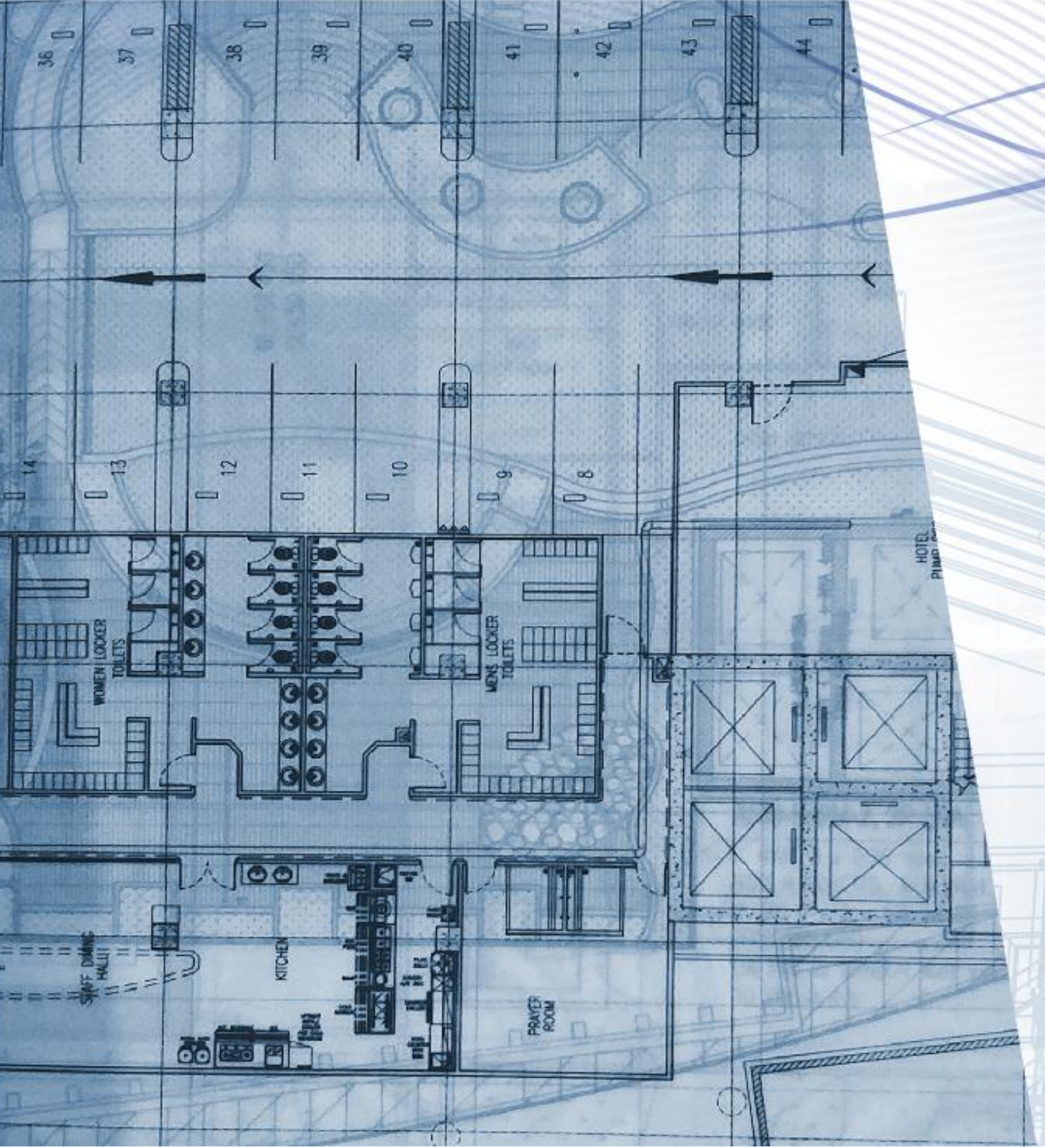

CIBERSEGURIDAD

Yornandy Martinez
Ingeniero Industrial

INSTITUCIÓN UNIVERSITARIA PASCUAL BRAVO 1938


CRACKS
DATA VIRUS
MALICIOUS SOFTWARE
THEFT
SOCIAL MEDIA ATTACKS
CYBERWARFARE
VIRUS
SOFTWARE FAILURE
NETWORK SNIFFING
YOUR DATA SAFETY
SPYWARE
HUMAN ERROR
SOFTWARE ERROR
STOLEN INFORMATION
TROJAN
CYBER ATTACKS
HACKING
PASSWORD CRACKING
FRAUD
CYBERCRIMINALS
TROJAN
ADWARE
CYBERSTALKING
SYSTEM PENETRATION

SEGURIDAD DE LA INFORMACIÓN

Es un conjunto de políticas, procedimientos, acciones y demás actividades, orientadas a proteger la información de un amplio rango de amenazas.

OBJETIVOS DE LA CIBERSEGURIDAD

Asegurar la continuidad del negocio.

Evitar el daño, perdida o alteración de la información.

Minimizar los impactos negativos a la organización.

DEFINICIONES

AMENAZA: es el evento que puede afectar los sistemas informáticos de la organización.

RIESGO: es el impacto que se puede producir sobre un sistema.

VULNERABILIDAD: es la debilidad que puede presentar un sistema sobre una amenaza.

IMPACTO: es el efecto que puede generar la materialización de una amenaza sobre un sistema.

DISPOSITIVOS INDUSTRIALES

Fuente: https://elpais.com/economia/2020

AMENAZAS INFORMÁTICAS

VIRUS	Software que tiene por objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático.

RANSOMWARE	Malware con el objetivo de secuestrar la información encriptándola, para luego pedir rescate.

FALLA SOFTWARE	Problema en un programa de computador o sistema de software que desencadena un resultado indeseado.

FALLA HARDWARE	Mal funcionamiento de uno o varios componentes físicos de un equipo informático.

FALLA RED DATOS	Fallos o eventos de una red como aquellos sucesos que interfieren en el correcto funcionamiento del trafico de datos.