Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

UNIDAD DE PLANIFICACIÓN RURAL AGROPECUARIA UPRA

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

BOGOTA D.C., JULIO DE 2018

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

1. INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información de la UPRA, está plasmado en la implementación del Sistema de Gestión de Seguridad de la Información, a través del cual se aterriza el Modelo de Seguridad y Privacidad de la Información (MSPI), que a su vez se encuentra alineado con el Marco de Referencia de Arquitectura de TI y soporta transversalmente la Política de Gobierno Digital.

El Sistema de Gestión de Seguridad de la Información de la UPRA, permite fortalecer las capacidades de la entidad para gestionar, tratar y mitigar los riesgos a los cuales se encuentran expuestos sus activos de información, para tal fin se implementan controles técnicos y administrativos que junto con el uso de las mejores prácticas, aseguran la confidencialidad, integridad y disponibilidad de los activos de información de la UPRA, garantizando su buen uso y la privacidad de los datos.

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

2. ESTADO DEL ARTE.

La implementación del Sistema de Gestión de Seguridad de la Información de la UPRA, se realiza en base al modelo de mejora continua también conocido como Ciclo PHVA por sus siglas en español de Planear, Hacer, Verificar y Actuar, o ciclo PDCA por sus siglas en inglés de Plan, Do, Check y Act, o es conocido como el Circulo Deming, en honor a su autor Edward Deming, y se ha convertido día a día en la sistemática más usada para la implementación de un sistema basado en la mejora continua.

El modelo de mejora continua o ciclo PHVA, es una metodología que define en cuatro fases la estructura sistemática a seguir para lograr el mejoramiento continuo de la calidad, cuyos objetivos principales son la disminución de fallos, aumento de la eficacia y eficiencia, solución de problemas, previsión y eliminación de riesgos potenciales.

Las cuatro fases del ciclo PHVA son Planear, Hacer, Verificar y Actuar.

- Planear (Plan): en esta fase se definen los objetivos a alcanzar, basados en los procesos y actividades que se deseen mejorar continuamente.

- Hacer (Do): esta fase está dedicada a la ejecución de lo planeado, implantación de cambios propuestos para alcanzar los objetivos establecidos, para lo cual se debe contar con responsables y recursos necesarios para la ejecución del plan además se debe documentar el desarrollo de las actividades para dar inicio a la siguiente fase.

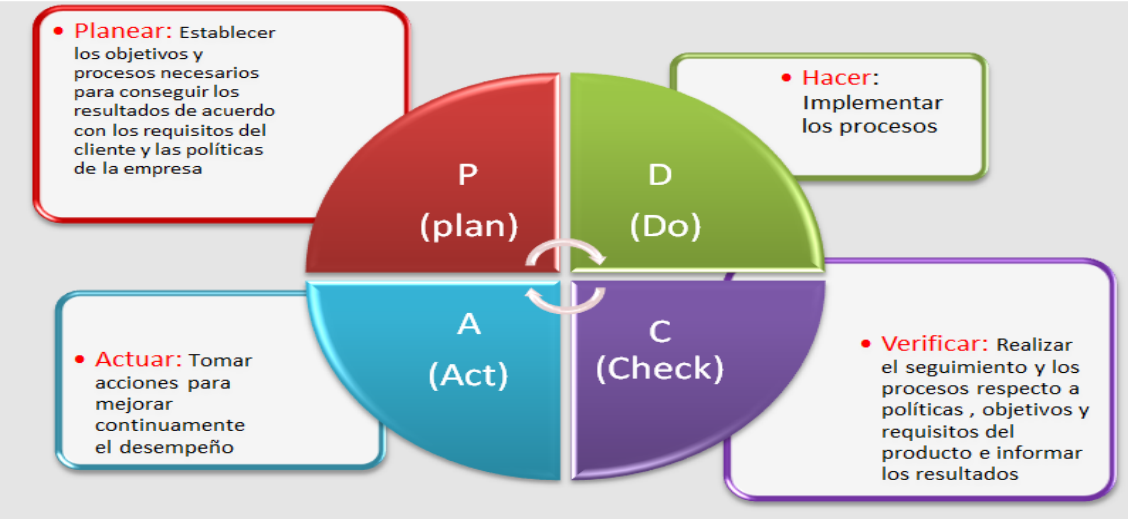
- Verificar (Check): esta fase se realiza mediante la adopción de mecanismos que permitan realizar el seguimiento y la verificación de las acciones adoptadas, a través de herramientas de indicadores y evaluación para determinar el grado de cumplimiento de lo planeado, se deben documentar los resultados obtenidos.

- Actuar (Act): tomando como insumo la documentación registrada en la verificación, se establecen las acciones correctivas, se documentan e inicia nuevamente el ciclo para continuar con la mejora continua.

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co



Con el fin de afianzar un marco de gestión de riesgos y proteger los activos de información de la Entidad, el Sistema de Gestión de Seguridad de la Información de la UPRA se encuentra alineado con con la norma ISO27000:2013 (estándar internacional, publicado por la International Organization for Standarization ISO), que certifica y proporciona el aseguramiento de la confidencialidad, la integridad y la disponibilidad de los activos de información de la UPRA, mediante la implementación de una estrategia integral de seguridad de la información que parta desde las políticas, prácticas y aborde toda la cadena de valor, en torno a los objetivos estratégicos de la Entidad, con el fin de diagnosticar, planear e implementar de manera coordinada acciones que sean pertinentes para que la UPRA cuente con un escenario donde se apliquen buenas prácticas en materia de seguridad de la información, que conlleven a la seguridad de los sistemas, los procesos, las personas que los ejecutan y los datos, bajo los únicos propósitos de reducir las vulnerabilidades a las que se encuentran expuestos los activos de información de la UPRA.

A continuación se describen las principales normas de seguridad de la familia ISO-27000.

- ISO 27001, esta norma define los requisitos de un Sistema de Gestión de Seguridad de la Información SGSI y es la norma en la cual se certifican los auditores externos. La Norma ISO27001 se basa en la gestión riesgos, para tal fin en el Anexo A se definen y agrupan los controles aplicables al tratamiento de los mismos en 11 dominios, como se demuestra en la siguiente tabla:

Control	Descripción
A.5	Política de Seguridad

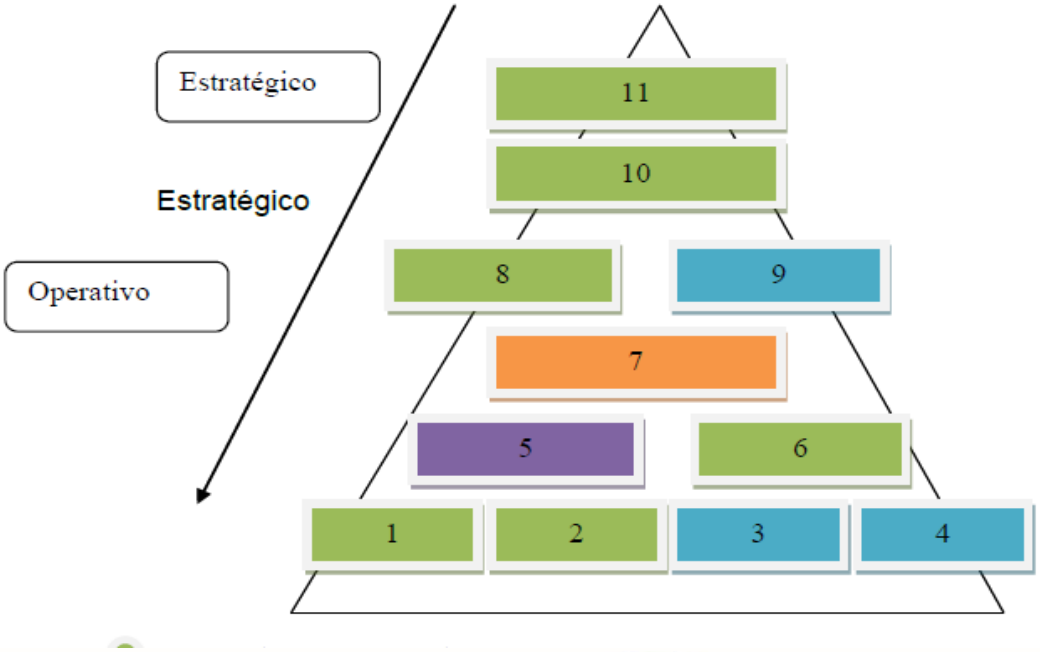
Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

A.6	Organización de la Información de Seguridad
A.7	Administración de recursos
A.8	Seguridad de los recursos humanos
A.9	Seguridad física y del entorno
A.10	Administración de las comunicaciones y operaciones
A.11	Control de accesos
A.12	Adquisición de sistemas de información, desarrollo y mantenimiento
A.13	Administración de los incidentes de seguridad
A.14	Administración de la continuidad de negocio
A.15	Cumplimiento (legales, de estándares, técnicas y auditorías)

En la siguiente gráfica se clasifican los controles del Anexo A, de acuerdo a su entorno de aplicación.



Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

1. Gestión de la continuidad del negocio.
2. Gestión de incidentes de seguridad de la información.
3. Gestión de comunicaciones y operaciones.
4. Adquisición, desarrollo y mantenimiento de sistemas de información.
5. Seguridad física y del entorno.
6. Seguridad en los recursos humanos.
7. Conformidad.
8. Gestión de activos.
9. Control de accesos.
10. Organización de la seguridad de la información.
11. Política de seguridad.

- ISO 27002, La norma ISO 27002 define los 114 controles que se deben considerar para la correcta Gestión de Riesgos de los activos de la organización, por lo tanto no se puede obtener una certificación de esta norma, ya que define las buenas practicas que se deben seguir para la implementación de un SGSI.

- ISO 27003, Al igual que la norma ISO-27002 no es certificable pero sirve de soporte a la norma ISO-27001 ya que establece lineamientos y directivas para la implementación de un SGSI y proporciona información acerca del uso del modelo de mejora continua PHVA y de los requerimientos de sus diferentes fases.

- ISO 27004, Define métricas y estándares para la medición de la eficacia del SGSI y de la eficiencia y efectividad de los controles implantados en la implementación del mismo.

- ISO 27005, Diseñada para realizar la gestión de riesgos de la seguridad de la información, es aplicable a todo tipo de organización.

- ISO 27006, Requisitos para las entidades de auditoría y requisitos específicos para la certificación de un SGSI.

- ISO 27007, Guía para auditar un SGSI.

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

3. METODOLOGÍA DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN.

3.1. Integración del SGSI con el SGI de la UPRA.

Dado que el Sistema de Gestión de Seguridad de la Información se enmarca dentro del Modelo de Mejora Continua, es uno de los elementos que se desarrollan en el Sistema de Gestión Integrado, por tal razón hace parte del manual del SGI de la UPRA.

3.2. Compromiso de la Dirección.

El Plan de Seguridad de la Información de la UPRA cuenta con el respaldo de la Dirección General, el cual se ve reflejado en la definición y actualización del alcance del SGSI, la política general y los objetivos de seguridad de la información.

3.3. Alcance del SGSI.

El alcance del SGSI de la UPRA se define en función de los procesos institucionales, su aplicación es responsabilidad de todos los empleados directos e indirectos, así como de aquellos terceros e involucrados internos y externos que tengan acceso a los diferentes activos de información de la unidad.

3.4. Política General de Seguridad de la Información.

La política de seguridad de la información de la UPRA, enmarca el que se va a proteger en términos generales, y se encuentra alineada con la política de calidad institucional, que a su vez debe apoya el cumplimiento de la misión. Está enfocada a la protección de los activos de información en términos de confidencialidad, integridad y disponibilidad y contempla la aplicación de diferentes contramedidas que permitan la gestión de los riesgos de seguridad de la información. Así mismo está alineada con los niveles de clasificación de los activos de información de la UPRA y no va en contravía con las leyes y normatividad aplicable al sector.

3.5. Objetivos Generales de Seguridad de la Información.

Los objetivos de seguridad de la información de la UPRA, definen cómo aplica la política general de seguridad de la información y contienen el compromiso de la dirección en la implementación y

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

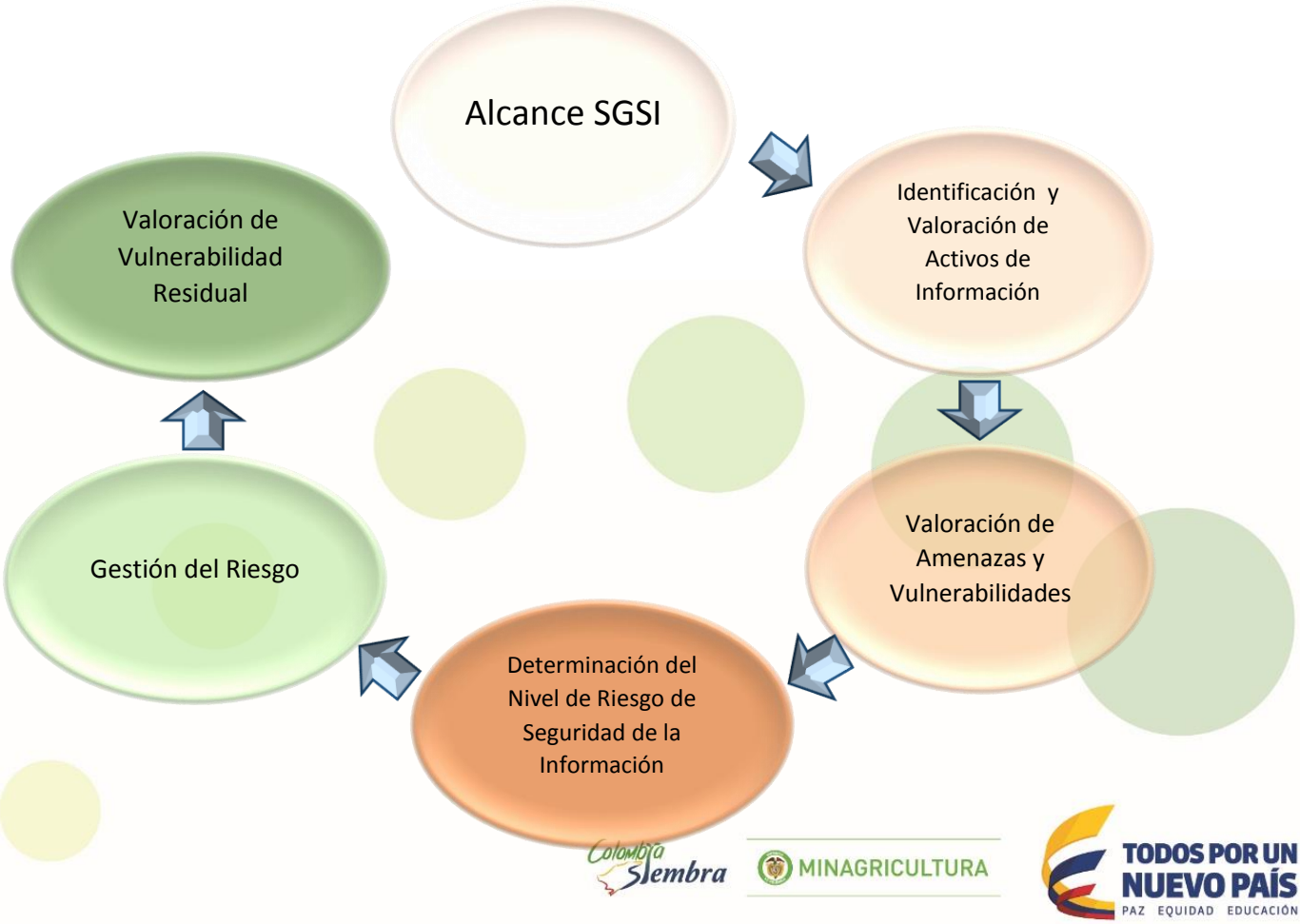
upra.gov.co

operación del SGSI, además de la disposición de recursos financieros, tecnológicos y humanos necesarios para tal fin; definen los requisitos de seguridad asociados al contexto de la unidad, las responsabilidades del personal frente al manejo de los activos de información, el esquema de comunicación de los aspectos asociados al Sistema de Gestión de Seguridad de la Información y la articulación del SGSI con el SGI.

4. GESTIÓN DE RIESGOS.

La gestión de riesgos de la UPRA, define como se realiza la identificación, análisis, valoración y gestión de riesgos de seguridad de la información del Sistema de Gestión de Seguridad de la Información (SGSI), con el propósito de obtener resultados reproducibles y comparables.

La evaluación de riesgos de seguridad de la información se basa en la ejecución de las actividades que se ilustran en siguiente Figura:



Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

4.1. Identificación y valoración de Activos de Información.

Esta fase inicia con la identificación del recurso humano responsable o dueño de los procesos contemplados en el alcance del SGSI, con quienes se recolecta la información necesaria para realizar la identificación y categorización de los activos de información, los cuales de acuerdo a la norma ISO 13335-1 , son definidos como "cualquier cosa que tiene valor para la organización" y extendiendo esta definición, a la metodología Magerit, que adopta el concepto que un activo corresponde a un componente o funcionalidad de un sistema de información susceptible de ser atacado con consecuencias para la organización, incluyendo dentro de éstos: información, datos, servicios, software, hardware, comunicaciones, recursos físicos y recursos humanos, se presenta la tabla de clasificación de activos de información, categorizados en la UPRA:

CATEGORÍA	DESCRIPCIÓN
Activos de Tipo Información	Toda aquella información de vital para el cumplimiento de los objetivos de la entidad, cuya producción o consecución y almacenamiento requiere recursos económicos, tecnológicos y humanos, también se incluye la información personal privada según la Ley de Protección de Datos
Activos de Tipo Físico	Son todos aquellos elementos físicos que soportan los procesos de tratamiento de información de la unidad.
Activos de Tipo Servicio	Servicios intangibles prestados o consumidos por la unidad relacionados con la seguridad o sus procesos.
Activos Tipo Persona	Recurso humano involucrado en los procesos.
Activos Tipo Software	Software utilizado en las actividades propias del proceso.
Activos Tipo Proceso	Están compuestos por el desarrollo de las actividades necesarias para cumplir con la misión de la unidad.
Activos Tipo Red	Elementos de infraestructura de telecomunicaciones.

Una vez identificados y categorizados los activos de información en la UPRA, se realiza la valoración de los mismos mediante un análisis de impacto, dicho análisis se realiza teniendo como ejes los atributos de Confidencialidad, Integridad y Disponibilidad; el atributo de confidencialidad es definido de acuerdo a la norma ISO/IEC 13335-1, como "la propiedad de que la información no esté disponible o no sea revelada a personal, entidades o procesos no autorizados"; de igual manera, la citada norma define el atributo de integridad como "la propiedad de salvaguardar la exactitud y completitud de los activos de

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

información para su correcto uso en los procesos de negocio"; por su parte, el atributo de disponibilidad, es definido en la norma citada como "la propiedad de hacer accesible y utilizable la información por una entidad autorizada en el momento preciso". Dicha valoración es realizada por los propietarios de los procesos a los que pertenecen los activos que se están valorando, evaluando el efecto que tendría en la unidad la pérdida de los atributos descritos previamente.

Para realizar la valoración de los activos de información de la entidad, se utilizó la siguiente tabla, la cual sirve de guía a los responsables para realizar una valoración cuantitativa de acuerdo al impacto que puede producir a la UPRA, la perdida de la confidencialidad, integridad y/o disponibilidad, esta valoración se realiza sin tener en cuenta medidas de seguridad aplicadas.

Valoración en Confidencialidad/Integridad/ Disponibilidad	Descripción	Justificación.
5	Esta valoración es la más alta que se le puede asignar a los activos de información de la UPRA y se evalúan todos aquellos que son necesarios para la supervivencia de la misma, quiere decir que se deben garantizar los tres atributos para que no se vea amenazada la supervivencia de la organización	El propietario deberá justificar el porqué de su valoración, ya que durante la fase hacer, estos activos de información serán los primeros a los que se les aplique medidas de seguridad.
4	La pérdida de alguno de los atributos ocasiona un daño grave en la unidad	No requiere justificación.
3	Daño considerable	No requiere justificación.
2	Daño menor	No requiere justificación.
1	Daño Insignificante	No requiere justificación.

Para realizar una valoración acertada del impacto que genera en la UPRA la pérdida de los atributos de los activos, es necesario establecer las dependencias entre los activos de información, estableciendo un grado jerárquico entre los mismos, así:

- Información
- Servicio
- Software
- Físicos
- Red
- Personal
- Etc.

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

El anterior esquema se interpreta de la siguiente manera:

La información depende de los servicios, los servicios dependen del software, el software de equipos físicos, los elementos físicos requieren una infraestructura de telecomunicaciones, la infraestructura depende de personal. Esto quiere decir que las relaciones de dependencia se establecen en un único nivel.

4.2. Valoración de amenazas y vulnerabilidades.

Una amenaza es definida de acuerdo a la norma ISO/IEC 13335-1 como una causa potencial de un incidente no deseado, la cual puede ocasionar daño a un sistema o a la organización. Existen amenazas de origen natural (terremotos, inundaciones, etc.), industrial (fallos eléctricos, fugas de líquidos, etc.), de aplicaciones (defectos de diseño o de funcionalidad técnica), causadas de forma accidental (errores u omisiones) o causadas de forma deliberada (actos deliberados y en búsqueda de beneficio).

Por otro lado una vulnerabilidad es definida igualmente por la norma ISO/IEC 13335-1 como una debilidad de un activo o un conjunto de activos, la cual puede ser explotada por una amenaza. Las vulnerabilidades corresponden a defectos en las medidas de protección que deben garantizan la protección del valor del activo de información.

El conjunto de amenazas y vulnerabilidades están asociadas a los diferentes tipos de activos de información de la organización.

Con el fin de realizar el análisis de riesgos de seguridad de la información sobre los activos de información de una organización, la norma ISO/IEC 27005 incorpora un conjunto de amenazas y vulnerabilidades, las cuales deben ser tenidas en cuenta para la valoración de amenazas y vulnerabilidades relacionadas con los mismos, la metodología de evaluación de riesgos valora los riesgos resultantes de amenazas de carácter interno y externo, ya sean deliberadas o accidentales que aplican sobre los activos de información identificados con cada propietario. La aplicabilidad de un riesgo sobre un activo de información depende de la existencia de la vulnerabilidad sobre este.

La evaluación de amenazas y vulnerabilidades se realiza de acuerdo a las amenazas contenidas en la norma de referencia ISO/IEC 27005, con el fin de priorizar dichas amenazas de acuerdo a los requisitos de la entidad, el equipo encargado de tal actividad está conformado por el Oficial de Seguridad de la

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

Información y los líderes de procesos propietarios de los activos de información. Para tal fin se utiliza la siguiente tabla:

Nivel de Amenaza	Descripción	Justificación.
3	La amenaza se considera presente en el entorno de la unidad y la probabilidad de que explote vulnerabilidades propias de los activos de información identificados es alta, ya que se ha evidenciado una o más veces al año.	No se requiere justificar, ya que se puede comprobar la ocurrencia de la amenaza.
2	La amenaza se considera presente en el entorno de la unidad y con probabilidad media de que explote vulnerabilidades propias de los activos de información identificados, ya que se ha evidenciado al menos una vez en los últimos dos años	No se requiere justificar, ya que se puede comprobar la ocurrencia de la amenaza.
1	La amenaza se considera presente en el entorno de la unidad y con baja probabilidad de que explote vulnerabilidades propias de los activos de información identificados, ya que se ha evidenciado al menos una vez o no se ha presentado en los últimos cinco años.	Requiere justificación ya que no existen evidencias de su ocurrencia.
0	La amenaza no está presente en el entorno de la unidad, por lo tanto no afectaría los activos de información identificados.	Requiere justificar por qué no está presente la amenaza en el entorno.

Una vez realizada la valoración de las amenazas, se evalúa cada vulnerabilidad en función del grado de cumplimiento de los controles de seguridad que la mitigan, según guías de implantación ISO/IEC 27002:20013. Los controles de seguridad también denominados contramedidas o salvaguardas de acuerdo a la norma ISO/IEC 13335-1 corresponden a prácticas, procedimientos, o mecanismos que tratan el riesgo de seguridad de la información. Existen controles de tipo correctivo (cuando la amenaza ya se ha materializado y el control corrige el evento antes de que se produzcan pérdidas), detectivo (cuando se identifica un riesgo pero no se corrige), disuasorio (ofrece un efecto disuasivo para reducir la probabilidad de materialización de un riesgo) o preventivo (evita la ocurrencia de un riesgo, detiene la materialización de una amenaza).

Valoración de la Probabilidad de la Vulnerabilidad	Descripción	Justificación

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

5	Sin importar si el control ha sido implantado, la vulnerabilidad ha sido explotada en el pasado. Las vulnerabilidades clasificadas en este nivel son todas aquellas para las cuales existen evidencias de que un control ha sido implantado y/o el mismo se encuentra documentado, pero en ninguno de los dos casos ha sido efectivo para evitar la explotación de las vulnerabilidades.	No requiere.
4	Es probable que la vulnerabilidad sea explotada a corto, mediano o largo plazo, ya que no existen evidencias de que se haya implantado algún control y tampoco ha sido documentado, por lo tanto no se puede determinar si es efectivo.	No requiere
3	Es probable que la vulnerabilidad sea explotada a corto, mediano o largo plazo, ya que el control ha sido implantado de forma parcial, esto quiere decir que existen evidencias de que el control ha sido implantado y/o se encuentra documentado, pero no es efectivo.	Requiere justificación.
2	Es poco probable que la vulnerabilidad sea explotada a corto, mediano o largo plazo, ya que el control está implantado, es decir, que existen evidencias de su aplicación y se puede comprobar su efectividad, aunque no se encuentre documentado.	Requiere justificación.
1	Es muy improbable que la vulnerabilidad sea explotada ya que el control se encuentra implantado y auditado, es decir, existen evidencias de su aplicación, está documentado y se ha comprobado su efectividad.	Requiere.
0	La vulnerabilidad no se encuentra asociada al activo, lo que quiere decir que no es necesario aplicar el control	Requiere.

4.3. Determinación del Nivel de Riesgo de Seguridad de la Información.

El nivel de riesgo de seguridad de la información de los activos de información identificados en la UPRA, es el producto resultante de multiplicar la valoración de los activos de información, el nivel de amenaza y la valoración de la probabilidad de la vulnerabilidad, es decir: Nivel de Riesgo = Valoración del Activo * Nivel de Amenaza * Vulnerabilidad

Debido a que la valoración de los activos de información de la entodad fue realizada por los propietarios de los procesos, dicha valoración es estática durante el ciclo de vida del análisis de riesgo, no obstante en la revisión periódica que se hace sobre los activos esta valoración puede ser modificada, evaluando si la pérdida de alguno de sus atributos (confidencialidad, integridad y disponibilidad) representa un

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

impacto mayor o incluso menor por cambios en el sistema, por ejemplo debido a nuevas regulaciones legales o contractuales. La metodología de evaluación de riesgos consiste en comparar las medidas de seguridad implantadas actualmente, con los controles de seguridad de la información establecidos en el anexo A de la norma NTC-ISO/IEC 27001:2013, e identificar y gestionar las vulnerabilidades existentes o potenciales en los procesos y sistemas de información de la unidad.

De acuerdo a lo anterior los niveles de riesgo calculados para cada activo de información de la UPRA, se ubican en el siguiente mapa de calor de acuerdo a la Metodología para la Gestión de Riesgos de Seguridad de la Información.

		NIVEL DE AMENAZA														
		1					2					3				
	NIVEL DE VULNERABILIDAD	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
VALORACIÓN DEL ACTIVO	1	1	2	3	4	5	2	4	6	8	10	3	6	9	12	15
	2	2	4	6	8	10	4	8	12	16	20	6	12	18	24	30
	3	3	6	9	12	15	6	12	18	24	30	9	18	27	36	45
	4	4	8	12	16	20	8	16	24	32	40	12	24	36	48	60
	5	5	10	15	20	25	19	20	30	40	50	15	30	45	60	75
		NIVEL DE RIESGO														

La forma como se interpretan los datos reflejados en el mapa de calor es la siguiente:

NIVEL DE RIESGO	DESCRIPCIÓN
1 - 24	No se requiere implantar controles ya que el nivel de riesgo es bajo.
25-48	La alta dirección de la organización determina el nivel de riesgos aceptables y cuales deberán ser tratados.
49-75	El nivel de riesgos no es aceptable, y sólo se podrán excluir controles que los mitiguen justificando dicha exclusión por parte de la dirección de la entidad. El Oficial de Seguridad de la Información de la UPRA determina los controles que tendrán que aplicarse para mitigar los riesgos.

4.4. Gestión del Riesgo.

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

Para la gestión de riesgos se establecen cuatro métodos:

- ACEPTAR EL RIESGO: La Dirección General de la UPRA puede aceptar riesgos que no serán tratados en los siguientes casos:

  a) El riesgo sea menor o igual al nivel de riesgo aceptable.

  b) El coste de tratar el riesgo sea mayor que el impacto del daño en la entidad.

  c) La unidad no cuenta con los recursos necesarios para tratar el riesgo.

- TRATAR EL RIESGO: La Dirección General de la UPRA determina la prioridad en la implantación de las medidas de tratamiento de riesgo, en proporción al nivel de riesgo, la facilidad de la implantación, el coste o a los cambios en la organización, para tal fin se tienen los siguientes escenarios:

  a) Cuando el riesgo es ALTO ($R \geq 49$): Si el nivel de riesgo resultante para un activo es igual o superior a 49, la Dirección General debe apoyarse en la norma NTC-ISO/IEC ISO 27001:2013 Anexo A, para seleccionar los objetivos de control y controles que mitiguen el riesgo a un nivel aceptable y que encajen con los requisitos establecidos por la organización. En relación a los activos y a sus vulnerabilidades/amenazas asociadas, se implantarán todos los controles adicionales que tengan un efecto positivo en el negocio o en los procesos existentes y cuyo coste sea aceptable. Se determina que un riesgo ALTO es inaceptable para la organización, a menos que así lo decida la dirección general y sobre el que dependa la propiedad y el derecho de uso del activo afectado mediante la justificación de dicha decisión.

  b) Cuando el riesgo es MODERADO ($25 \leq R \leq 48$): el Oficial de Seguridad de la Información y el jefe de la oficina TIC de la UPRA podrán aceptar un riesgo con un nivel entre 25 y 48 por cualquiera de las razones expuestas a continuación:

  - El control o el proceso asociado no está alineado con la cultura de la unidad o va en contravía del modelo de dirección.
  - No se cuentan con los recursos económicos y humanos necesarios.
  - No existe un beneficio claro para la unidad.
  - El coste de implantación del control supera el coste del activo que protege o el coste de una brecha de seguridad actual o futura.

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

La aceptación del riesgo es documentada en el Análisis de Riesgos institucional. En caso de no aceptación del riesgo, se actuará, como se indica para el caso de riesgo ALTO, seleccionando los procedimientos, mejores prácticas y mecanismos que mitiguen el riesgo a un nivel aceptable.

c) Cuando el riesgo es BAJO (R ≤ 24): Los niveles de riesgo entre 1 y 24 son bajos y no requieren actuación ninguna.

- TRANSFERIR EL RIESGO: Cuando sea conveniente, la UPRA podrá transferir el riesgo a terceros. La oficina TIC debe asegurarse que las responsabilidades que han sido transferidas son proporcionales al riesgo y de que sus colaboradores, proveedores o socios de negocio están conscientes de dichas responsabilidades. En caso de optar por transferir un riesgo, las acciones tomadas deben quedar documentadas y ser revisadas.

- EVITAR EL RIESGO: Este caso solamente puede darse mediante la eliminación o modificación de los procesos y/o actividades a los que pertenecen los activos cuyo riesgo se desea evitar, para tal fin una, vez realizada alguna de las acciones mencionadas se realizará el análisis de riesgos específico y se los resultados obtenidos.

4.5. Valoración de Vulnerabilidad Residual.

El riesgo residual para cualquiera de los activos y una vez aplicados las medidas de control previstas se sitúan en un rango de valores por debajo del valor de riesgo aceptable determinado por la Dirección General.

Para aquellos casos en que, tras el tratamiento con los controles previstos, se determina un nivel de riesgo moderado, se debe obtener la aprobación de la Dirección General para aceptar el riesgo residual resultante, lo cual queda documentado.

Para realizar la valoración de la vulnerabilidad residual se utiliza la siguiente tabla:

Vulnerabilidad Residual	Descripción	Justificación
3	La vulnerabilidad residual es parcial ya que el activo ha sido evaluado metodológicamente y se ha decidido aceptar su riesgo.	No requiere.
2	Es poco probable que la vulnerabilidad residual sea explotada a corto, mediano o largo plazo, ya que el conjunto de controles aplicables estará implantado.	No requiere.

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

1	Es muy improbable que la vulnerabilidad residual sea explotada, ya que el conjunto de controles estará implantado y auditado.	No requiere
0	La vulnerabilidad residual no aplica al activo porque la amenaza no aplica, o porque el conjunto de controles no aplica.	No requiere

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

5. PLAN DE TRATAMIENTO DE RIESGOS.

El Plan de Tratamiento de Riesgos de la UPRA, identifica las acciones, responsables, recursos y prioridades en la gestión de los riesgos de seguridad de la información ya identificados, lo cual es aterrizado en una serie de políticas y procedimientos aplicados en la entidad.

5.1. Políticas de Seguridad de la Información.

Aportan en la implementación de los controles de Seguridad identificados en el Análisis de Riesgos realizado, y de acuerdo a la familia del control 5 de norma ISO 27002, "Política de Seguridad, la organización debe establecer las políticas de seguridad asociadas a diferentes dominios específicos de la seguridad de la información, abordando aspectos de la seguridad organizativa, lógica, física y legal, que permitan realizar una eficiente gestión de los activos de información identificados y valorados por los propietarios de los procesos, de tal forma que se vele por el adecuado aseguramiento de la información.", en este sentido la UPRA ha definido el Manual de de Políticas de Seguridad de la Información, las cuales se encuentran alineadas con el alcance del SGSI, es decir son aplicables a los procesos y procedimientos de alcance del SGSI.

Entre las políticas de seguridad de la información de la UPRA, se encuentran:

- Política de Contraseñas
- Política de uso aceptable de activos
- Política de control de acceso
- Política de Backups
- Política de Retiro de Activos
- Política de entornos de desarrollo, pruebas y producción
- Política de borrado seguro
- Política de centro de datos
- Política de seguridad física y del entorno
- Política de control de cambios
- Política de gestión de medios removibles
- Política de continuidad y gestión de continuidad del negocio

5.2. Procedimientos

Calle 28 no. 13-22
Torre C, piso 3
Edificio Palma Real
Bogotá, Colombia

(571) 552 9820
(571) 245 7307
direccion@upra.gov.co

upra.gov.co

Si bien las políticas definidas en la UPRA establecen el qué, mediante procesos y procedimientos se establecen actividades del cómo ponerlas en funcionamiento, para lo cual la UPRA cuenta con procedimientos para:

- Soporte y Asistencia Técnica.
- Copias de Respaldo
- Gestión de servicios tecnológicos
- Actualización o modificación de componentes de TI.
- Gestión de situaciones de seguridad de la información
- Mantenimiento preventivo y/o correctivos de bienes e IT.

5.3. Formación.

La UPRA desarrolla jornadas de sensibilización y comunicación que permiten involucrar a todos los actores que forman parte de la implementación del SGSI, a través de la creación de conciencia y entendimiento de los mismos, enmarcadas en diferentes temáticas de seguridad de la información, dando cumplimiento al control 7.2.2 de la Norma ISO 27002 "Concientización, educación y capacitación de la seguridad de la información".

El diseño y desarrollo de la estrategia de sensibilización, tiene como objetivo aportar en el desarrollo de las actividades que giran alrededor de la formación de competencias en los colaboradores de la unidad, que les sirva de base en la toma de decisiones acertadas y bien informadas sobre los temas de seguridad de la información, sus actuaciones y responsabilidades que se generen.

5.4. Clasificación de la Información.

Durante la implementación del SGSI de la UPRA, se definió la guía de clasificación de la información, que permite dar cumplimiento de los controles A.8.2.1, A.8.2.2 y A.8.2.3 del Anexo A de la norma ISO27001:2013. La guía comprende los niveles de clasificación de la información de la entidad, los roles identificados en el manejo de la información y el tratamiento indicado para cada nivel de clasificación.

5.5. Sistema de Métricas.

La UPRA cuenta con indicadores que permiten obtener resultados para medir la eficacia de los controles implantados, alineados con el SGI de la unidad y aplicados a la implementación del Modelos de Seguridad y Privacidad de la Información, que permiten asegurar un proceso de mejoramiento continuo en la aplicación de los controles requeridos para la gestión de los riesgos de seguridad de la información identificados en los activos de información.