

Security



Code

Safety

Protection



Information



Data

Privacy

PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD  
Y PRIVACIDAD DE LA INFORMACIÓN  
2024



Dirección de las Tecnologías y  
Sistemas de Información y  
de las Comunicaciones



## TABLA DE CONTENIDO

1.	INTRODUCCIÓN .....	4
2.	JUSTIFICACION.....	5
3.	OBJETIVOS .....	5
	<i>a.General</i> .....	5
	<i>b. Específicos</i> .....	6
4.	ALCANCE DEL SGSI.....	6
5.	RECURSOS.....	7
	5.1 <i>Recurso Humano</i> .....	7
	5.2 <i>Recurso Tecnológico</i> .....	9
	5.2.1 <i>Equipos de Computo</i> .....	10
	5.2.2 <i>Tecnologías Utilizadas</i> .....	10
	5.2.3 <i>Servicio de Internet</i> .....	11
	5.2.4 <i>Sistemas de Información</i> .....	12
	5.2.5 <i>Salas de informática</i> .....	13
	5.2.6 <i>Recursos Financieros</i> .....	18
6	VISION GENERAL DEL PROCESO DE RIESGOS DE SEGURIDAD DE LA INFORMACION.....	19
	6.1 <i>Criterios de Evaluación de Riesgos de Seguridad</i> .....	21
	6.2 <i>Criterios de Impacto</i> .....	21
7	VALORACION DE LOS RIESGOS.....	22
	7.1 <i>Identificación Del Riesgo</i> .....	22
	7.2 <i>Estimación Del Riesgo</i> .....	25
	7.3 <i>Determinación del Riesgo</i> .....	27
	7.4 <i>Valoración de los Riesgos de Seguridad</i> .....	29
	7.5 <i>Tratamiento de Riesgos de Seguridad</i> .....	29
	7.6 <i>Monitoreo</i> .....	30
	7.7 <i>Metodología</i> .....	30



8	<i>Actividades a Realizar</i> .....	31
9	MEDICION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION .....	32
9.1	<i>Medición</i> .....	32
9.2	<i>Normativa Aplicada</i> .....	35
	Glosario .....	36
	Referencias bibliográficas .....	41

#### **TABLA DE ILUSTRACIONES**

Ilustración 1	Recurso Humano DTIC .....	7
Ilustración 2	Organigrama DTIC .....	8
Ilustración 3	servicios de red .....	11
Ilustración 4	sistemas de información por proceso .....	13
Ilustración 5	contexto y valoración del riesgo .....	19
Ilustración 6	enfoque basado en procesos .....	20
Ilustración 7	Escala de Probabilidad .....	25
Ilustración 8	Valor de impacto .....	26
Ilustración 9	Tabla 1: evaluación del riesgo .....	28
Ilustración 10	Zona de Riesgo .....	28
Ilustración 11	Efectividad de controles .....	33
Ilustración 12	Brecha .....	33
Ilustración 13	Ciclo PHVA .....	34
Ilustración 14	Modelo Operacion .....	34
Ilustración 15	Nivel de Madurez .....	35



# 1. INTRODUCCIÓN

Las empresas hoy día, nos encontramos inmersas en la denominada revolución digital, en donde se reconoce el protagonismo de la información en sus procesos productivos, por tanto la importancia de tener su información adecuadamente identificada y protegida, como también la proporcionada por sus partes interesadas, enmarcada bajo las relaciones de cumplimiento, comerciales y contractuales como los son acuerdos de confidencialidad y demás compromisos, que obligan a dar un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia.

La Seguridad de la Información en las empresas tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio.

La UPTC decide vincular el modelo de administración de los riesgos de seguridad de la información y las actividades de valoración de mismos riesgos en cumplimiento de la política de seguridad de la información aprobada por la Alta Dirección, y como medio o herramienta para el logro de los objetivos de mantener la información de la Entidad confidencial, íntegra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación.



## 2. JUSTIFICACION

El presente documento tiene como fin generar una cultura de prevención contra los riesgos a los que día a día se pudieran ver sometidos los activos de información de la Universidad Pedagógica y Tecnológica de Colombia UPTC. Basados en un enfoque de planeación de gestión del riesgo se pretende realizar una estrategia que permita diagnosticar, evaluar, implementar y desarrollar la gestión de incidentes que afectan al activo de información e implantar unas contramedidas en el sistema de gestión informático para disminuir la probabilidad de su materialización.

## 3. OBJETIVOS

### *a. General*

Proporcionar a la Universidad Pedagógica y Tecnológica de Colombia una herramienta que brinde las pautas necesarias para el adecuado tratamiento de los riesgos a los que están expuestos los activos de información. Esto permitirá una toma de decisiones informada para reducir la probabilidad de que se materialice una amenaza, así como para disminuir la vulnerabilidad del sistema y el posible impacto en la entidad.



## b. Específicos

- Consolidar una administración de riesgos acorde con las necesidades de la Universidad
- Proteger los activos de información de acuerdo a su clasificación y criterios de Confidencialidad, Integridad y Disponibilidad
- Crear conciencia a nivel institucional de la importancia y la necesidad de una correcta gestión del riesgo de seguridad de la información.

## 4. ALCANCE DEL SGSI

La gestión de riesgos de seguridad de la información y su tratamiento, podrá ser aplicada sobre cualquier proceso de la Universidad, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información, análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

## 5. RECURSOS

### 5.1 *Recurso Humano*

La Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones, cuenta con personal, quienes colaboran en la atención de los diferentes servicios establecidos en el Catálogo de servicios y de velar por la seguridad de la información tanto en la Sede Tunja como en las Seccionales, de la siguiente manera:



Ilustración 1 Recurso Humano DTIC



De las 61 personas que trabajan en la Dirección de Tecnologías actualmente se distribuyen las labores de la siguiente manera:



**Ilustración 2 Organigrama DTIC**

## 5.2 Recurso Tecnológico



Para la red de intranet la Universidad cuenta con un Servidor que la soporta en donde se encuentran instalados todos los Sistemas de Información de la Universidad y desde allí se da acceso por cableado de fibra óptica a todas las dependencias Académico-Administrativas de la Institución. Uno de los servicios que presta la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones -DTIC-, es la asignación y administración de los correos electrónicos Institucionales, los cuales son asignados para todos los estudiantes, docentes y personal administrativo. Además, se mantienen cuentas de correo electrónico, activas vigentes, para los graduados de la Universidad.

La universidad dentro de su infraestructura tecnológica cuenta con:

Imagen tomada de <https://www.qdm.com.mx/hs-hubfs/Transformacio%CC%81n%20digital%20en%20Recursos%20Humanos%20copia.png?width=544&name=Transformacio%CC%81n%20digital%20en%20Recursos%20Humanos%20copia.png>



## 5.2.1 *Equipos de Computo*

- Un Datacenter dotado con aire acondicionado, sistema de extinción, control de acceso, planta eléctrica y UPS.
- Granja de 42 servidores en Tunja, 1 en Duitama, 1 en Sogamoso y 1 en Chiquinquirá.
- Materiales necesarios para el préstamos y atención de los servicios de TI y de seguridad de la información.

## 5.2.2 *Tecnologías Utilizadas*

La Dirección de las Tecnologías y Sistemas de Información de las Comunicaciones con el fin de prestar los servicios con calidad y velar por la seguridad de la información ha integrado tecnologías de punta como son:

- Servidores de alta disponibilidad con sistema operativo red hat, los cuales ofrecen fiabilidad rendimiento y escalabilidad.
- Sistema Veritas NetBackup para realizar las copias de seguridad automatizadas.
- Arquitectura para el desarrollo de aplicaciones basadas en servicios.
- Red Wifi de alto rendimiento que permite conectar un mínimo de 400 conexiones por AP
- Se viene implementando el Cableado certificado categoría IPV6.

## 5.2.3 Servicio de Internet

Se cuenta con un canal de datos de 4175 Mbps e interconexión de fibra óptica entre todos los edificios, tal como se puede visualizar en la imagen 1: Infraestructura tecnológica.

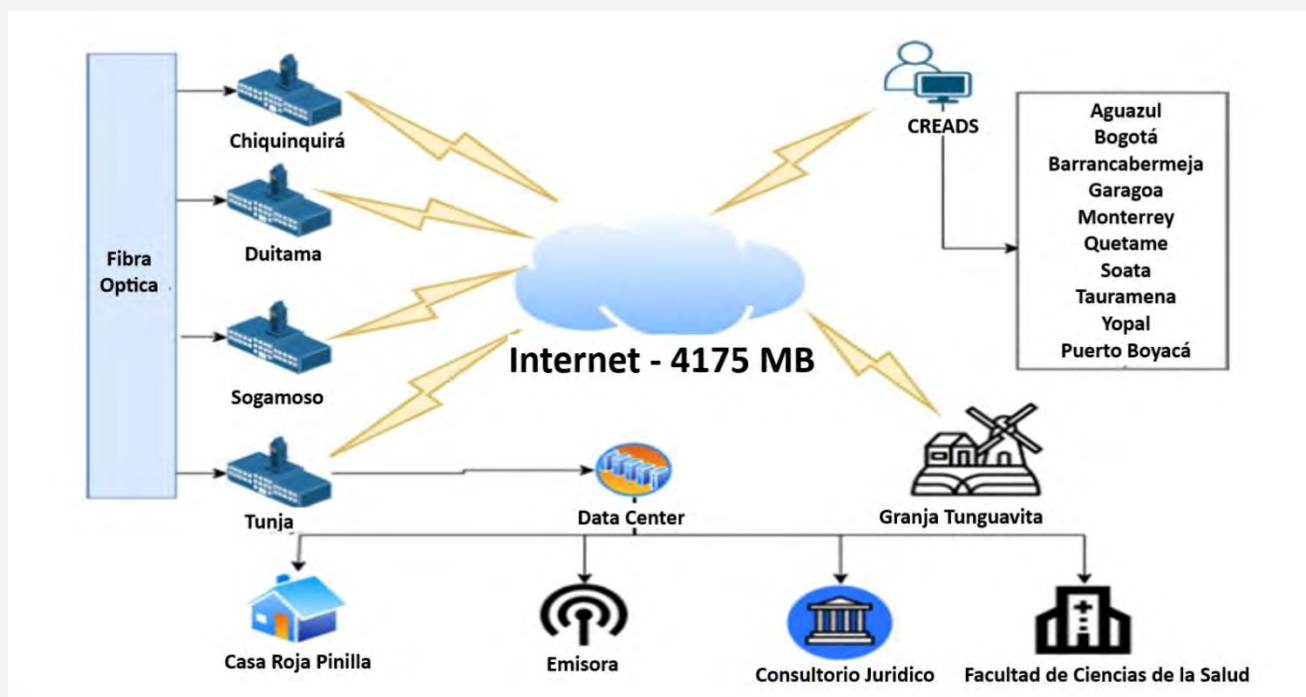


Ilustración 3 servicios de red

**Nota:** Al 2024 se pretende llegar a 4175 MB/S se tiene proyectado realizar la ampliación de MB para el 2025 con 5850 MB/S y para el 2026 7340 MB/S

## 5.2.4 Sistemas de Información

A continuación, se relacionan los sistemas de información, los cuales son utilizados por los procesos institucionales para llevar a cabo sus actividades diarias y son soportados por los gestores de bases de datos Oracle y MySQL.





## PROCESOS DE APOYO

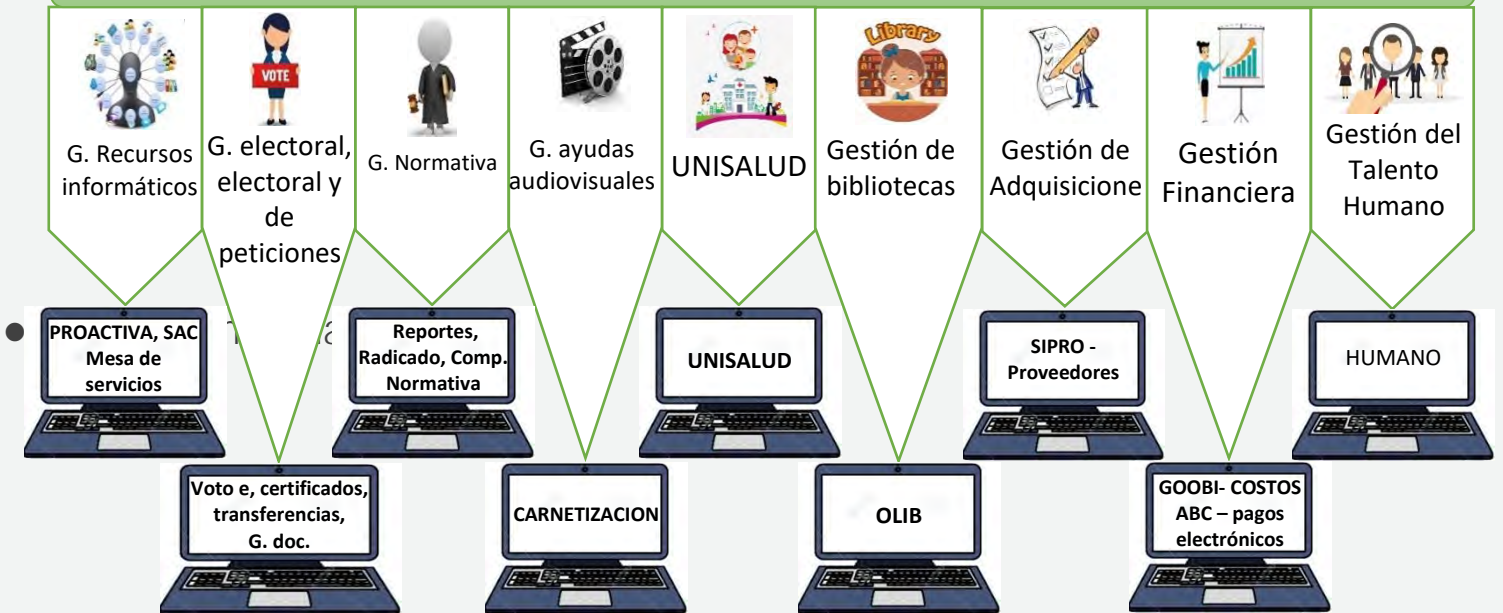


Ilustración 4 sistemas de información por proceso

## 5.2.5 Salas de informática

RELACIÓN EQUIPOS SEDE CENTRAL TUNJA

	AULAS MATEMÁTICAS	N° EQUIPOS	AULAS RA	N° EQUIPOS	AULAS CENTRAL	N° EQUIPOS	AULAS LABORATORIOS	TOTAL EQUIPOS	BIBLIOTECA CENTRAL	TOTAL EQUIPOS	AULAS SALUD	TOTAL EQUIPOS
1	M102	17	RA301	21	C101	18	L216	17	PISO 1	2	Salud 1	23
2	M203	17	RA302	35	C124	25	L301	37	PISO 2	72	Salud 2	23
3			RA303	31	C140	16	L302	37	PISO 4	132		
4			RA304	30	C142	15	L303	37				
5					C143	15	L304	31				
6					C239	16	L305	25				
7					C246	20	L306	19				
8							L307	35				
9							L308	21				
10							L309	19				
11							L310	25				
12							L311	0				
TOTAL EQUIPOS POR EDIFICIO		34		117		125		303		206		46
TOTAL AULAS POR EDIFICIO	2		4		7		11		3		2	

TOTAL EQUIPOS	846
TOTAL AULAS	27



### RELACIÓN EQUIPOS SECCIONAL CHIQUINQUIRÁ

	AULAS GEOMOLOGÍA	N° EQUIPOS	AULA CENTRAL	N° EQUIPOS	BIBLIOTECA	N° EQUIPOS
1	G - 103	24	C - 208	32	BIBLIOTECA	24
2	G - 201	18				
3	G - 202	20				
4	G - 205	32				
TOTAL EQUIPOS POR EDIFICIO		94		32		24
TOTAL AULAS POR SEDE	4		1		1	

TOTAL EQUIPOS	150
TOTAL AULAS	5



## RELACIÓN EQUIPOS SECCIONAL DUITAMA

	AULAS	N° EQUIPOS	SALA BASE DATOS BIBLIOTECA	N° EQUIPOS
1	SALA A	29	SALA BIBLIOTECA	133
2	SALA B	23	SEGUNDO PISO BIBLIOTECA	52
3	SALA C	24		
4	SALA D	20		
5	SALA 304	20		
6	SALA 306	25		
7	SALA 307	25		
8	SALA 308	25		
9	SALA 310	25		
10	SALA 219	25		
11	SALA EAA 203	25		
12	SALA EAA 204	25		
	TOTAL EQUIPOS POR EDIFICIO	291		185
	TOTAL AULAS POR SEDE	12	2	

TOTAL EQUIPOS	476
TOTAL AULAS	12



### RELACIÓN EQUIPOS PUERTO BOYACÁ

	AULAS DTICS	N° EQUIPOS
1	SALA 1	48
TOTAL EQUIPOS POR EDIFICIO		48
TOTAL AULAS POR SEDE	1 (2DO PISO)	
TOTAL EQUIPO	48	
TOTAL AULAS	1	

GRAN TOTAL EQUIPO	1819
GRAN TOTAL AULAS	56



## 5.2.6 *Recursos Financieros*



Estos recursos dependen de la programación anual de presupuesto que realiza la Universidad, se reflejarán en los planes de compras, planeas de inversión y en los recursos asignados para proyectos de Inversión por el rubro Red de Sistematización y Computarización de la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones, el proyecto Mejoramiento Red Inalámbrica para las sedes y la facultad de salud, y el Proyecto de telefonía IP y control de acceso.

En la medida que se requiera se generaran propuestas de proyectos para que se asignen recursos de inversión a la Dirección de las Tecnologías y Sistemas de Información y de las Comunicaciones como proveedor de servicios de TI en la UPTC, junto con las solicitudes de mantenimiento que son requeridas anualmente.

# 6 VISION GENERAL DEL PROCESO DE RIESGOS DE SEGURIDAD DE LA INFORMACION

A continuación, se presenta el modelo de gestión de riesgos de seguridad de la información diseñado y basado tanto en la norma ISO/IEC 31000 como en la ISO 27005 aprobado por la UPTC para la adecuada administración de riesgos en la seguridad de la información; los elementos que lo componen son:

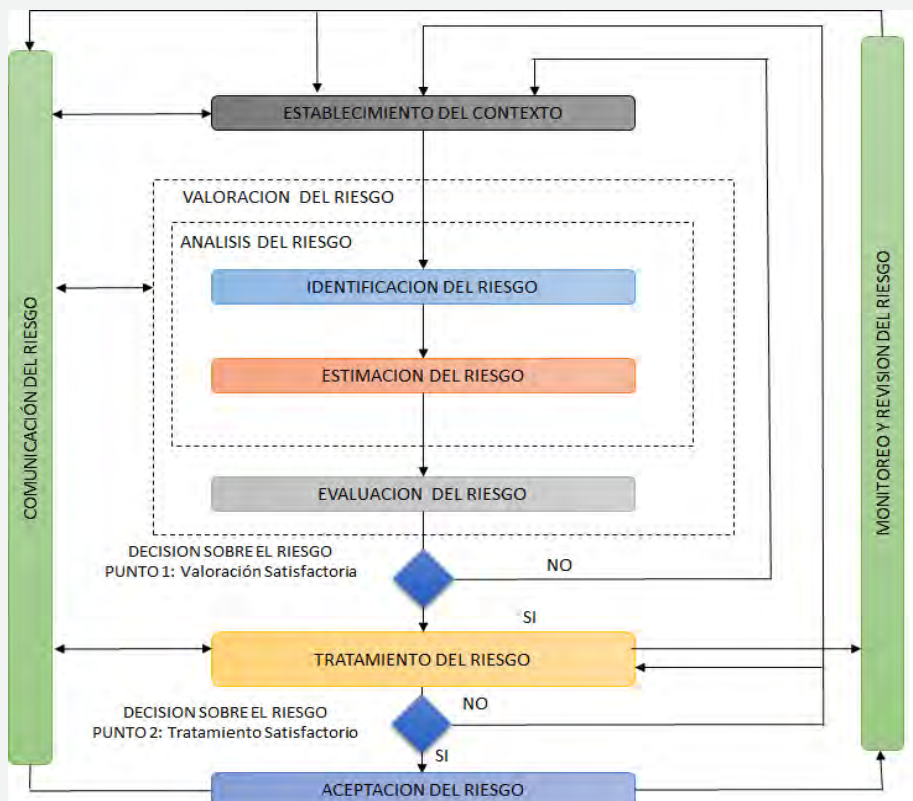


Ilustración 5 contexto y valoración del riesgo



Este conjunto de normas ISO /IEC promueve la adopción del enfoque basado en procesos, para que una organización funcione eficazmente, se debe identificar y gestionar muchas actividades, por lo que se considera como proceso a cualquier actividad que consume recursos y que, además, su gestión promueva la transformación de entradas en salidas. El enfoque basado en procesos consiste en que la organización identifique las actividades del funcionamiento de esta y la interacción entre las actividades; así, para la gestión de la Seguridad de la Información se hace énfasis en la importancia de la norma ISO 27001:2013.



**Ilustración 6 enfoque basado en procesos**

El contexto de gestión de riesgos de seguridad de la información define los criterios básicos que serán necesarios para enfocar el ejercicio por parte de la UPTC y obtener los resultados esperados, basándose en la identificación de las fuentes que pueden dar origen a los riesgos y oportunidades en los procesos de la Agencia, en el análisis de las debilidades y amenazas asociadas, en la valoración de los riesgos en términos de sus consecuencias para la Entidad y en la probabilidad de su ocurrencia, al igual que en la construcción de acciones de mitigación en beneficio de lograr y mantener niveles de riesgos aceptables para la Entidad. Como criterios para la gestión de riesgos de seguridad de la información se establecen:



## 6.1 Criterios de Evaluación de Riesgos de Seguridad

La evaluación de los riesgos de seguridad de la información se enfoca en:

- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones de la UPTC
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la Universidad.

## 6.2 Criterios de Impacto

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para la Universidad, causados por un evento de seguridad de la información, considerando aspectos tales como:

- Nivel de clasificación de los activos de información impactados
- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad)
- Operaciones deterioradas (afectación a partes internas o terceras partes) • Pérdida del negocio y del valor financiero
- Alteración de planes o fechas límites
- Daños en la reputación
- Incumplimiento de los requisitos legales, reglamentarios o contractuales



# 7 VALORACION DE LOS RIESGOS

Previo a la valoración de riesgos de seguridad de la información se determina la relevancia de identificar un inventario de activos de información de los procesos, el cual será la base del enfoque de la valoración de los riesgos de seguridad de la información.

Se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para la Universidad, esta fase consta de las siguientes etapas:

La valoración del Riesgo de seguridad de la información

- Análisis de riesgos
- Identificación de los riesgos`
- Estimación del riesgo
- Evaluación del riesgo

## 7.1 *Identificación Del Riesgo*

Para la evaluación de riesgos de seguridad de la información en primer lugar se deberán identificar los activos de información por proceso en evaluación. Los activos de información se clasifican en dos tipos:



## 7.1.1 Primarios:

- a. **Procesos o subprocesos y actividades del Negocio:** procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.
- b. **Información:** información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.
- c. **Actividades y procesos de negocio:** que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

## 7.1.2 De Soporte

- a. **Hardware:** Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).
- b. **Software:** Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)



- c. **Redes:** Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)
  
- d. **Personal:** Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)
  
- e. **Sitio:** Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)
  
- f. **Estructura organizativa:** responsables, áreas, contratistas, etc.

Después de tener una relación con todos los activos se han de conocer las amenazas que pueden causar daños en la información, los procesos y los soportes. La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc.

Posterior a la identificación del listado de activos, sus amenazas y las medidas que ya se han tomado, a continuación, se revisarán las vulnerabilidades que podrían aprovechar las amenazas y causar daños a los activos de información de la Universidad.

Existen distintos métodos para analizar amenazas, por ejemplo:

- Entrevistas con líderes de procesos y usuarios
- Inspección física
- Uso de las herramientas para el escaneo automatizado



Para cada una de las amenazas analizaremos las vulnerabilidades (debilidades) que podrían ser explotadas.

Finalmente se identificarán las consecuencias, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.

## 7.2 Estimación Del Riesgo

La estimación del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos.

El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos. Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- **Probabilidad:** La posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse.

ESCALA DE PROBABILIDAD	
NIVEL	DESCRIPCION
1	<b>Raro</b> Evento que puede ocurrir sólo en circunstancias excepcionales, entre 0 y 1 vez en 1 semestre.
2	<b>Improbable</b> Evento que puede ocurrir en pocas de las circunstancias, entre 2 y 5 veces en un semestre.
3	<b>Posible</b> Evento que puede ocurrir en algunas de las circunstancias entre seis y 10 veces en 1 semestre.
4	<b>Probable</b> Evento que puede ocurrir en casi siempre entre 11 y 15 veces en 1 semestre.
5	<b>Casi Seguro</b> Evento que puede ocurrir en la mayoría de las circunstancias más de 15 veces en 1 semestre.

Ilustración 7 Escala de Probabilidad



- **Impacto:** Hace referencia a las consecuencias que puede ocasionar a la Universidad la materialización del riesgo; se refiere a la magnitud de sus efectos.

VALOR DE IMPACTO		
NIVEL	DESCRIPCION	ESCALA
1	<b>Insignificante</b> Impacta negativamente de forma leve la imagen y operación de un rol. No tiene impacto Financiero para la Universidad o sus procesos. Impacta negativamente, posibilidad de recibir multas.	$\geq 1$ y $\leq 4$
2	<b>Menor</b> Impacta negativamente la imagen y de manera importante la operación de un proceso. Se pueden presentar sobrecostos debido a reprocesos a nivel de un proceso. Impacta negativamente, posibilidad de recibir multas.	$\geq 5$ y $\leq 8$
3	<b>Moderado</b> Afecta negativamente la imagen Institucional a nivel regional por retrasos en la prestación de los servicios y la operación no sólo del proceso evaluado sino de otros procesos. Se pueden presentar sobrecostos por reprocesos y aumento de carga operativa, no sólo en el proceso evaluado sino a otros procesos. Impacta negativamente, posibilidad de recibir una investigación disciplinaria.	$\geq 9$ y $\leq 12$
4	<b>Mayor</b> Imagen Institucional a nivel nacional afectada, al igual que la operación por el incumplimiento en la prestación de servicios de la Universidad o el cumplimiento de sus objetivos estratégicos. Se pueden presentar sobrecostos por reprocesos significativos para una sede seccional de la Institución. Impacta negativamente, posibilidad de recibir una investigación fiscal.	$\geq 13$ y $\leq 16$
5	<b>Catastrófico</b> Imagen Institucional afectada a nivel nacional e Internacional. Impacta negativamente la operación y el cumplimiento en la prestación de los servicios de la Institución y el incumplimiento de sus objetivos estratégicos. Se pueden presentar sobrecostos debido a reprocesos y aumento de carga operativa importante en toda la Universidad. Impacta negativamente, posibilidad de recibir una intervención o sanción, por parte de entes de control o cualquier ente regulador.	$\geq 17$ y $\leq 20$

Ilustración 8 Valor de impacto



Se sugiere realizar este análisis con todas o las personas que más conozcan del proceso, y que por sus conocimientos o experiencia puedan determinar el impacto y la probabilidad del riesgo de acuerdo con los rangos señalados en las tablas que se muestran más adelante.

Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas financieras, costes de reparación o sustitución, interrupción del servicio, disminución del rendimiento, infracciones legales, pérdida de ventaja competitiva, daños personales, entre otros. Además de medir las posibles consecuencias se deberán analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información o la operación del negocio.

## 7.3 *Determinación del Riesgo*

La valoración de los riesgos de Información se hace de manera cualitativa, generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final la Matriz IP, con la cual la guía **A-RI-P35-G01** (*GUIA IDENTIFICACION, CLASIFICACION Y GESTION DE RIESGOS DE ACTIVOS DE INFORMACION*) presenta la forma de calificar los riesgos con los niveles de impacto y probabilidad establecidos, así como las zonas de riesgo presentando la posibles formas de tratamiento que se le puede dar a ese riesgo, tal como se muestra en la siguiente imagen:



### MATRIZ IP

IMPACTO	VALOR	EVALUACION				
Catastrófico	5	5	10	15	20	25
Mayor	4	4	8	12	16	20
Moderado	3	3	6	9	12	15
Menor	2	2	4	6	8	10
Insignificante	1	1	2	3	4	5
	Valor	1	2	3	4	5
	PROBABILIDAD	Raro	Improbable	Posible	Probable	Casi Seguro

**Ilustración 9 Tabla 1: evaluación del riesgo**

*Tomado de la guía para la gestión del riesgo de Activos de información A-RI-P35-G01*

El análisis del riesgo determinado por su probabilidad e impacto permite tener una primera evaluación del riesgo (escenario sin controles) y ver el grado de exposición al riesgo que tiene la entidad. La exposición al riesgo es la ponderación de la probabilidad e impacto, y se puede ver gráficamente en la matriz de riesgo, instrumento que muestra las zonas de riesgos y que facilita el análisis gráfico. Permite analizar de manera global los riesgos que deben priorizarse según la zona en que quedan ubicados los mismos (zona de riesgo bajo, moderado, alto o extremo) facilitando la organización de prioridades para la decisión del tratamiento e implementación de planes de acción. Las zonas de riesgo se diferencian por colores y por número de zona de la siguiente manera:

ZONA DE RIESGO
B: Zona de riesgo baja (color verde) 12 zonas siendo la Z-4 la de mayor riesgo
M: Zona de riesgo moderada (color amarillo) 8 zonas siendo la Z-9 la de mayor riesgo
A: Zona de riesgo alta (color rojo) 6 zonas siendo la Z-15 la de mayor riesgo
E: Zona de riesgo extrema (color vino tinto) 4 zonas siendo la Z-25 la de más alto riesgo

**Ilustración 10 Zona de Riesgo**



## 7.4 Valoración de los Riesgos de Seguridad

La valoración de los riesgos se puede consultar en el documento **A-RI-P35-G01** *GUIA IDENTIFICACION, CLASIFICACION Y GESTION DE RIESGOS DE ACTIVOS DE INFORMACION* o en el link <http://desnet.uptc.edu.co:17012/DocSigma/Guias/A-RI-P35-G01-V01.pdf>

## 7.5 Tratamiento de Riesgos de Seguridad

El Líder del SGSI con su equipo de trabajo presentará anualmente un plan de tratamiento de los riesgos de seguridad de la información identificados, este plan contiene lo siguiente:

- ✓ La matriz de resultados de selección de objetivos de control y controles referenciando los riesgos para los cuales aplican los controles seleccionados, obtenido con el procedimiento de A-RI-P35 Gestión del Riesgo de Seguridad de la Información y la Guía asociada a este procedimiento.
- ✓ Documento de declaración de aplicabilidad
- ✓ Planes de proyectos de seguridad de la información que hay que adelantar para implementar los controles seleccionados, indicando en este los recursos necesarios, los tiempos de desarrollo de los mismos y la prioridad de implementación de cada proyecto. Estos planes de proyectos de seguridad de la información son identificados y definidos en conjunto entre el Líder del SGSI y los responsables de los procesos y serán consolidados por el Líder del SGSI.



## 7.6 Monitoreo

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

Los riesgos son dinámicos como la misma Entidad por tanto podrán cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte:


- Nuevos activos o modificaciones en el valor de los activos
- Nuevas amenazas
- Cambios o aparición de nuevas vulnerabilidades
- Aumento de las consecuencias o impactos
- Incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.

## 7.7 Metodología

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos. De acuerdo con esto, se definen las siguientes fases de implementación del MSPI: 1. Diagnosticar 2. Planear 3. Hacer 4. Verificar 5. Actuar.





# 9 MEDICION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La medición se realiza con un indicador de gestión que está orientada principalmente en la medición de eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicador que se alimenta de indicadores internos en el marco de la implementación del Eje de Seguridad de la Información y que servirán como insumo para el componente de mejora continua permitiendo adoptar decisiones de mejora sobre Seguridad de la información.

## *9.1 Medición*

La medición se realiza diligenciando la matriz de seguimiento del MSPI, que está orientado principalmente a determinar el porcentaje de implementación de los controles definidos en el tratamiento de riesgos de seguridad y privacidad de la información.

No.	Evaluación de Efectividad de controles			EVALUACIÓN DE EFECTIVIDAD DE CONTROL
	DOMINIO	Calificación Actual	Calificación Objetivo	
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	95	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	100	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	100	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	89	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	100	100	OPTIMIZADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	90	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	90	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	100	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	100	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	50	100	EFFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	50	100	EFFECTIVO
A.18	CUMPLIMIENTO	100	100	OPTIMIZADO
<b>PROMEDIO EVALUACIÓN DE CONTROLES</b>		<b>90</b>	<b>100</b>	<b>OPTIMIZADO</b>

Ilustración 11 Efectividad de controles



Ilustración 12 Brecha

## AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2020	Planificación	40%	40%
	Implementación	19%	20%
	Evaluación de desempeño	17%	20%
	Mejora continua	16%	20%
<b>TOTAL</b>		<b>92%</b>	<b>100%</b>

Ilustración 13 Ciclo PHVA

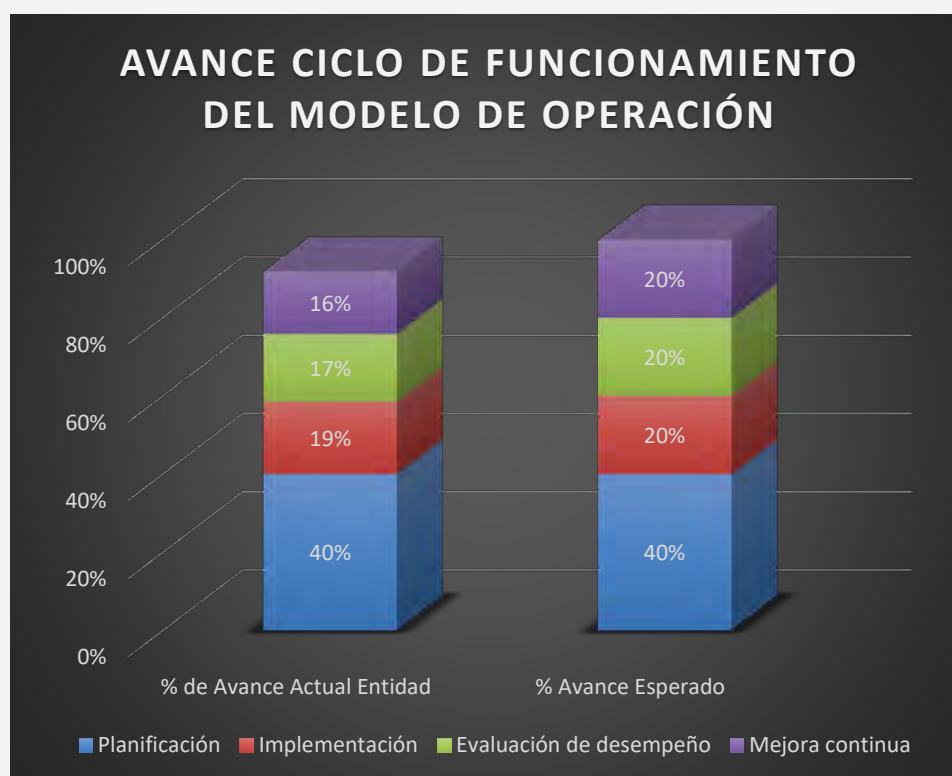


Ilustración 14 Modelo Operacion

## NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

### NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	NIVEL DE CUMPLIMIENTO		Nivel	Descripción	TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
	Inicial	SUFICIENTE	Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información	CRÍTICO	0% a 35%
	Repetible	SUFICIENTE	Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentran gestionados dentro del componente planificación del MSPI.	INTERMEDIO	36% a 70%
	Definido	SUFICIENTE	Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.	SUFICIENTE	71% a 100%
	Administrado	SUFICIENTE	Administrado	En este nivel se encuentran las entidades, que cuentan con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.		
	Optimizado	SUFICIENTE	Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.		

Ilustración 15 Nivel de Madurez

## 9.2 Normativa Aplicada

Guía de Gestión de riesgos. Guía No.7 (Seguridad y Privacidad de la Información) de MINTIC. “Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en la norma técnica colombiana NTC ISO/IEC 27001:2013.




# Glosario

- *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 controlar en su calidad de tal.*
- *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).*
- *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).*



- *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 reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).*
- *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 legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).*

- *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)*
- *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.*
- *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 o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).*
- *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).*

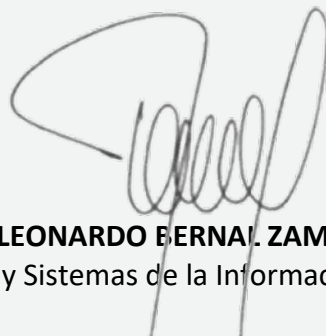


- *Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).*
- *Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación 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).*
- *Trazabilidad: Calidad 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).*

# Referencias bibliográficas

- *Norma técnica colombiana NTC-ISO /IEC 27005*
- *Norma técnica colombiana NTC-ISO /IEC 27005*
- *Metodología para la evaluación del desempeño de controles en sistema de gestión de seguridad de la información sobre la norma ISO/IEC 27001 de la Universidad Nacional, 2016*
- *Guía de gestión de riesgos, seguridad y privacidad de la información, MINTIC*
- *Manual integrado de gestión, SIG-UPTC, versión 31*
- *Procedimiento elaboración y control de documentos, SIG-UPTC, versión 13*
- *Guía aspectos generales de la documentación, SIG-UPTC, versión 3*
- *Guía para la gestión de riesgos de activos de información, SIG-UPTC, versión 7*

**Proyectó: Grupo de Gestión y Gobierno DTIC**



**LEONARDO BERNAL ZAMORA**

Director de Tecnologías y Sistemas de la Información y de las Comunicaciones