**Actividad 1:**

Indica un ejemplo de cada proceso de comunicación en los que se ponga de manifiesto la confidencialidad, la integridad, la disponibilidad, la autenticidad, la fiabilidad, el no repudio y la auditabilidad.

* Confidencialidad: Una empresa decide cifrar todos los mensajes que se envíen o a través de su sistema informático. De esta forma tan sólo los usuarios autorizados de esta empresa podrán conocer el contenido de los mensajes
* Integridad: Por ejemplo, cuando se está creando una base de datos el encargado del proyecto (o profesora) puede pedir que la base de datos compruebe los datos al ser introducidos para no tener errores como introducir un número de teléfono en el campo del salario por lo que se garantiza que la información no esté siendo alterada de manera voluntaria o involuntaria.
* Disponibilidad: Una tienda de ropa puede decidir montar un servidor de back-up (reserva) en caso de avería para que de este modo su página web pueda estar abierta a los usuarios en todo momento y no pierdan ninguna venta.
* Autenticidad: La empresa N.O.E.L.I.A decide pedir el DNI a toda persona que quiera entrar a la sala donde se encuentran los servidores. De este modo se puede comprobar la identidad de toda persona que quiera acceder a esta sala y permitir o denegar el acceso en función si dicha persona dispone del permiso para acceder.
* Fiabilidad: La NASA utiliza microprocesadores bastante antiguos para sus satélites espaciales. Aunque estos procesadores ofrezcan una potencia de procesado mucho inferior a los microprocesadores comerciales actuales, han sido puestos a prueba durante muchos más años por lo que van a poder proporcionar un rendimiento constante.
* No repudio: Un sistema de mensajería puede implementar un sistema de no repudio a través del cifrado para que tanto una persona que envía un mensaje no pueda negar su autoría y el receptor no pueda negar que no lo ha recibido (aunque ella siempre me deje en visto ☹).
* Auditabilidad: Además de pedir el DNI, la empresa N.O.E.L.I.A decide llevar un registro con todas las personas que entran a la sala donde se encuentran los servidores. De este modo, en caso de accidente se puede acceder a dicho registro para conocer la identidad de las personas que estuvieron en la sala.

**Actividad 2:**

Localiza los errores conceptuales que encuentres en la siguiente información:

“Un SO que no está actualizado tiene una ~~amenaza~~ (vulnerabilidad) por un fallo de seguridad que un atacante aprovecha ejecutando una ~~vulnerabilidad~~ (amenaza) de alto riesgo. El administrador de seguridad atenúa ~~la brecha~~ (el riesgo) mejorando ~~el riesgo provocado por las contramedidas~~ (la seguridad a través de las contramedidas)”.

**Actividad 3:**

Confecciona un mapa conceptual de los tipos de amenazas y vulnerabilidades a que están expuestos los sistemas informáticos.

Datos

Software

Hardware

Amenaza lógica

Amenaza física

Amenaza externa

Amenaza interna

Vía de ataque

Procedencia

Se pueden clasificar segun

Vulnerabilidades

Amenazas

Se puede poner en riesgo a través de

Sistema Informático

**Actividad 4:**

Busca noticias recientes de incidente graves de seguridad que han ocurrido en el mundo. Indica que ha ocurrido y como lo han solucionado. (2 ejemplos)

**Noticia A:**

* Fecha: 14 de septiembre de 2020 (el incidente se produjo el 18 de agosto de 2020)
* Fuente: <https://www.theverge.com/2020/9/14/21436160/razer-data-leak-elasticsearch-sever-misconfiguration>
* Incidente: Razer hizo público por accidente la información personal de cien mil usuarios revelando sus correos electrónicos y direcciones de envío debido a un fallo del servidor.
* Solución: Razer avisó a todos los usuarios afectados para actualizarán la información y tuvieran especial cuidado con posibles phishing que les pudieran llegar al correo. Además, se realizó una rápida actualización en el servidor que evito que información más sensible de los consumidores pudiera ser filtrada.

**Noticia B:**

* Fecha: 26 de agosto de 2020
* Fuente: <https://www.biobiochile.cl/noticias/ciencia-y-tecnologia/pc-e-internet/2020/08/26/freepik-confirma-que-las-cuentas-de-mas-de-8-millones-de-usuarios-fueron-hackeadas.shtml>
* Incidente: La aplicación Freepik recibió un ataque de inyección SQL que permitió a los hackers obtener la dirección de correo de más de ocho millones de usuario y hashear las contraseñas de casi 4 millones.
* Solución: Freepik optó por cancelar las cuentas de los usuarios afectados y enviar un e-mail para cambiar la contraseña y poder volver a activar la cuenta. Además recomendó a todos los usuarios mantener tanto la aplicación como el dispositivo actualizado para contar con las nuevas medidas de seguridad.