UPeU
UNIVERSIDAD PERUANA UNION

ESCUELA DE
INGENIERÍA DE SISTEMAS

Universidad de Babahoyo

El Alcance

Integrantes:

- 🚀 Jhon J. Melendres velasco
- 🚀Jhon E. Melendrez Huaman
- 🚀Jheyfer Arevalo Cavanillas.
- 🚀 Junior Cercado Vásquez

Que Alcance presenta el caso 03?

Identificación de los Activos.

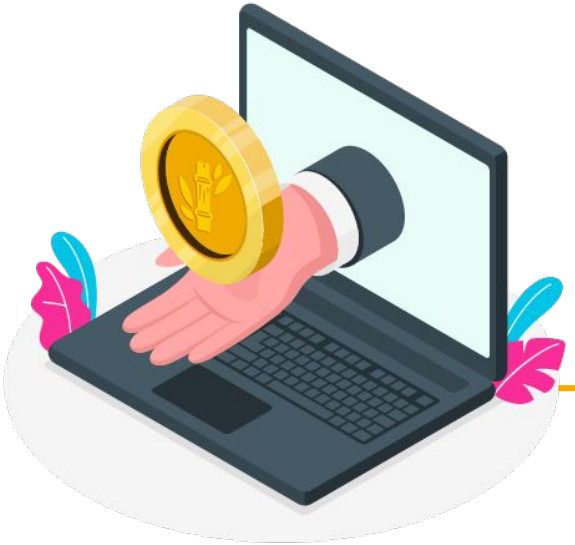
Activos Primarios. Son aquellos que implican procesos del negocio.

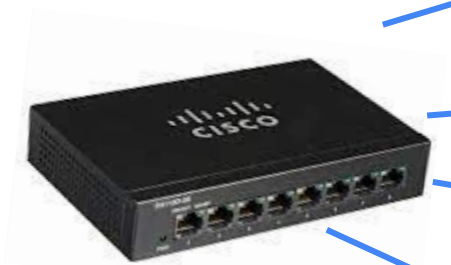
Información. Son considerados manuales de usuario entre otros

Activos de Soporte. Estos dependen los elementos primarios del alcance, de todos los tipos: hardware, software, redes, personal, sitio, estructura de la organización.

Valoración de Activos.

La base para la valoración de los activos del departamento de TIC es el costo en que se incurre debido a la pérdida de la confidencialidad, integridad y disponibilidad como resultado de un incidente





Facultad 1

Facultad 2

Facultad 4

Facultad 3

centro de datos

PARAMETROS/VALORACION		DEPENDENCIA	FUNCIONALIDAD	INTEGRIDAD , CONFIDENCIALIDAD Y DISPONIBILIDAD
1	MUY BAJO	Ningún otro activo depende de este para la entrega de servicios	Activo con capacidades tecnológicas muy limitadas	La divulgación, modificación y no disponibilidad de su archivo de configuración puede afectar de forma insignificante la entrega de servicios
2	BAJO	Pocos activos dependen de este para la entrega de servicios	Activo con capacidades tecnológicas limitadas	La divulgación, modificación y no disponibilidad de su archivo de configuración podría afectar en parte la entrega de servicios
3	MEDIO	Una mínima cantidad de activos dependen de este para la entrega de servicios	Activo con capacidades tecnológicas avanzadas	La divulgación, modificación y no disponibilidad de su archivo de configuración podría afectar significativamente la entrega de servicios
4	ALTO	Un número considerable de activos dependen de éste para la entrega de servicios	Activo con capacidades tecnológicas muy avanzadas.	La divulgación, modificación y no disponibilidad de su archivo de configuración podría afectar gravemente la entrega de servicios.
5	CRITICO	Todos los activos dependen de éste para la entrega de servicios	Activo con capacidades tecnológicas de última generación	La divulgación, modificación y no disponibilidad de su archivo de configuración podría afectar totalmente la entrega de servicios

El listado de ejemplos de vulnerabilidades con sus respectivas amenazas se encuentra en la norma ISO 27005 y detallado en la tabla 5

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
	Falta de esquemas de reemplazo periódico. Susceptibilidad a la humedad, el polvo y la suciedad	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Falta de control de cambio con configuración eficiente	Error en el uso
	Susceptibilidad a las variaciones de tensión	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios o documentos

Tabla 5: Ejemplo de vulnerabilidades y amenazas. **Fuente:** ISO 27005

resultado que se obtuvo a través de la observación y reuniones trabajo para obtener las amenazas y vulnerabilidades que influyen en cada uno de los activos

ACTIVOS	AMENAZAS	VULNERABILIDAD	PROBABILIDAD OCURRA LA AMENZA	Facilidad de explotación
PORTATIL	INCUMPLIMIENTO EN EL MANTENIMIENTO	MANTENIMIENTO INSUFICIENTE	ALTA	ALTA
	HURTO DE MEDIOS O DOCUMENTOS	ALMACENAMIENTO SIN PROTECCIÓN	MEDIA	MEDIA
EQUIPOS DE ESCRITORIO	INCUMPLIMIENTO EN EL MANTENIMIENTO	MANTENIMIENTO INSUFICIENTE	ALTA	ALTA
	HURTO DE MEDIOS O DOCUMENTOS	COPIA NO CONTROLADA	ALTA	ALTA
		ALMACENAMIENTO SIN PROTECCIÓN	ALTA	ALTA
	ERROR DE USO	FALTA DE CONTROL DE CAMBIO EN LA CONFIGURACION	MEDIA	MEDIA

Tabla 7: Cálculo que ocurra la amenaza y facilidad con la que puede ocurrir sobre los activos.

Fuente: Elaboración propia

Valores	Nivel de riego	Descripción del riesgo y acciones necesarias
8	ALTO	Requiere fuertes medidas correctivas. Planes de tratamiento implementados en corto tiempo, reportados y controlados con atención directa de alta dirección
6-7	MEDIO ALTO	Requiere vigilancia de alta dirección con planes de tratamiento implementados y reportados a los gerentes de UTB
4-5	MEDIO	Se requieren acciones correctivas controladas por grupos de manejo de incidentes en período de tiempo razonable
2-3	MEDIO BAJO	Riego aceptable-Administrado por los grupos de incidentes bajo procedimientos normales de control
0-1	BAJO	El propietario del activo lo administra con procedimientos rutinarios o decide aceptar el riesgo

Evaluación del Riesgo:

"Es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente" (Roa, 2013).

Activos	Amenazas	Vulnerabilidad	Valor activo	Probab. que ocurra la amenaza	Facilidad de explotación	Riesgo
Portátil	Incumplimiento en el mantenimiento	Mantenimiento insuficiente	5	ALTA	ALTA	8
	Hurto de medios o documentos	Almacenamiento sin protección	5	MEDIA	MEDIA	6
Equipos de escritorio	Incumplimiento en el mantenimiento	Mantenimiento insuficiente	5	ALTA	ALTA	8
	Hurto de medios o documentos	Copia no controlada	5	ALTA	ALTA	8
		Almacenamiento sin protección	5	ALTA	ALTA	8
	Error de uso	Falta de control de cambio en la configuración	5	MEDIA	MEDIA	6

Conclusiones

- Para realizar la aplicabilidad de controles es necesario tener en cuenta las actualizaciones que se realizan en la Norma ISO 27002, porque se incorporan nuevos controles a las tecnologías

- Una vez realizado el proceso de evaluación del riesgo y la aplicabilidad de controles, se debe realizar en ciertos periodos de tiempo un análisis y evaluación del riesgo nuevamente para establecer Una vez realizado el proceso de evaluación del riesgo y la aplicabilidad de controles, se debe realizar en ciertos periodos de tiempo un análisis y evaluación del riesgo nuevamente para establecer qué controles se deben mejorar e incorporar, porque continuamente el departamento de TIC incorpora nuevos servicios.que controles se deben mejorar e incorporar, porque continuamente el departamento de TIC incorpora nuevos servicios.

- La evaluación del riesgo es identificar y ponderar los riesgos que están expuestos los activos de la empresa estos pueden ser software, hardware, documentación y servicios, para finalizar con una selección de controles que ayudan a mitigar el riesgo.


UPeU
UNIVERSIDAD PERUANA UNION
ESCUELA DE
INGENIERÍA DE SISTEMAS