

**RESOLUCIÓN No**

"Por medio de la cual se designa al oficial de seguridad y privacidad de la información de la universidad Pedagógica y Tecnológica de Colombia."

El Rector de la Universidad Pedagógica y Tecnológica de Colombia, en uso de sus atribuciones legales y estatutarias y en especial las consignadas en la Ley 30 de 1992, los Acuerdos 074 de 2010 y 066 de 2005 y

**CONSIDERANDO:**

Que, para cumplir este propósito se debe contar con un fundamento normativo, políticas de ejecución, procedimientos, recursos tecnológicos, recursos administrativos y humanos necesarios para gestionar efectivamente el riesgo. En este sentido, las entidades deben adoptar los lineamientos para la gestión de la seguridad de la información y seguridad digital que emita el ministerio de tecnologías de la información y de las comunicaciones.

Que es función del Rector expedir mediante Resoluciones, actos administrativos, según el Artículo 22 del Acuerdo 066 de 2005.

Que la Ley 1712 de 2014 crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Que el Decreto 728 de 2017 adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.

Que el Decreto 1499 de 2017 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.

Que el decreto 1008 de 2018, establece los lineamientos generales de la política de Gobierno Digital y subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del decreto 1078 de 2015, único reglamentario del sector de las tecnologías y sistemas de la información y de las comunicaciones el cual determina que la seguridad de la información busca crear condiciones de uso confiable en el entorno digital mediante un enfoque en la gestión basado en la gestión de riesgos preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del estado, elemento fundamental que permite el desarrollo de gobierno digital y privacidad de los datos.

Que la Resolución 2999 del 2008 adopta las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC.

Que el artículo 2.2.17.5.6 del decreto 620 del 2020 establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales, seguridad de la información y seguridad digital, determinando que los actores que realicen el tratamiento de la información , deberán contar con una estrategia de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio en la que se lleve periódicamente una evaluación del riesgo de seguridad digital que incluya una identificación de las mejoras a implementar en el Sistema de Administración de Riesgo Operativo.

Que el decreto 338 del 8 de marzo de 2022 por el cual se adiciona el Título 21 a la parte 2 del libro 2 decreto 1078 de 2015 único reglamentario del sector de tecnologías de la información y de las comunicaciones, establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el modelo y las instancias de gestión de riesgos y atención de incidentes y se dictan otras disposiciones.

Que, en el manual de Gobierno Digital, expedido por el Ministerio de Tecnologías de la Información y de las Comunicaciones, se establecen las pautas que deben aplicar las entidades públicas para la implementación de la Políticas de Gobierno Digital, entre ellas, la aplicación del Modelo de Seguridad y Privacidad de la Información (MSPI), cuyos lineamientos e indicadores permiten establecer el nivel de madurez en materia digital para las entidades públicas.

Que el mencionado manual se encuentra alineado con las buenas prácticas en seguridad (Norma ISO/IEC 27001:2013), con la Ley 1581 de 2012 que trata de la protección de datos personales y con la ley 1712 de 2014 (Ley de Transparencia y Acceso a la información publica)

Que la implementación del Modelo de seguridad y privacidad de la información MSPI en la Universidad Pedagógica y Tecnológica de Colombia está determinada por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la entidad, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo.

Que mediante la adopción del Modelo de Seguridad y Privacidad de la Información por parte de las entidades del Estado se busca contribuir al incremento de la transparencia de la gestión publica promoviendo el uso de las mejores practicas de Seguridad de la Información cumpliendo con la aplicación del concepto de seguridad digital.

Que para el cumplimiento del Modelo de Seguridad y Privacidad de la información se debe establecer las funciones y responsabilidades del líder de la planeación, implementación y verificación a cargo del oficial de seguridad y privacidad de la información

En mérito de lo anterior, el Rector de la Universidad Pedagógica y Tecnológica de Colombia,

9



RESUELVE: 1314

**Artículo 1º.** Designar al oficial de seguridad y privacidad de la información de la Universidad Pedagógica y Tecnológica de Colombia al funcionario JOSE ALEXANDER ARAGON GUERRA identificado con cedula de ciudadanía 77.093.025 en calidad de Oficial de Seguridad y Privacidad de la Información de la Universidad Pedagógica y Tecnológica de Colombia - UPTC, con todas las facultades y responsabilidades inherentes al cargo.

**Artículo 2º.** El Oficial de Seguridad y Privacidad de la Información (OSPI) será responsable de planificar, implementar, supervisar y mantener las políticas, programas y procedimientos relacionados con la seguridad y privacidad de la información en la UPTC, de acuerdo con las normativas y estándares vigentes.

**Artículo 3º.** Para la presente Resolución se tendrán en cuenta las siguientes definiciones, las cuales fueron tomadas del Modelo de Seguridad y Privacidad de la Información de la Dirección de Tecnologías y Sistemas de la Información y de las Comunicaciones de la UPTC:

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
  - **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).
  - **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
  - **Acuerdo de Confidencialidad o Contrato de Confidencialidad:** Es un acuerdo legal entre al menos dos entidades para compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público.
- ADMINISTRACIÓN DE RIESGOS: Conjunto de elementos de control que al interrelacionarse permiten a la Entidad Pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos, que permitan identificar oportunidades para un mejor cumplimiento de su función. Se constituye en el componente de control

que al interactuar sus diferentes elementos le permite a la entidad pública autocontrolar aquellos eventos que pueden afectar el cumplimiento de sus objetivos. (Función Pública. Guía para la Administración del Riesgo. Bogotá, 2011)  
AMENAZAS: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Ambiente de Desarrollo:** Conjunto de elementos de hardware y de software como compiladores, editores, instaladores de lenguaje de programación, donde residen todos los recursos informáticos necesarios para efectuar tareas relacionadas con la generación o modificación de aplicaciones
- **Ambiente de producción:** Conjunto de elementos de hardware y de software que soportan los sistemas utilizados por los funcionarios para la ejecución de las operaciones de la entidad. En este ambiente deben residir aplicaciones y producción, bibliotecas o directorios que contengan archivos de datos, bases de datos, programas ejecutables o compilados.
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)
- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

af





- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
- **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las

convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)
- **Gestión de incidentes de seguridad:** de la información Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias
- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008. Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

4



- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.
- **OSPI:** Oficial de Protección de Datos Personales
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)
- **Responsabilidad Demostrada:** Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias. Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

IX

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000). Vulnerabilidad Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).
- **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

**Artículo 4º.** El Oficial de Seguridad y Privacidad de la Información tendrá las siguientes funciones:

1. El OSPI es responsable de desarrollar y mantener políticas, estándares y procedimientos de seguridad de la información que cumplan con las regulaciones y estándares de seguridad aplicables.
2. El OSPI identifica y evalúa los riesgos de seguridad de la información de la organización, y desarrolla estrategias para mitigar dichos riesgos.
3. El OSPI coordina la respuesta a incidentes de seguridad de la información, investiga incidentes de seguridad reportados y toma medidas correctivas según sea necesario.

9





4. El OSPI supervisa la implementación y efectividad de controles de seguridad de la información, como la autenticación de usuarios, el cifrado de datos, el control de acceso y la seguridad de la red.
5. El OSPI realiza evaluaciones periódicas de seguridad de la información, como evaluaciones de vulnerabilidad, pruebas de penetración y revisiones de cumplimiento de seguridad.
6. El OSPI desarrolla y ofrece programas de concienciación sobre seguridad de la información para empleados, contratistas y otros usuarios autorizados.
7. El OSPI colabora estrechamente con otras áreas de la organización, como Dirección de Tecnologías y Sistemas de la Información y de las Comunicaciones, Dirección Jurídica, Talento Humano y Control interno, para garantizar una seguridad integral de la información.
8. En organizaciones sujetas a regulaciones de privacidad de datos, el OSPI puede ser responsable de desarrollar y gestionar programas de privacidad de datos para proteger la información personal de los individuos.
9. El OSPI se mantiene al tanto de las últimas amenazas y tendencias de seguridad de la información y ajusta las políticas y procedimientos de seguridad en consecuencia.
10. Actualizar y definir políticas, normas, procedimientos y estándares, manuales metodologías y documentación del MSPI que sea de su competencia, así como apoyar otros procesos que requieran brindar lineamientos relacionados con seguridad de la información.
11. Realizar análisis de riesgo a las aplicaciones y sistemas de información y uso de la Universidad.
12. Asesorar en la aplicación de la metodología para el mantenimiento de los planes de contingencia y continuidad de las funciones misionales de la Entidad.
13. Realizar estudios de penetración y pruebas y vulnerabilidades en todos los ambientes (Desarrollo, pruebas, producción y contingencia) a los servidores, equipos de comunicación, seguridad y sistemas de información, resultado de los procesos de Gestión de Sistemas de Información y Gestión de la Configuración y Activos de los servicios de Tecnologías de la Información. De igual forma,

SD

1181

recomendar controles o planes de tratamiento para mitigación de las vulnerabilidades.

14. Apoyar las auditorias internas y externas al sistema de gestión de seguridad de la información.
15. Estar al tanto de las nuevas modalidades de ciberataques que pudieran afectar a la entidad en materia de seguridad y privacidad de la información, de acuerdo con la evaluación de riesgo.
16. Reportar a la oficina de Control Disciplinario las presuntas violaciones de los funcionarios públicos al cumplimiento de las políticas del manual de Seguridad y Privacidad de la información que generaron algún incidente de seguridad que afecto la integridad, disponibilidad o confidencialidad de la información de la entidad, para su respectiva investigación y acciones a las que haya lugar.
17. Aplicar las demás consideraciones que a juicio de la entidad contribuyan a elevar sus estándares de seguridad y privacidad de la información.

**Artículo 5°.** El Oficial de Seguridad y Privacidad de la información, realizara informe con respecto al avance de su gestión de manera semestral al Grupo de Gobierno Digital.

**Artículo 6°.** La presente Resolución rige a partir de la fecha de su publicación.



**PUBLÍQUESE Y CÚMPLASE**

07 FEB 2024

Dado en Tunja, a los



**ENRIQUE VERA LOPEZ**  
Rector UPTC

Reviso William Iván Cabiativa Piracun.   
Doctor Javier Andres Camacho Molano.   
Director Jurídico.  
Ing Leonardo Bernal Zamora  
Director de las DTIC.