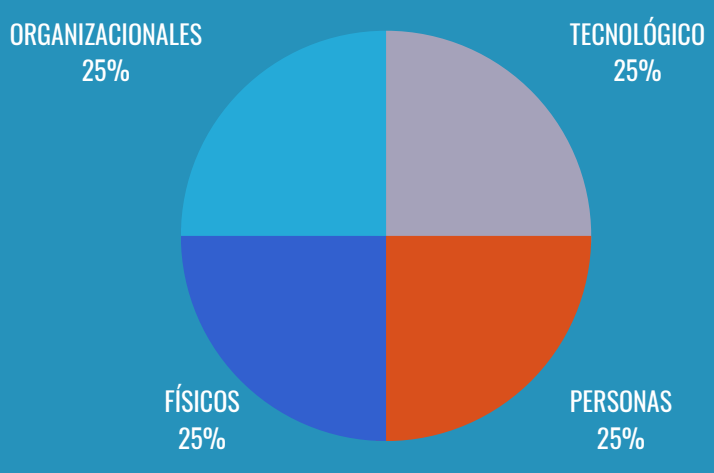
# SEGURIDAD DE LA INFORMACIÓN

## "La seguridad de la información es un compromiso de todos"

### Aspectos que influyen en la seguridad de la información

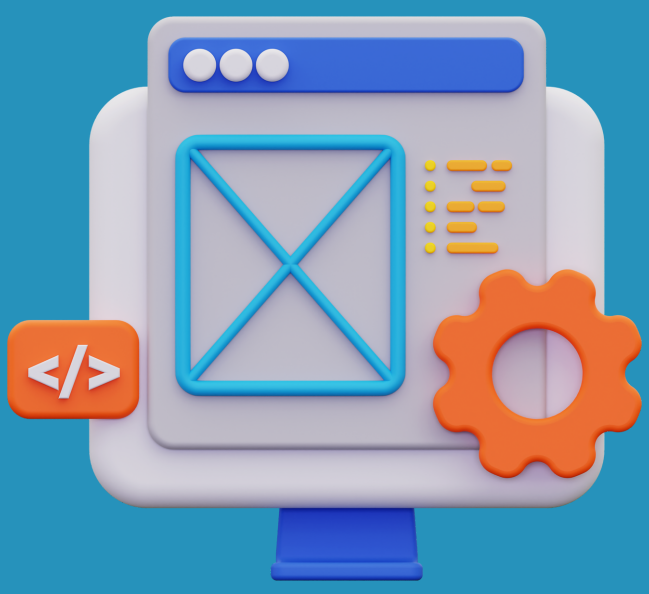



### OBJETIVO

**PROTEGER LA INFORMACIÓN**
Independientemente de donde se encuentre.

### Mi responsabilidad y primeros pasos para mantener la seguridad de la información de mis trámites y servicios:

1. Conocer que información genero o solicito al brindar los trámites y/o servicios.
2. Tener definido como preservo la información una vez iniciado y concluido el trámite o servicio (virtual o física).
3. Determinar el uso de la información necesaria de acuerdo al trabajo que realizo (se transfiere, se resguarda o se tiene para consulta).
4. Identificar el tipo de datos que contiene la información de mi trámite o servicio (datos personales, datos sensibles o información que pueda ser clasificada).
5. Conocer y aplicar el tratamiento necesario de la información (documentos) según el tipo de datos que contiene.



### Características de la seguridad de la información

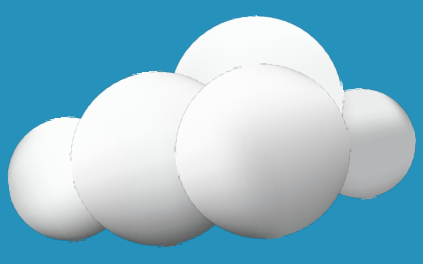
- Confidencialidad: información de acceso no autorizado que solo determinadas personas tienen acceso a ella.
- Integridad: mantener la precisión y la integridad de los datos, garantizando que no se alteren o manipulen sin autorización.
- Disponibilidad: garantizar que los sistemas y la información estén disponibles para su uso en todo momento, y que cualquier interrupción en la disponibilidad sea mitigada y resuelta rápidamente.
- Autenticidad: corroborar la identidad de un usuario o recurso, así se protegerá que dicha identidad no se falsifique.
- Resiliencia: capacidad de recuperarse rápidamente de cualquier interrupción o ataque de seguridad.

### Recomendaciones de seguridad a la hora de navegar en línea

- Evitar el acceso a sitios web de dudosa reputación.
- Deshabilitar la opción de recordar contraseñas en el navegador.
- Ser cuidadoso con los archivos que se descargan en sus dispositivos.
- Tener precaución al dar clic en enlaces y al descargar archivos adjuntos en correos.
- Reforzar la seguridad de tu equipo teniendo siempre actualizado el sistema operativo y el antivirus.

### Recomendaciones para la persona servidora pública

- Evitar tener documentos oficiales o con información que debe ser salvaguardada bajo la Ley de protección de datos en posesión de sujetos obligados para el Estado de Guanajuato a la vista y alcance de todos.
- Contar con una correcta gestión de archivo.
- Evitar dejar sesiones abiertas en los dispositivos del trabajo.
- Si necesitas mostrar la pantalla de tu equipo de cómputo a las personas usuarias, usar pantalla de privacidad o no mostrar pantalla hasta que se muestre únicamente la información que se quiere compartir.
- SI manejas algún sistema de información institucional, asegurar un correcto control de acceso y realizar revisiones periódicas a los accesos.
- No compartir, ni dar acceso a otras personas de tus cuentas y contraseñas.
- Cambiar la contraseña de tus cuentas cada 3 meses.
- Crear contraseñas seguras, utilizando una combinación de letras, números y símbolos.
- Verificar la fuente de información y el remitente de tus correos entrantes.
- No abrir correos de usuarios desconocidos o que no hayas solicitado, eliminarlos directamente y notificar a Dirección de Servicios y Tecnologías de la Información (DSTI) al correo seguridad.correo@ugto.mx



MEJORA EN LA ATENCIÓN DE LOS TRÁMITES Y SERVICIOS INSTITUCIONALES
Plan de Mejora 2023

Nota: En caso de duda, contactar directamente a la DSTI por medio del correo electrónico seguridad.correo@ugto.mx