PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

OFICINA DE SISTEMAS

DIRECCIÓN ADMINISTRATIVA Y FINANCIERA

2021

1. INTRODUCCIÓN

Actualmente, la información es considerada como uno de los activos más importantes y por lo tanto valioso dentro de una organización, siempre y cuando sea utilizada de manera adecuada, integra, segura, oportuna y de manera responsable, lo que implica, que se hace necesario que dichas organizaciones posean o implementen una adecuada gestión de los recursos y activos de información que aseguren y controlen el acceso, tratamiento y uso de la información.

El aseguramiento y la protección de la seguridad de la información de las organizaciones y de los datos de carácter personal de los usuarios, representan un reto al momento de pretender garantizar su confidencialidad, integridad, disponibilidad y privacidad, razón por la cual, la seguridad de la información se ha convertido en uno de los aspectos de mayor preocupación a nivel mundial.

Debido a los múltiples riesgos y amenazas que hoy en día atentan contra la seguridad de la información y la protección y privacidad de los datos, es fundamental que las organizaciones establezcan, implementen, mantengan y mejoren continuamente un sistema de gestión de seguridad de la información basado en los riesgos y a su vez, alineado con los objetivos estratégicos y necesidades tanto del negocio como de sus partes interesadas.

AGUAS DEL CESAR S.A. E.S.P. es consciente que la protección y aseguramiento de su información es fundamental para garantizar su debida gestión financiera, administrativa y operativa, razón por la cual debe establecer un marco normativo de Seguridad de la Información que contemple políticas, límites, responsabilidades y obligaciones frente a la seguridad y privacidad de la información de la entidad.

En atención a lo anterior, la entidad asumió el reto de implementar el Sistema de Gestión de Seguridad de la Información (SGSI), siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) de la Estrategia de Gobierno en Línea, a su vez reglamentado a través del Decreto 1078 de 2015 para el sector de tecnologías de la información y comunicaciones y el Decreto 2573 de 2014 por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea.

2. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Definición

Mediante esta política de Seguridad y Privacidad de la Información, la empresa Aguas del Cesar S.A. E.S.P., muestra su posición frente a la protección de los activos de la información que soportan todos los procesos de la Entidad y a su vez, apoya la implementación del SGSI por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

2.1 OBJETIVO

Implementar el Plan de Seguridad y Privacidad de la Información, el cual es un documento que muestra la posición de la empresa Aguas del Cesar S.A. E.S.P., frente a la protección de los activos de la información que soportan todos los procesos de la Entidad y a su vez, apoya la implementación del SGSI por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

2.2 OBJETIVOS ESPECÍFICOS

Con la implementación de esta política la empresa Aguas del Cesar S.A. E.S.P., busca garantizar un direccionamiento estratégico enfocado en:

- ✓ Cumplir con la política de Seguridad de la Información.
- ✓ Disminuir cualquier riesgo tecnológico que pueda afectar la entidad.
- ✓ Generar seguridad y confianza entre los funcionarios, contratistas y terceros.
- ✓ Innovar en el campo tecnológico.
- ✓ Proteger los activos de la información de la entidad.
- ✓ Implementar el Sistema de Gestión y Seguridad de la Información - SGSI.
- ✓ Fomentar el buen uso de la seguridad de la información en los funcionarios, contratistas y clientes de la empresa.
- ✓ Garantizar la continuidad del servicio ante cualquier incidente, mediante el uso eficiente y seguro de los activos de la información.

2.3 ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

La política de Seguridad y Privacidad de la Información es aplicable a todos los niveles y procesos de la entidad, servidores públicos, contratistas y terceros que estén relacionados con la empresa Aguas del Cesar S.A. E.S.P.

2.4 BASE LEGAL

Decreto 1151 de 2008 se estableció como objetivo de la Estrategia Gobierno en Línea "Contribuir con la construcción de un Estado más eficiente, más transparente y participativo, y que preste mejores servicios a los ciudadanos y a las empresas, a través del aprovechamiento de las Tecnologías de la Información y la Comunicación". La política de Gobierno Digital establecida mediante el Decreto 1008 de 2018 (cuyas disposiciones se compilan en el Decreto 1078 de 2015, "Decreto Único Reglamentario del sector TIC", específicamente en el capítulo 1, título 9, parte 2, libro 2), forma parte del Modelo Integrado de planeación y Gestión (MIPG).

La política de Gobierno Digital tiene como ámbito de aplicación, las entidades que conforman la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas.

3. LA ENTIDAD

3.1 MISIÓN

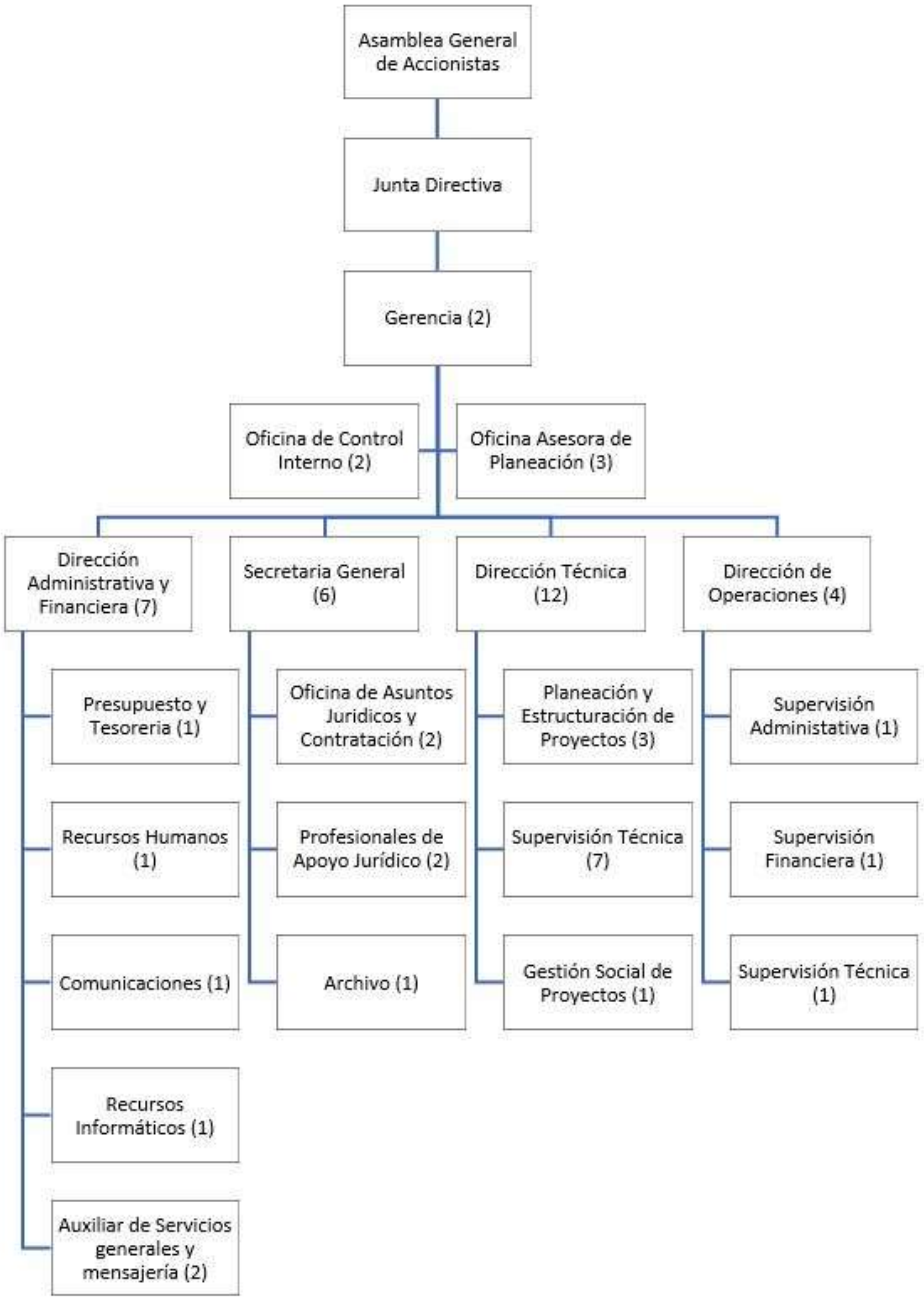
Liderar articuladamente las políticas de Agua Potable, Saneamiento Básico y Desarrollo Sostenible con efectividad para la gestión y operatividad de la prestación satisfactoria de los servicios públicos del Sector en el Departamento del Cesar.

3.2 VISIÓN

En el 2022 AGUAS DEL CESAR S.A. E.S.P., seguirá liderando la gestión de estrategias y acciones encaminadas a garantizar la prestación eficiente y eficaz de los servicios públicos del sector Agua Potable y Saneamiento Básico para el Desarrollo Económico, Social y Ambiental Sostenible de las comunidades del Departamento del Cesar.

3.3 ESTRUCTURA ORGANIZACIONAL

Mediante Acta de Junta Directiva Número 035 del 13 de septiembre de 2013, se aprobó la Nueva Estructura Organizacional de la Empresa Aguas del Cesar S.A. E.S.P., con su respectiva planta de personal y del Manual de Funciones y Competencias Laborales de la entidad.



4. IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD

"La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse al componente de TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

La Seguridad y Privacidad de la Información se alinea al componente de TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Entidad, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

El componente de TIC para Gobierno Abierto se alinea con el componente de Seguridad y Privacidad de la Información que permite la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal forma que los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables." [1]

[1] Modelo de Seguridad y Privacidad, MINTIC, Pág. 20

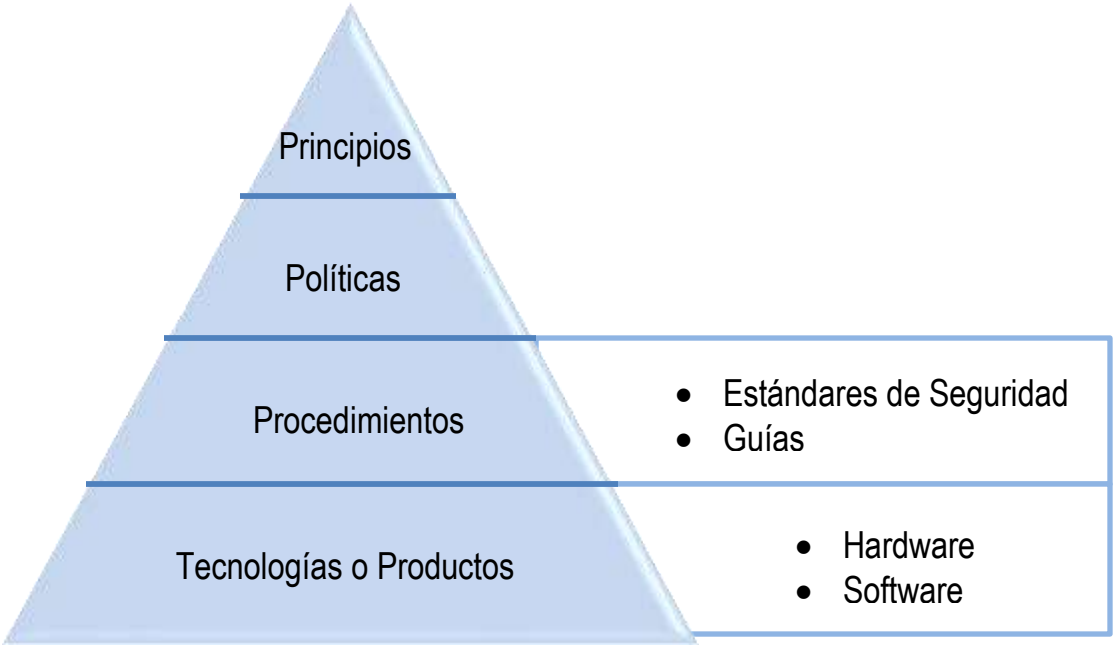
4.1 CICLO DE OPERACIÓN

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

- **Diagnóstico:** En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.
- **Planificación:** Para el desarrollo de esta fase la entidad debe utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional de la entidad, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.
- **Implementación:** Esta fase le permitirá a la Entidad, llevar acabo la implementación de la planificación realizada en la fase anterior del MSPI.
- **Evaluación de Desempeño:** El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.
- **Mejora Continua:** En esta fase la Entidad debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

4.2 DESCRIPCIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN

En el ámbito de la Seguridad de la información, los componentes del sistema se ubican en diferentes niveles de acuerdo con su importancia, a continuación se ilustran dichos componentes:



4.3 FASE DE DIAGNÓSTICO

OBJETIVO

Identificar el estado de la Entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

METAS	ACTIVIDADES - INSTRUMENTOS - RESULTADOS
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	• **Diagnóstico** de la **situación actual** de la entidad con relación a la gestión de seguridad de la información. • **Diagnostico nivel de cumplimiento** de la entidad frente a los objetivos de control y controles establecidos. • **Valoración estado actual** de la gestión de seguridad de la entidad con base en el Instrumento de Evaluación MSPI de MINTIC.
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.	• **Valoración** del **nivel de estratificación** de la entidad frente a la seguridad de la información **con base en** el método planteado en el documento '*ANEXO 3: ESTRATIFICACIÓN DE ENTIDADES*' del modelo seguridad de la información para la estrategia de Gobierno en Línea 2.0. • **Valoración** del **nivel de madurez** de seguridad y privacidad de la información en la entidad de acuerdo con los lineamientos establecidos en el capítulo '*MODELO DE MADUREZ*' del documento Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea.
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	• **Ejecución prueba de vulnerabilidades** con el fin de identificar el nivel de seguridad y protección de los activos de información de la entidad y definición de planes de mitigación.

Para la recolección de la información, en esta fase se utilizarán mecanismo como:

• Documentación existente en el sistema de calidad de la entidad relacionada con la información de las partes interesadas de la entidad y los roles y funciones asociados a la seguridad de la información.

• Fuentes externas, como las guías de autoevaluación, encuesta y estratificación dispuestas por la estrategia de gobierno en línea Ministerio de Tecnologías de la Información y las Comunicaciones.

4.4 FASE DE PLANIFICACIÓN

OBJETIVO

Definir la estrategia metodológica, que permita establecer el alcance, objetivos, procesos y procedimientos, pertinentes a la gestión del riesgo y mejora de seguridad de la información, en procura de los resultados que permitan dar cumplimiento con las metas propuestas del SGSI.

METAS	ACTIVIDADES - INSTRUMENTOS - RESULTADOS
Realizar un análisis de Contexto y factores externos e internos de la Entidad en torno a la seguridad de la información.	• **Realizar** un **Análisis de Contexto** de la entidad entorno a la seguridad de la información con el fin de poder determinar las cuestiones externas e internas de la organización que son pertinentes para la implementación del Sistema de Gestión de Seguridad de la Información.
Definir el alcance del SGSI de la entidad.	• Definir el alcance del Sistema de Gestión de Seguridad de la Información 'SGSI' de la entidad aprobado por la Alta Dirección y socializado al interior de la Entidad. • Definir el alcance del SGSI, en el cual se establece los límites y la aplicabilidad del Sistema de Gestión de Seguridad de la Información.
Definir Roles, Responsables y Funciones de seguridad y privacidad de la información.	• Definir un marco de gestión que contemple roles y responsabilidades para la implementación, administración, operación y gestión de la seguridad de la información en la entidad. • Definir la estructura organizacional de la Entidad que contendrá los roles y responsabilidad
Definir la metodología de riesgos de seguridad de la información.	• Definir Metodología de Valoración de Riesgos de Seguridad. • Integrar la metodología definida con la metodología de riegos operativos de la entidad. • Implementar un sistema de información para la administración y gestión de los riesgos de seguridad de la entidad.
Elaborar las políticas de seguridad y privacidad de la información de la entidad.	• Elaborar Política General de Seguridad y Privacidad la cual debe ser aprobada por la Alta Dirección y socializada al interior de la Entidad. • Elaborar el manual de Políticas de Seguridad y Privacidad de la Información, que corresponde a un documento que contiene las políticas y los lineamientos que se implementaran en la Entidad con el objetivo de proteger la disponibilidad, integridad y confidencialidad de la información. Estas políticas deben ser aprobadas por la Alta Dirección y socializadas al interior de la Entidad.
Elaborar documentación de operación (formatos de procesos, procedimientos y documentos debidamente definidos y establecidos) del sistema de seguridad de la información.	Elaborar los documentos de operación del sistema de seguridad de la información, tales como: • Declaración de aplicabilidad • Procedimiento y/o guía de identificación y clasificación de activos de información. • Procedimiento Continuidad del Negocio, Procedimientos operativos para gestión de TI. • Procedimiento para control de documentos (SGI)

	• Procedimiento para auditoría interna (SGI) • Procedimiento para medidas correctivas (SGI) • Procedimiento para la gestión de eventos e incidentes de seguridad de la información. • Procedimiento para la gestión de vulnerabilidades de seguridad de la Información. • Entre otros.
Identificar y valorar activos de información.	• Realizar la identificación y valoración de los activos de información de la entidad de acuerdo con su nivel de criticidad de acuerdo con el alcance del SGSI. • Documentar el inventario de activos de información de la entidad.
Identificar, valorar y tratar los riesgos de seguridad de la información de la entidad.	• Realizar la identificación y valoración de los riesgos transversales de seguridad de la información y definir los respectivos planes de tratamiento. • Realizar la valoración de riesgos de seguridad de la información de acuerdo con el alcance del SGSI. • Definir los planes de acción que incluya los controles a implementar con el objetivo de mitigar los riesgos identificados en el proceso de valoración de riesgos.
Establecer plan de capacitación, comunicación y sensibilización de seguridad de la información.	• Elaborar plan anual de capacitación y sensibilización anual de seguridad de la información.

4.5 FASE DE IMPLEMENTACIÓN

OBJETIVO

Llevar acabo la implementación de la fase de planificación del SGSI, teniendo en cuenta para esto los aspectos más relevantes en los procesos de implementación del Sistema de Gestión de Seguridad de la Información de la entidad.

METAS	ACTIVIDADES - INSTRUMENTOS - RESULTADOS
Establecer el plan de implementación de seguridad de la información.	• Implementar el plan de implementación del modelo de seguridad y privacidad de la información el cual debe ser revisado y aprobado.
Ejecutar el plan de tratamiento de riesgos.	• Ejecutar el plan de tratamiento de los riesgos transversales de seguridad de la información identificados en la fase de planificación que fue presentado en el comité de riegos.
Establecer indicadores de gestión de seguridad.	• Definir los indicadores para medir la gestión del modelo de seguridad y establecer los mecanismos para su medición. Estos indicadores deben permitir verificar la eficacia y efectividad de los controles implementados para mitigar los riesgos de seguridad de la entidad.
Implementar procedimiento de gestión de eventos e incidentes de seguridad.	• Implementar el procedimiento y los mecanismos para la gestión de los eventos e incidentes de seguridad de la información.
Implementar procedimiento de gestión de vulnerabilidades.	• Implementar el procedimiento y los mecanismos para la gestión de vulnerabilidades seguridad de la información.
Ejecutar plan de capacitación y sensibilización de seguridad.	• Ejecutar el plan anual de capacitación, socialización y sensibilización de seguridad de la información.

4.6 FASE DE EVALUACIÓN

OBJETIVO	Evaluar el desempeño y la eficacia del SGSI, a través de instrumentos que permita determinar la efectividad de la implantación del SGSI.

METAS	ACTIVIDADES - INSTRUMENTOS - RESULTADOS
Ejecución de auditorías de seguridad de la información.	Ejecución de auditorías del modelo de seguridad y de temas normativos y de cumplimiento de seguridad de la información aplicables a la entidad, de acuerdo con el plan de auditoria revisado y aprobado por la Alta Dirección. Las auditorías internas se deberán llevar a cabo para la revisión del Sistema de Gestión de Seguridad 'SGSI' de la Información implementado en la entidad, con la finalidad de verificar que los objetivos de control, controles, procesos y procedimientos del SGSI cumpla con los requisitos establecidos.
Plan de seguimiento, evaluación y análisis de SGSI.	Elaboración documento con el plan de seguimiento, evaluación y análisis del SGSI revisado y aprobado por el Comité.

4.7 FASE DE MEJORA

OBJETIVO	Consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el SGSI

METAS	ACTIVIDADES - INSTRUMENTOS - RESULTADOS
Diseñar plan de mejoramiento.	Diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el Sistema de Gestión de Seguridad de la Información.

5. IMPLEMENTACIÓN DEL POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

5.1 JUSTIFICACIÓN

Aguas del Cesar S.A. E.S.P., con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.

La seguridad de la información se entiende como la preservación de las siguientes características:

- ✓ ***Confidencialidad:*** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- ✓ ***Integridad:*** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- ✓ ***Disponibilidad:*** Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.