	<p>I.E. FRANCISCO ABEL GALLEGO</p> <p>Taller # 1 Tecnología</p>	TECH
		2026
		II PERIODO

## RIESGOS DE SEGURIDAD

### Dominio uno: Seguridad y gestión de riesgos (security and risk management)

Todas las organizaciones deben desarrollar su propia postura de seguridad. La postura de **seguridad es la capacidad de una organización para gestionar la defensa de sus activos y datos críticos y reaccionar ante los cambios**. Los elementos del ámbito de la seguridad y la gestión de **riesgos** que afectan la postura de seguridad de una organización incluyen:

- ✓ **Metas y objetivos de seguridad**
- ✓ **Procesos de mitigación de riesgos:**

Disponer de procedimientos y normas adecuados para **reducir el impacto** de un riesgo como una violación.

- ✓ **Cumplimiento:**

Es el método para **desarrollar políticas** de **seguridad** interna de una organización, los **requisitos** reglamentarios y las **normas** independientes.

- ✓ **Planes de continuidad de negocio:**

La capacidad de mantener su productividad diaria mediante planes de recuperación ante desastres por riesgos.

- ✓ **Normas legales:**


Son diferentes en todo el mundo

- ✓ **Ética profesional y organizacional:**

Minimizar la negligencia, el fraude y el abuso

La **seguridad de la información, o InfoSec**, también está relacionada con este dominio y se refiere a un **conjunto de procesos establecidos para proteger la información**. Una organización puede utilizar manuales de estrategias e implementar capacitación como parte de su programa de seguridad y gestión de riesgos, según sus necesidades y el riesgo percibido. Existen muchos procesos de diseño de InfoSec, como:

- ✓ Respuesta a incidentes
- ✓ Gestión de vulnerabilidades
- ✓ Seguridad de la aplicación

	<p>I.E. FRANCISCO ABEL GALLEGO</p> <p>Taller # 1 Tecnología</p>	TECH
		2026
		II PERIODO

- ✓ Seguridad en la nube
- ✓ Seguridad de la infraestructura

Por ejemplo, un equipo de seguridad puede necesitar modificar el modo en que se trata la información de identificación personal (PII) para cumplir con el Reglamento General de Protección de Datos (GDPR) de la Unión Europea.

### Dominio dos: Seguridad de los activos (Asset security)


La seguridad de los activos implica la “**PROTEGER LOS ACTIVOS DIGITALES Y FISICOS**” **gestión de los procesos de ciberseguridad de los activos** de la organización, incluidos el **almacenamiento**, el **mantenimiento**, la **retención** y la **destrucción de datos físicos y virtuales**. Debido a que la pérdida o el robo de activos puede exponer a una organización y aumentar el nivel de riesgo, es esencial realizar un seguimiento de los activos y los datos que contienen. **Realizar un análisis del impacto de la seguridad, establecer un plan de recuperación y gestionar la exposición de los datos dependerá del nivel de riesgo asociado con cada activo**. Es posible que los analistas de seguridad deban almacenar, mantener y conservar datos mediante la **creación de copias de seguridad** para garantizar que puedan restaurar el entorno si un incidente de seguridad pone en riesgo los datos de la organización.

### Dominio tres: Arquitectura e ingeniería de seguridad (Security Architecture and Engineering)

Este dominio se centra en la **OPTIMIZAR LA SEGURIDAD DE LOS DATOS** **gestión de la seguridad de los datos**. Garantizar la implementación de herramientas, sistemas y procesos eficaces ayuda a **proteger los activos y los datos de una organización**. Los arquitectos e ingenieros de seguridad crean estos procesos.

Un aspecto importante de este dominio es el concepto de responsabilidad compartida. La **RESPONSABILIDAD COMPARTIDA** significa que **todas las personas involucradas asumen un papel activo en la reducción de riesgos durante el diseño de un sistema de seguridad**. Otros principios de diseño relacionados con este dominio, que se analizan más adelante en el programa, incluyen:

- ✓ Modelado de amenazas
- ✓ Mínimo privilegio
- ✓ Defensa en profundidad

	<p align="center"><b>I.E. FRANCISCO ABEL GALLEGO</b></p> <p align="center"><b>Taller # 1 Tecnología</b></p>	<b>TECH</b>
		<b>2026</b>
		<b>II PERIODO</b>

- ✓ Fallar de forma segura
- ✓ Separación de funciones
- ✓ Manténlo simple
- ✓ Confianza cero
- ✓ Confía, pero verifica

Un **ejemplo** de gestión de datos es el uso de una herramienta de gestión de eventos e información de seguridad (**SIEM**) para monitorear señales relacionadas con inicios de sesión o actividades del usuario inusuales que podrían indicar que un actor de amenazas está intentando acceder a datos privados.

#### **Dominio cuatro: Seguridad de las comunicaciones y redes (Communication and Network Security)**

Este dominio se centra en la **GESTIÓN Y PROTECCIÓN DE REDES FÍSICAS Y COMUNICACIONES INALÁMBRICAS**. Esto incluye comunicaciones in situ, remotas y en la nube.

Las organizaciones con entornos de trabajo remotos, híbridos y presenciales deben garantizar la seguridad de los datos, pero gestionar las conexiones externas para garantizar que los trabajadores remotos accedan de forma segura a las redes de la organización es un desafío. El diseño de controles de seguridad de la red (como el acceso restringido a la red) puede ayudar a proteger a los usuarios y garantizar que la red de una organización **se mantenga segura** cuando los empleados viajan o trabajan fuera de la oficina principal.

#### **Dominio cinco: Gestión de identidad y acceso (Identity and Access Management)**

El dominio de gestión de identidades y accesos (**IAM**) se centra en **MANTENER LA SEGURIDAD DE LOS DATOS**. Para ello, garantiza que las identidades de los usuarios sean confiables y estén autenticadas, y que el acceso a los activos físicos y lógicos esté autorizado. Esto ayuda a evitar el acceso de usuarios no autorizados y, al mismo tiempo, permite que los usuarios autorizados realicen sus tareas.


Components (IAM):

Identification: Proporciona nombre y usuario, tarjeta de acceso huella dactilar, biometría.

Autenticación: verificación de la identidad; contraseña o pin.

Autorización: se confirma la identidad del usuario y su nivel de acceso a la información.

Accountability: supervisión y registros de las acciones de los usuarios.

	<p>I.E. FRANCISCO ABEL GALLEGO</p> <p><b>Taller # 1 Tecnología</b></p>	TECH
		2026
		II PERIODO

Básicamente, IAM utiliza lo que se conoce como el principio del **MÍNIMO PRIVILEGIO**, que es el **concepto de otorgar solo el acceso y la autorización mínimos necesarios para completar una tarea**. Por ejemplo, se le puede pedir a un analista de ciberseguridad que se asegure de que los representantes de servicio al cliente solo puedan ver los datos privados de un cliente, como su número de teléfono, mientras trabajan para resolver el problema del cliente y que luego retiren el acceso cuando se resuelva el problema del cliente.

### **Dominio seis: evaluación y pruebas de seguridad (Security Assessment and Testing)**

El ámbito de evaluación y LA **REALIZACIÓN DE PRUEBAS CONTROL DE SEGURIDAD** se centra en **Recopilar Y Analizar Datos identificar y mitigar riesgos, amenazas y vulnerabilidades Y REALIZAR AUDITORIAS**. Las evaluaciones de seguridad ayudan a las organizaciones a determinar si sus sistemas internos son seguros o están en riesgo. Las organizaciones pueden emplear evaluadores de penetración, a menudo denominados "pen testers", para encontrar vulnerabilidades que podrían ser explotadas por un actor de amenazas.


Este **dominio sugiere que las organizaciones realicen pruebas de control de seguridad, así como también recopilen y analicen datos**. Además, enfatiza la importancia de **realizar auditorías de seguridad** para monitorear y reducir la probabilidad de una violación de datos. Para contribuir con este tipo de tareas, los profesionales de la ciberseguridad pueden encargarse de auditar los permisos de los usuarios para validar que estos tengan los niveles correctos de acceso a los sistemas internos.

### **Dominio siete: Operaciones de seguridad (Security Operations)**

El dominio de las operaciones de seguridad se centra en la **investigación de una posible violación de datos y la implementación de medidas preventivas** después de que se haya producido un incidente de seguridad. **Debe llevarse a cabo una investigación forense digital para identificar cuando cómo y por qué se produjo la brecha para mitigar futuros ataques**.

Esto incluye el uso de estrategias, procesos y herramientas como:

- ✓ Formación y sensibilización
- ✓ Informes y documentación
- ✓ Detección y prevención de intrusiones
- ✓ Herramientas SIEM
- ✓ Gestión de registros
- ✓ Gestión de incidentes
- ✓ Manuales de juego
- ✓ Análisis forense posterior a la violación
- ✓ Reflexionando sobre las lecciones aprendidas

	<p align="center"><b>I.E. FRANCISCO ABEL GALLEGO</b></p> <p align="center"><b>Taller # 1 Tecnología</b></p>	<b>TECH</b>
		<b>2026</b>
		<b>II PERIODO</b>

Los profesionales de la ciberseguridad que participan en este ámbito trabajan en equipo para gestionar, prevenir e investigar amenazas, riesgos y vulnerabilidades. Estas personas están capacitadas para gestionar ataques activos, como el acceso a grandes cantidades de datos desde la red interna de una organización, fuera del horario laboral normal. Una vez que se identifica una amenaza, el equipo trabaja diligentemente para mantener los datos y la información privados a salvo de los agentes de amenazas.

### **Dominio ocho: Seguridad en el desarrollo de software (Software Development security)**


El dominio de la **Seguridad Del Desarrollo De Software** se centra en el **uso de prácticas y pautas de programación seguras para crear aplicaciones seguras**. Tener aplicaciones seguras ayuda a brindar servicios seguros y confiables, lo que ayuda a proteger a las organizaciones y a sus usuarios.

La **seguridad debe incorporarse** en cada elemento del ciclo de vida del **desarrollo** de software, desde el **diseño** y el desarrollo hasta las **pruebas** y el lanzamiento. Para lograr la seguridad, el proceso de desarrollo de software debe tener la seguridad en mente en cada paso. La seguridad no puede ser una idea de último momento.

**Realizar pruebas de seguridad** de aplicaciones puede ayudar a **garantizar que se identifiquen y mitiguen las vulnerabilidades en consecuencia**. Es necesario contar con un sistema para probar las convenciones de programación, los ejecutables de software y las medidas de seguridad integradas en el software. Contar con **profesionales** de control de calidad y de **pruebas de penetración que se aseguren de que el software cumple** con los estándares de seguridad y rendimiento también es una parte esencial del proceso de desarrollo de software. Por ejemplo, a un analista de nivel inicial que trabaja para una empresa farmacéutica se le puede pedir que se asegure de que el cifrado esté configurado correctamente para un nuevo dispositivo médico que almacenará datos privados de pacientes.

#### **En resumen:**

En esta lectura, **aprendió** más sobre las áreas de enfoque de los ocho dominios de seguridad **CISSP**. Además, aprendió sobre **InfoSec** y el principio del mínimo privilegio. Estar familiarizado con estos dominios de seguridad y los conceptos relacionados lo ayudará a comprender mejor el campo de la ciberseguridad.

	<p align="center"><b>I.E. FRANCISCO ABEL GALLEGO</b></p> <p align="center"><b>Taller # 1 Tecnología</b></p>	<b>TECH</b>
		<b>2026</b>
		<b>II PERIODO</b>

### Actividad

**Responder las siguientes preguntas**

1. **Rellene el espacio en blanco: El dominio \_\_\_\_\_ se centra en el acceso y la autorización para mantener la seguridad de los datos, asegurándose de que los usuarios sigan las políticas establecidas para controlar y gestionar los recursos.**
  - a. Operaciones de seguridad
  - b. Gestión de identidad y acceso
  - c. Seguridad de los recursos
  - d. Comunicación y seguridad de redes
2. **¿En qué se centra el dominio de la seguridad y la gestión de riesgos?**
  - a. Optimizar la seguridad de los datos garantizando la existencia de procesos eficaces
  - b. Gestionar y asegurar las comunicaciones inalámbricas.
  - c. Redes físicas seguras y comunicaciones inalámbricas.
  - d. Definir metas y objetivos de seguridad, mitigación de riesgos, cumplimiento, continuidad del negocio y regulaciones.
3. **¿En que dominio realizaría un profesional de la seguridad pruebas de control de la seguridad; recopilaría y analizaría datos, llevaría a cabo auditorias de seguridad para monitorizar riesgos, amenazas y vulnerabilidades?**
  - a. Arquitectura de seguridad e ingeniería.
  - b. Gestión de identidad y acceso.
  - c. Evaluación y pruebas de seguridad.
  - d. Comunicación e ingeniería de redes.
4. **Rellene el espacio en blanco: el Dominio \_\_\_\_\_ se refiere a la realización de investigaciones y a la implementación de medidas preventivas.**
  - a. Seguridad de los recursos.
  - b. Seguridad en el desarrollo del software.
  - c. Operaciones de seguridad.
  - d. Ingeniería de comunicación y redes.