BUENAS PRÁCTICAS EN ARQUITECTURA Y DISEÑO

JORGE IBARRA PEÑA. #20310025

IVAN ALEXANDER LUCE VILLEGAS. #20310017

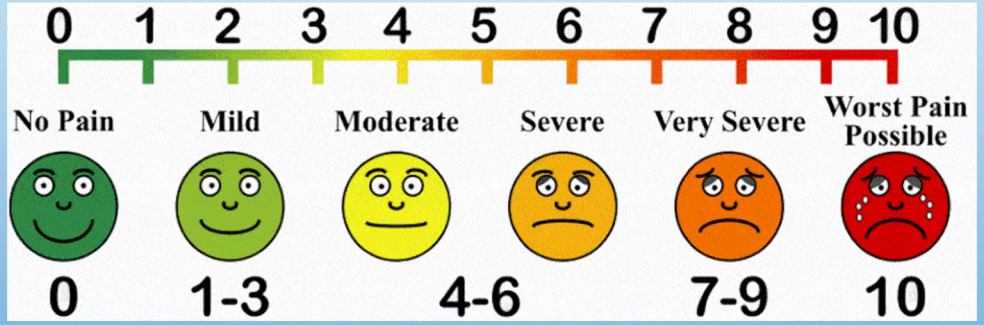
RUBÉN VALDIVIA PÉREZ #20310014

ANGEL GABRIEL MUNGUIA GONZALEZ #20310041

ROGELIO REYNAGA SALAZAR #203100

¿QUÉ ES DREAD?

- DAMAGE POTENTIAL (¿QUÉ TANTO DAÑO PUEDE CAUSAR?)
- REPRODUCIBILITY (¿QUÉ TAN FÁCIL ES DE REPLICAR?)
- EXPLOITABILITY (¿QUÉ TAN FÁCIL ES DE EXPLOTAR?)
- AFFECTED USERS
- DISCOVERABILITY (¿QUÉ TAN FÁCIL SE PUEDE DESCUBRIR?)



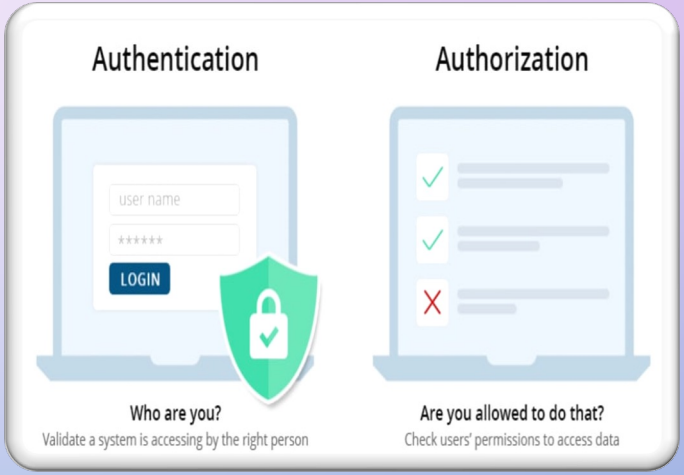
EJEMPLO DE DREAD

Evaluación Cualitativa del Riesgo	
Amenaza	Usuario interno
Componente Afectado	Los componentes que no pasan por auditoría
Descripción	No existen registros de auditoría ni trazabilidad
Resultado	No queda registro de las operaciones de un atacante
Estrategias de mitigación	Hacer obligatorios logs de auditoría

Evaluación Cuantitativa del Riesgo **Criterio**	**Puntuación**
Daño potencial	9
Reproducibilidad	9
Explotabilidad	9
Proporción de usuarios afectados	9
Posibilidad de descubrir la vulnerabilidad	4
Promedio	8

¿QUÉ SON LAS BUENAS PRÁCTICAS EN ARQUITECTURA Y DISEÑO?

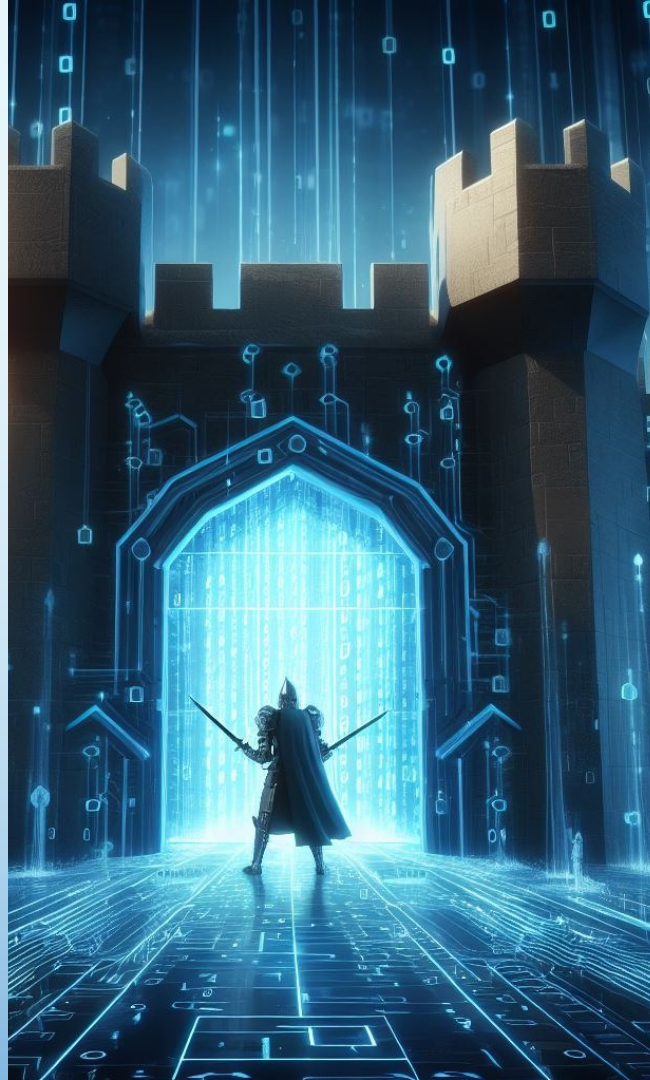
- SON TÉCNICAS Y ENFOQUES PARA QUE LOS SISTEMAS SEAN EFICIENTES Y SEGUROS.
- ASEGURAN QUE EL SOFTWARE CUMPLA REQUISITOS Y SEA MANTENIBLE.
- MINIMIZAN RIESGOS, ERRORES Y PROBLEMAS FUTUROS.
- ES FUNDAMENTAL PARA CALIDAD, SEGURIDAD Y CONFIABILIDAD DEL SOFTWARE.



PROTECCIÓN DE DATOS

- SE REFIERE A LA IMPLEMENTACIÓN DE MEDIDAS Y PROCESOS DESTINADOS A GARANTIZAR LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LOS USUARIOS Y DE LA EMPRESA EN EL SOFTWARE DESARROLLADO.

- ESTO ES POSIBLE CON LA CREACIÓN DE UN EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD).



QUÉ ES EL RGPD?

- ES UNA LEY DE PRIVACIDAD Y PROTECCIÓN DE DATOS QUE ENTRÓ EN VIGOR EL 25 DE MAYO DE 2018 EN LA UNIÓN EUROPEA (UE) Y EL ESPACIO ECONÓMICO EUROPEO (EEE).

- EL OBJETIVO PRINCIPAL DEL RGPD ES BRINDAR A LOS CIUDADANOS UN MAYOR CONTROL SOBRE SUS DATOS PERSONALES Y ESTANDARIZAR LAS REGULACIONES DE PRIVACIDAD EN TODA LA UE PARA GARANTIZAR UN ENFOQUE MÁS COHERENTE Y ROBUSTO EN CUANTO A LA PROTECCIÓN DE DATOS.

OBJETIVOS DEL RGPD

EL RGPD OFRECE EL REGLAMENTO PARA GESTIONAR Y PROTEGER ESTOS DATOS AL TIEMPO QUE CREA POLÍTICAS Y PRÁCTICAS CONSISTENTES.

Privacida
d

Controles
y avisos

Políticas
transparentes

Informática e
información

CHECKLIST DE ARQUITECTURA Y DISEÑO

- ESTE ES UN CHECKLIST DE CONSIDERACIONES DE ARQUITECTURA Y DISEÑO QUE SE DEBEN TENER EN CUENTA PARA GARANTIZAR LA CALIDAD Y SEGURIDAD DE UN SISTEMA EN DESARROLLO.

- **EL DISEÑO IDENTIFICA, ENTIENDE Y SE ACOMODA A LAS POLÍTICAS DE SEGURIDAD DE LA COMPAÑÍA.**
- EL DISEÑO RECONOCE Y SE ACOMODA A LOS AMBIENTES IMPUESTOS POR SERVICIOS DE HOSTING.
- **EL NIVEL DE ACCESO QUE SE TENDRÁ EN EL AMBIENTE EN QUE SE VA DESPLEGAR ES CONOCIDO.**
- EL DISEÑO IDENTIFICA LA AUTORIDAD CERTIFICADORA QUE USARÁ EL SITIO PARA SOPORTAR SSL.
- **EL DISEÑO TIENE EN CUENTA LA ESCALABILIDAD Y DESEMPEÑO QUE SE NECESITARÁ LA APLICACIÓN.**

RESPECTO A MANEJO DE SESIONES ES IMPORTANTE TENER EN CUENTA:

Se utiliza SSL para proteger cookies de autenticación.

El contenido de las cookies está cifrado.

El tiempo de sesión es limitado.

El estado de la sesión está protegido contra acceso no autorizado.

Los identificadores de sesión no se transmiten usando. query strings

RESPECTO A DATOS SENSIBLES ES IMPORTANTE CONSIDERAR LO SIGUIENTE:

Los secretos (como claves) no deben ser almacenados, a menos de que sea estrictamente necesario.

Secretos no se almacenan en el código. Nunca debe tener una clave “quemada” en el código.

Las conexiones a base de datos, passwords, llaves, u otros secretos no se deben almacenar en texto claro.

Los datos sensibles no son registrados en el log en texto claro.

El diseño tiene en cuenta la protección de datos sensible que deben viajar por la red.

La información sensible no es almacenada en cookies persistentes.

Los datos sensibles no se transmiten con protocolo GET.

MANTENIMIENTO Y AJUSTES

- IMPORTANCIA DEL MANTENIMIENTO Y LA PREVENCIÓN DE RIESGOS OPERATIVOS.
- MANTENER POLÍTICAS DE CONTRASEÑAS SÓLIDAS DURANTE LAS ACTUALIZACIONES.
- GESTIÓN ADECUADA DE SESIONES, PRUEBAS RIGUROSAS Y CHECKLIST DE SEGURIDAD.
- DESACTIVACIÓN DE COMPONENTES NO UTILIZADOS PARA REDUCIR LA SUPERFICIE DE ATAQUE.
- SEGURIDAD EN ACTUALIZACIONES Y POLÍTICA DE RETENCIÓN DE DATOS.

FIN DE LA VIDA DEL PRODUCTO

- AL DAR DE BAJA UN SISTEMA, SE DEBEN CONSIDERAR RIESGOS OPERACIONALES Y DE SEGURIDAD. CASOS DE DONACIÓN DE COMPUTADORAS CON INFORMACIÓN SENSIBLE EN SUS DISCOS DUROS SON COMUNES. LA PROTECCIÓN DE DATOS NO DEBE DESCUIDARSE EN LA FASE DE CESE DE OPERACIONES.