Público de Empleo para garantizar la continuidad de los procesos y servicios críticos ante eventos que puedan afectar la disponibilidad, integridad o confidencialidad de la información, tales como incidentes de seguridad, fallas tecnológicas, errores humanos o eventos externos. En una primera fase, la estrategia se enfoca en el diseño y formulación del Plan de Recuperación ante Desastres (DRP), partiendo de la identificación de procesos y servicios críticos, la definición de escenarios de riesgo, la asignación de roles y responsabilidades, y la determinación de estrategias de recuperación acordes con la arquitectura tecnológica y de aplicaciones de la entidad.
En fases posteriores, el DRP será implementado y validado mediante ejercicios de prueba controlados, que permitirán evaluar su efectividad, identificar brechas técnicas y procedimentales, y fortalecer la capacidad de respuesta institucional. Estas pruebas se programarán de manera gradual y conforme al nivel de madurez alcanzado, priorizando la sostenibilidad y la mejora continua. Desde el enfoque de arquitectura empresarial, esta estrategia se articula principalmente con los dominios de arquitectura de aplicaciones y tecnología, y constituye un habilitador clave para la resiliencia institucional, la continuidad de los servicios digitales y la confianza de los ciudadanos en la gestión de la entidad.

8.6 Cultura y Apropiación de la Seguridad de la Información

Esta estrategia busca consolidar una cultura organizacional orientada a la seguridad y privacidad de la información, promoviendo la corresponsabilidad de funcionarios, contratistas y terceros mediante acciones de sensibilización, capacitación y comunicación. Se articula transversalmente con todos los dominios de la arquitectura empresarial y constituye un factor crítico para la efectividad de las demás estrategias, al integrar la seguridad de la información en el comportamiento cotidiano de la organización.

9. ACTIVIDADES DEL PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

Las actividades definidas en el Plan Estratégico de Seguridad de la Información constituyen el conjunto de acciones mediante las cuales la Unidad Administrativa Especial del Servicio Público de Empleo materializa la estrategia institucional de seguridad y privacidad de la información, en coherencia con la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información y el Marco de Referencia de Arquitectura Empresarial del Ministerio de Tecnologías de la Información y las Comunicaciones.

Las actividades se encuentran estructuradas, priorizadas y programadas con base en los resultados del Formulario Único de Reporte de Avances de la Gestión (FURAG), el análisis del estado actual de la seguridad de la información y la gestión institucional del riesgo, con el propósito de fortalecer progresivamente las capacidades, los controles y la gobernanza de la seguridad de la información en la entidad. El detalle de las actividades del Plan Estratégico de Seguridad de la Información, incluyendo su descripción, responsables institucionales, resultados esperados, indicadores de seguimiento y períodos de evaluación trimestral, se presenta en la Tabla 5. Tabla de Actividades del Plan Estratégico de Seguridad de la Información, la cual constituye el principal instrumento de seguimiento y control del presente plan.

Cada una de las actividades relacionadas en la Tabla 5 se encuentra alineada con al menos una de las estrategias específicas de seguridad de la información definidas en el numeral 8 del presente documento y contribuye al fortalecimiento de uno o más dominios de la arquitectura empresarial —negocio, información, aplicaciones y tecnología— asegurando la integración de la seguridad de la información en los procesos, sistemas y servicios institucionales.

La ejecución de las actividades se realizará bajo un enfoque de corresponsabilidad institucional, involucrando a la Subdirección de Desarrollo y Tecnología, las áreas misionales y de apoyo, así como a los líderes de proceso, de acuerdo con los roles y responsabilidades definidos. El seguimiento se efectuará de manera periódica, conforme a los períodos de evaluación establecidos, permitiendo identificar avances, desviaciones, riesgos y oportunidades de mejora. Los resultados del seguimiento a las actividades del plan permitirán:

- Evaluar el nivel de cumplimiento de los objetivos estratégicos de seguridad de la información.
- Medir la efectividad de los controles implementados.
- Alimentar los reportes institucionales de gestión y desempeño, incluyendo FURAG y MIPG.
- Ajustar y priorizar acciones para vigencias posteriores, bajo un enfoque de mejora continua.

En este sentido, la Tabla 5. Tabla de Actividades del Plan Estratégico de Seguridad de la Información se consolida como el eje operativo y de control del plan, garantizando la trazabilidad entre el diagnóstico, la estrategia, la ejecución y los resultados en materia de seguridad y privacidad de la información.

Tabla 5 Actividades Plan Estratégico de Seguridad de la Información, *Fuente: Unidad SPE*

No.	Actividad	Responsable	Resultado esperado	Indicador	Periodo de evaluación
1	Actualización y publicación oficial de la Política de Seguridad y Privacidad de la Información	Subdirección de Desarrollo y Tecnología – Planeación – Comunicaciones	Política vigente, aprobada y alineada con PGD, MSPI y MRAE	Política aprobada y publicada (Sí/No)	Trimestre II
2	Actualización y publicación del Inventario de Activos de Información	Subdirección de Desarrollo y Tecnología – Todas las áreas	Inventario completo, clasificado y actualizado	% de activos identificados y clasificados	Trimestre III
3	Revisión de procedimientos, formatos, manuales e instructivos de seguridad digital	Subdirección de Desarrollo y Tecnología – Planeación	Marco procedimental actualizado y coherente con la estrategia	% de documentos actualizados	Trimestre II
4	Sensibilización sobre la Política de Seguridad y Privacidad de la Información	Subdirección de Desarrollo y Tecnología – Comunicaciones	Funcionarios y contratistas sensibilizados	% de funcionarios sensibilizados	Trimestres I, II, III y IV
5	Generación de boletines o cápsulas de seguridad de la información	Subdirección de Desarrollo y Tecnología	Cultura organizacional fortalecida	Nº de boletines emitidos vs. planificados	Trimestres I, II, III y IV
6	Inducción y reinducción en seguridad de la información y protección de datos personales	Subdirección de Desarrollo y Tecnología – Talento Humano	Capacidades institucionales fortalecidas	% de funcionarios capacitados	Trimestres I y III
7	Actualización y publicación de la matriz de control de accesos	Subdirección de Desarrollo y Tecnología – Planeación	Control y trazabilidad de accesos a activos críticos	Matriz actualizada y aprobada (Sí/No)	Trimestre II
8	Análisis del uso de doble factor de autenticación y contraseñas	Subdirección de Desarrollo y Tecnología	Decisiones informadas sobre fortalecimiento de autenticación	Informe elaborado y aprobado (Sí/No)	Trimestre II
9	Análisis de vulnerabilidades tecnológicas	Subdirección de Desarrollo y Tecnología	Vulnerabilidades identificadas y priorizadas	% de vulnerabilidades con plan de acción	Trimestre III
10	Diseño, formulación e implementación progresiva del Plan de Recuperación ante Desastres (DRP) del SPE	Subdirección de Desarrollo y Tecnología – Todas las áreas	Plan de Recuperación ante Desastres (DRP) formulado, documentado y alineado con los procesos y servicios críticos de la entidad, con definición de escenarios, roles, estrategias de recuperación y hoja de ruta para su implementación y pruebas posteriores.	DRP formulado y documentado conforme a lineamientos institucionales (Sí/No).	Trimestre IV
11	Gestión de incidentes de seguridad de la información	Subdirección de Desarrollo y Tecnología	Incidentes gestionados conforme a procedimiento	% de incidentes gestionados oportunamente	Trimestres I, II, III y IV
12	Diseño del Plan de Seguridad y Privacidad de la Información 2027	Subdirección de Desarrollo y Tecnología	Planeación estratégica de seguridad formulada	Plan 2027 aprobado (Sí/No)	Trimestre IV
13	Actualización y publicación del Registro de Riesgos de Seguridad de la Información	Subdirección de Desarrollo y Tecnología – Todas las áreas	Riesgos actualizados y tratados	% de riesgos con tratamiento definido	Trimestre II
14	Revisión de la matriz de riesgos de seguridad y propuesta de controles	Subdirección de Desarrollo y Tecnología	Riesgos críticos priorizados con controles definidos	% de riesgos críticos con controles implementados	Trimestre IV

10. GLOSARIO

A continuación, se relaciona el glosario del documento, el cual, está alineado con la información publicada por el Ministerio TIC en su página web (Glosario, s.f.):

- **Arquitectura de TI:** describe la estructura y las relaciones de todos los elementos de TI de una organización. Se descompone en arquitectura de información, arquitectura de sistemas de información y arquitectura de servicios tecnológicos. Incluye además las arquitecturas de referencia y los elementos estructurales de la estrategia de TI (visión de arquitectura, principios de arquitectura, lineamientos y objetivos estratégicos).
- **Arquitectura Empresarial:** es una práctica estratégica que consiste en analizar integralmente las entidades desde diferentes perspectivas o dimensiones, con el propósito de obtener, evaluar y diagnosticar su estado actual y establecer la transformación necesaria. El objetivo es generar valor a través de las Tecnologías de la Información para que se ayude a materializar la visión de la entidad.
- **Capacidades de TI:** son un subconjunto de las capacidades institucionales operativas que tienen como propósito asegurar el adecuado aprovisionamiento del talento humano y los recursos que se necesitan para ofrecer los servicios de TI definidos en su catálogo.
- **Dominio:** cada uno de los seis componentes que conforman la estructura de la primera capa del diseño conceptual del Marco de Referencia de Arquitectura Empresarial para la gestión de TI. Los dominios son las dimensiones desde las cuales se debe abordar la gestión estratégica de TI. Agrupan y organizan los objetivos, áreas y temáticas relativas a las TI.
- **Estándares:** en el contexto de TI, un estándar es un documento que contiene un conjunto de especificaciones técnicas de aplicación voluntaria, que ha sido construido a través de consenso y que refleja la experiencia y las mejores prácticas en un área en particular.
- **Gestión TI:** es una práctica, que permite operar, innovar, administrar, desarrollar y usar apropiadamente las tecnologías de la información (TI), con el propósito de agregar valor para la organización. La gestión de TI permite a una organización optimizar los recursos, mejorar los procesos de negocio y de comunicación y aplicar las mejores prácticas.
- **Lineamiento:** es una orientación de carácter general, corresponde a una disposición o directriz que debe ser implementada en las entidades del Estado colombiano.
- **Marco de Referencia de Arquitectura Empresarial:** es un modelo de referencia puesto a disposición de las instituciones del Estado colombiano para ser utilizado como orientador estratégico de sus arquitecturas empresariales, tanto sectoriales como institucionales. El marco establece la estructura conceptual, define lineamientos, incorpora mejores prácticas y traza una ruta de implementación para lograr una administración pública más eficiente, coordinada y transparente, a través del fortalecimiento de la gestión de las Tecnologías de la Información.
- **Mejores prácticas:** conjunto de acciones que han sido implementadas con éxito en varias organizaciones, siguiendo principios y procedimientos adecuados.
- **Normatividad:** leyes, decretos y demás desarrollos normativos que guían las acciones para implementar el Marco de Referencia de Arquitectura Empresarial para la gestión de TI.
- **Valor:** en un contexto organizacional, generar y entregar valor significa, en general, proveer un conjunto de servicios y productos para facilitarle a alguien el logro de un objetivo. TI genera y entrega valor a una institución mediante la implementación de los servicios de TI.

11. BIBLIOGRAFÍA

Arquitectura, M. T. (2022). *Marco de Referencia de Arquitectura Empresarial*. Obtenido de https://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8118.html
Función_Pública. (2023). *Resultados FURAG*. Obtenido de https://app.powerbi.com/view?r=eyJrIjoiZmE5Mjg3ZTktNzVkMy00OWQ0LTk2MDctNDM2YmU0YzdlYmU3IiwidCI6IjU1MDNhYWMyLTdhMTUtNDZhZi1iNTIwLTJhNjc1YWQxZGYxNiIsImMiOjR9
Glosario, M. T. (s.f.). *Glosario*. Obtenido de https://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8161.html
Guía, P. M. (s.f.). *Arquitectura TI*. Obtenido de https://www.mintic.gov.co/arquitecturati/630/w3-article-15031.html
PGD, M. T. (s.f.). *Política de Gobierno Digital*. Obtenido de https://gobiernodigital.mintic.gov.co/portal/Politica-de-Gobierno-Digital/