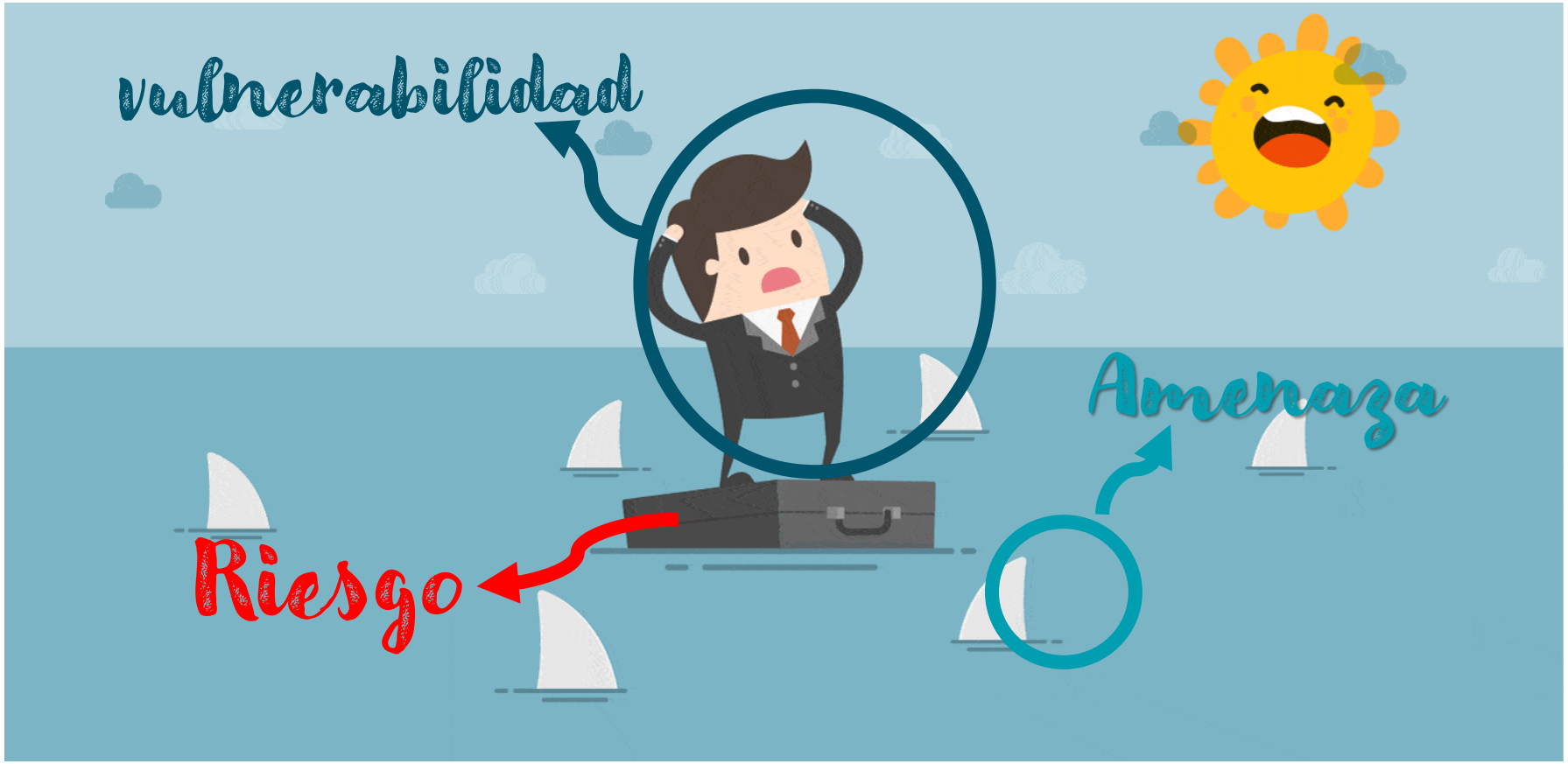
COMUNICAR IMPACTO DE LAS VULNERABILIDADES A ALTO NIVEL

(C-levels y no-técnicos)

WOMCY
LATAM Women in Cybersecurity

Conceptualizar



Conceptualizar

VULNERABILIDAD

Debilidad inherente o provocada en un bien o control.

AMENAZA

Situación o acción que puede producir un daño.

RIESGO

Probabilidad de que se produzca un daño que genere un impacto negativo

AMENAZA, RIESGO Y VULNERABILIDAD

VULNERABILIDAD => CARACTERÍSTICA

AMENAZA => ACCION

RIESGO => MEDIDA DE INCERTIDUMBRE

Enfocarnos en el mensaje al negocio

Las vulnerabilidades sólo son significativas mientras representen un riesgo para la organización.

Mi responsabilidad es comunicar estos riesgos a las partes interesadas de una manera que les permita tomar decisiones bien informadas.

MEDIR EL RIESGO

Riesgo = Amenaza x Vulnerabilidad x Activo

Riesgo = Probabilidad x Impacto

Likelihood severity occurs	Potential Severity Rating: Minor	Moderate	Significant	Catastrophic
Very Likely	Moderate	High	Extreme	Extreme
Likely	Low	Moderate	High	Extreme
Unlikely	Very Low	Low	Moderate	High
Rare	Very Low	Very Low	Low	Moderate

WOMCY
LATAM Women in Cybersecurity

MEDIR EL RIESGO

Impacto/Probabilidad	Poco Probable	Probable	Muy probable
Alto impacto			
Medio impacto			
Bajo impacto	GARBAGGING		

GARBAGGING

Búsqueda en la basura para Identificar cualquier tipo de información útil para obtener el acceso a la organización.

WOMCY
LATAM Women in Cybersecurity

MEDIR EL RIESGO

Impacto/Probabilidad	Poco Probable	Probable	Muy probable
Alto impacto			TAILGATING
Medio impacto			
Bajo impacto	GARBAGGING		

TAILGATING

Ingreso a espacios físicos de personas no autorizadas por infiltración junto a personas autorizadas

WOMCY
LATAM Women in Cybersecurity

MEDIR EL RIESGO

Impacto/Probabilidad	Poco Probable	Probable	Muy probable
Alto impacto	CLONADO DE ACCESO		TAILGATING
Medio impacto			
Bajo impacto	GARBAGGING		

CLONADO DE ACCESO

Al dejar sin vigilancia una identificación, alguien utiliza los datos en la misma para generar una nueva.

WOMCY
LATAM Women in Cybersecurity

MEDIR EL RIESGO

Impacto/Probabilidad	Poco Probable	Probable	Muy probable
Alto impacto	CLONADO DE ACCESO		TAILGATING
Medio impacto	BAITING		
Bajo impacto	GARBAGGING		

BAITING

Acción de introducir malware en forma física a través de dispositivos extraíbles abandonados alrededor de una organización.

¿Dónde está el impacto?

WOMCY
LATAM Women in Cybersecurity

IMPACTO != RIESGO

WOMCY
LATAM Women in Cybersecurity

IMPACTO != RIESGO

PROBABILIDAD

IMPACTO

RIESGO

LA PARTE MÁS IMPORTANTE ES EL NEGOCIO

WOMCY
LATAM Women in Cybersecurity

WOMCY
LATAM Women in Cybersecurity

PROCESOS DE NEGOCIO

- ¿Cómo hace la organización para crecer?
- ¿Qué tan importante es lo que estoy evaluando?
- ¿Cuál es el proceso que permite a la organización seguir creciendo?

WOMCY
LATAM Women in Cybersecurity

PROCESOS DE NEGOCIO

¿Cuál es el proceso de negocio crítico de un cine?

WOMCY
LATAM Women in Cybersecurity

WOMCY
LATAM Women in Cybersecurity

¿Cuál es el proceso de Negocio Afectado?

IMPACTO != RIESGO

EJEMPLO 1

The application uses unverified data in a SQL call that is accessing account information:

```
pstmt.setString(1, request.getParameter("acct"));
 ResultSet results = pstmt.executeQuery( );
```

An attacker simply modifies the browser's 'acct' parameter to send whatever account number they want. Then,the attacker can access any user's account.

```
https://example.com/app/accountInfo?acct=notmyacct
```

WOMCY
LATAM Women in Cybersecurity

IMPACTO != RIESGO

EJEMPLO 1

- **AMENAZA** — Filtración de información a través de un control de acceso roto.
- **PROBABILIDAD** — Alta
- **ACTIVO** — Servidor core de base de datos para el sistema de alta de usuarios en ambiente productivo
- **IMPACTO** — Alto, el atacante puede acceder a la cuenta de cualquier usuario.
- **RIESGO** — Crítico

WOMCY
LATAM Women in Cybersecurity

¿Cuál es el proceso de Negocio Afectado?

IMPACTO != RIESGO

EJEMPLO 2

A cinema chain allows group booking discounts and has a maximum of fifteen attendees before requiring a deposit. Attackers could threat model this flow and test if they could book six hundred seats and all cinemas at once in a few requests, causing a massive loss of income.

WOMCY
LATAM Women in Cybersecurity

IMPACTO != RIESGO

EJEMPLO 2

- AMENAZA
- PROBABILIDAD
- ACTIVO
- IMPACTO
- RIESGO

WOMCY
LATAM Women in Cybersecurity

¿Cuál es el proceso de Negocio Afectado?

IMPACTO != RIESGO

EJEMPLO 3

An application's blind trust in frameworks may result in queries that are still vulnerable, (e.g., Hibernate Query Language (HQL)):

```
Query HQLQuery = session.createQuery("FROM accounts WHERE
    custID='" + request.getParameter("id") + "'");
```

In both cases, the attacker modifies the 'id' parameter value in their browser to send: `' UNION SLEEP(10);--`. For example:

```
http://example.com/app/accountView?id=' UNION SELECT SLEEP(10);--
```

This changes the meaning of both queries to return all the records from the accounts table.

WOMCY
LATAM Women in Cybersecurity

IMPACTO != RIESGO

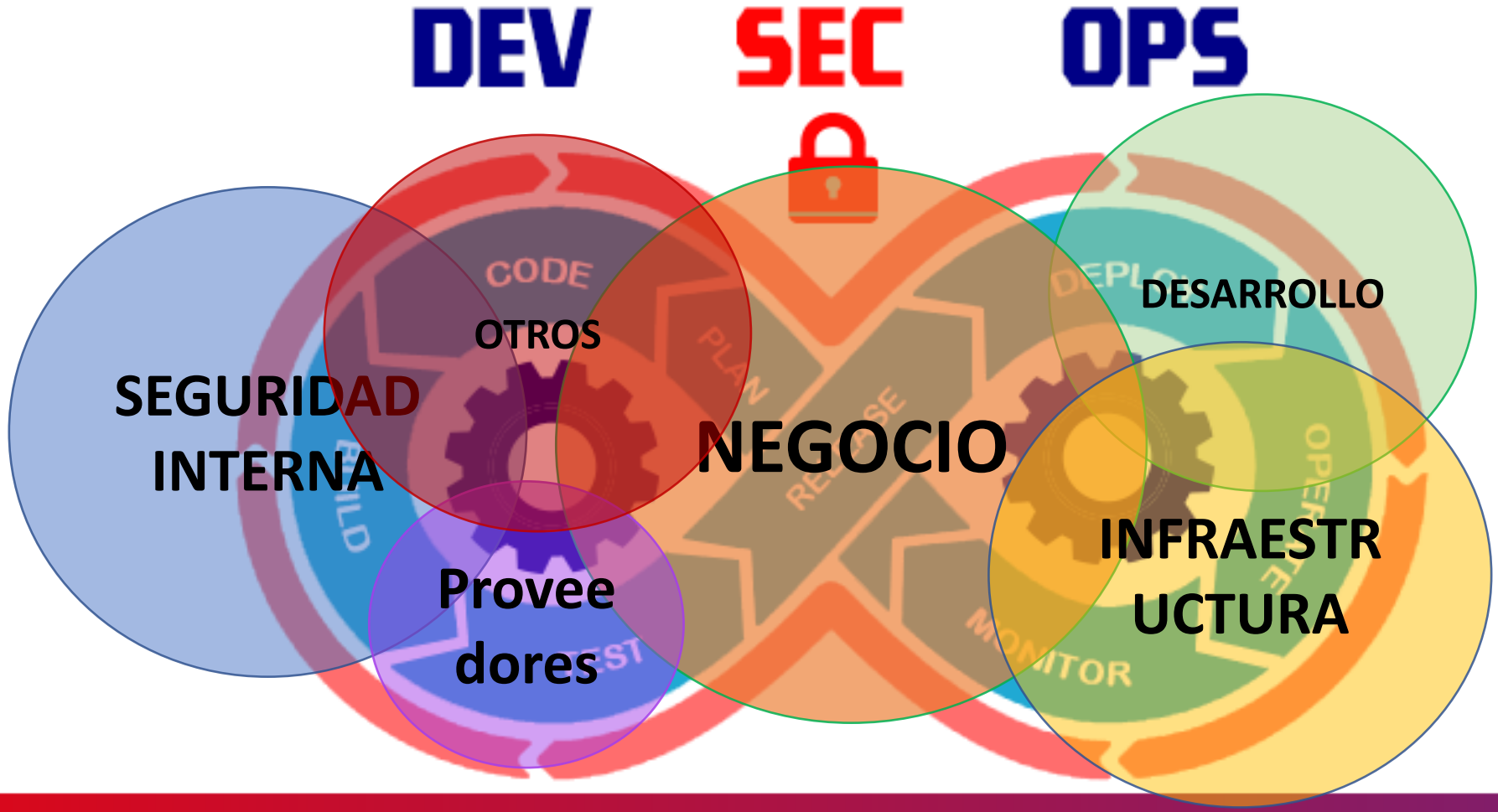
EJEMPLO 3

• AMENAZA	
• PROBABILIDAD	
• ACTIVO	Base de datos no productiva que contiene las fechas de ingreso a la organización exclusivamente.
• IMPACTO	
• RIESGO	


LA COMUNICACIÓN ES LA CLAVE
WOMCY
LATAM Women in Cybersecurity

WOMCY
LATAM Women in Cybersecurity

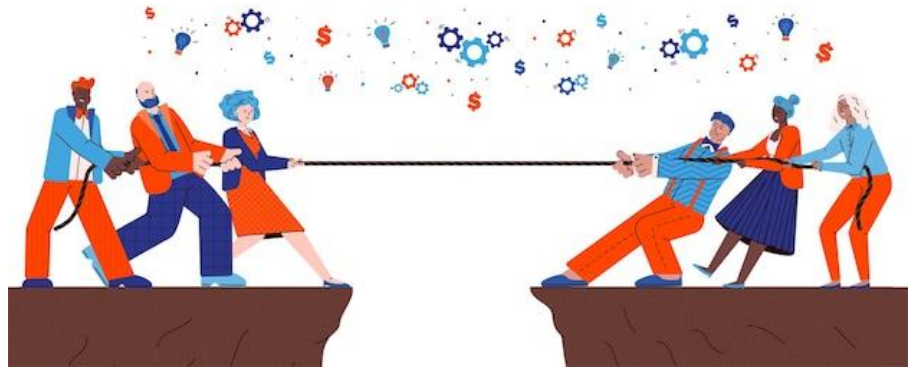
¿Y la comunicación?



WOMCY
LATAM Women in Cybersecurity

¿Y la comunicación?

1. Todos somos un mismo equipo con la misión de asegurar la información.
2. Si una recomendación no puede aplicarse directamente, buscamos el cómo si.
3. Los planes B, C y hasta D, tienen que ser válidos y aplicables.
4. Está bien que existan los falsos positivos.
5. Está mal creer que siempre vamos a tener la razón.
6. Lo que es crítico técnicamente, puede no ser crítico para el negocio.
7. Y viceversa.
8. Una prueba es replicable en la medida que se evalúe nuevamente en tiempo y forma.



AHORA TE TOCA A TI ☺
DUDAS

WOMCY
LATAM Women in Cybersecurity

¡GRACIAS!
Obrigada!
Thank You!

#OneWomcy #WomcyGrit
#YosoyWomcy #EuSouWomcy

WOMCY
LATAM Women in Cybersecurity