Requisitos OEC
Seguridad de la Información

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas

Noviembre, 2023

Requisitos OEC

Seguridad de la Información

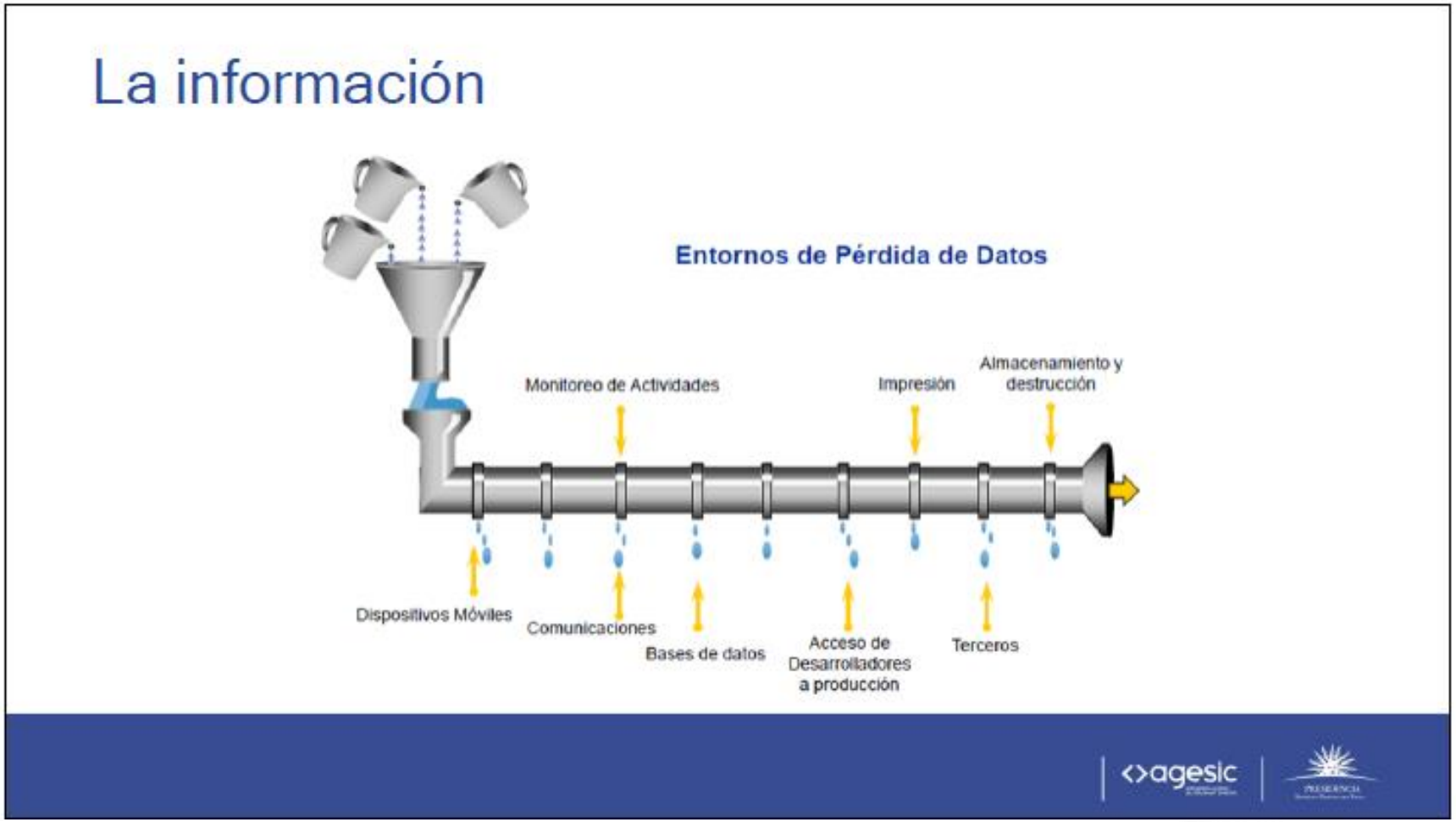
Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas

La información es un activo que tiene valor para la Organización, y como todo aquello que tiene valor para nosotros debe ser protegida.

Requisitos OEC
Seguridad de la Información

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas

¿Dónde podría darse «pérdida de datos» o «perdida de información»?



Requisitos OEC

Seguridad de la Información

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas

Principios de la Seguridad de la información

CONFIDENCIALIDAD

Asegurar que solamente personas autorizadas accedan a la información.

DISPONIBILIDAD

Asegurar que la información esté disponible cuando se la necesite.

INTEGRIDAD

Asegurar la exactitud y completitud de la información.

agesic

Requisitos OEC - Cibserseguridad

Ciclo de vida de la ciberseguridad

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas

Objetivos:

- Minimizar la exposición y determinar posibles puntos que puedan comprometer la integridad, disponibilidad o confidencialidad de los activos o la información que estos gestionan.
- Potenciar el servicio prestado de manera confiable y segura.

Requisitos OEC - Cibserseguridad

1. Identificar

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas

Debemos comprende el contexto de la organización, sus activos y riesgos asociados.

Requisitos regulatorios, legales, ambientales y operativos de la Organización.

La misión de la Organización, sus objetivos, interesados y actividades.

Riegos de ciberseguridad de sus operaciones, activos e individuos.

Decisiones sobre los riesgos operacionales, a partir de prioridades, restricciones, tolerancia al riesgo y supuestos de la Organización.

Requisitos OEC - Cibserseguridad

Activos de la Organización

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas

Los activos de la Organización soportan los procesos críticos de las operaciones y los riesgos asociados pertinentes.

Los datos, dispositivos, sistemas e instalaciones que permiten a la organización alcanzar los objetivos de negocio, se identifican y gestionan en forma consistente, en relación con los objetivos y la estrategia de riesgo de la organización.

Requisitos OEC - Cibserseguridad

2.Proteger

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas

Aplicación de medidas para proteger los procesos y los activos de la organización

Soluciones técnicas para garantizar la seguridad y resistencia de los sistemas y activos de la Organización.

El acceso a los activos e instalaciones se limita a usuarios, procesos o dispositivos, actividades y transacciones autorizadas.

El personal de la organización y socios de negocios, formados para cumplir con sus obligaciones alineadas con las políticas, procedimientos y acuerdos existente.

Componentes de los sistemas de información y de control industrial en buen estado.

Gestionar la protección de los sistemas de información y los activos.

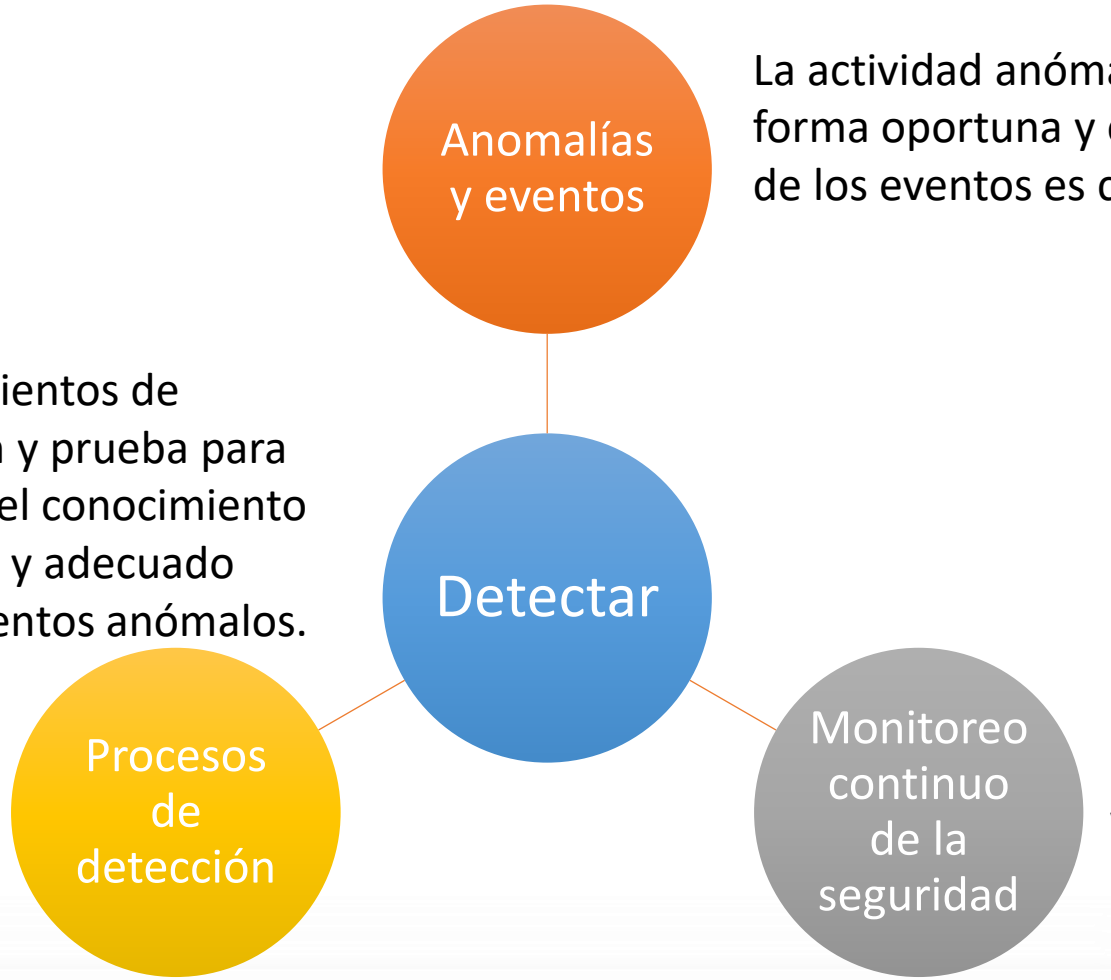
Proteger la confidencialidad, integridad y disponibilidad de la información.

Requisitos OEC - Cibserseguridad

3.Detectar

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas

Definición y ejecución de las actividades apropiadas dirigidas a la identificación temprana de los incidentes de seguridad.



La actividad anómala se detecta de forma oportuna y el potencial impacto de los eventos es comprendido.

Procedimientos de detección y prueba para asegurar el conocimiento oportuno y adecuado de los eventos anómalos.

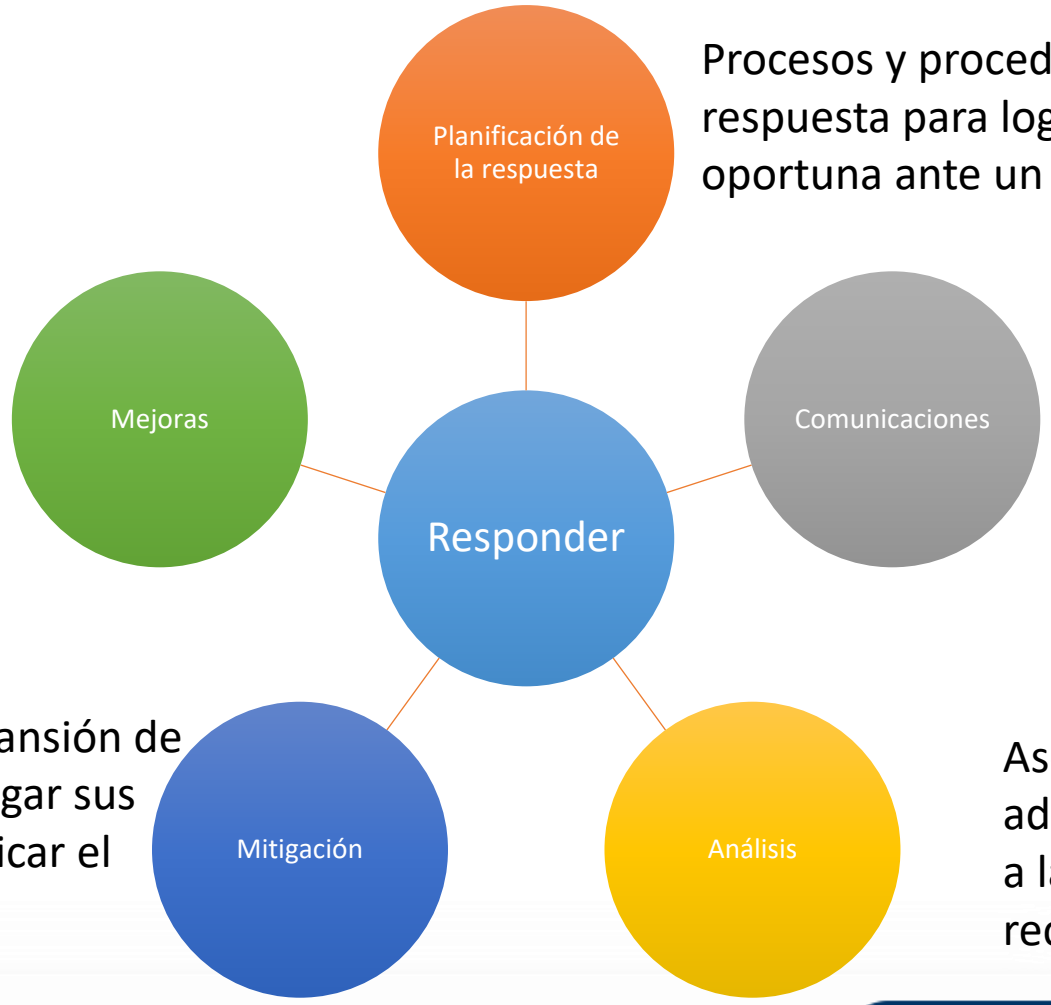
Los S.I. y los activos son monitoreados para identificar eventos de seguridad cibernética y verificar la eficacia de las medidas de protección.

Requisitos OEC - Cibserseguridad

4.Responder

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas

Definición y ejecución de las actividades en caso de detección de un evento de seguridad. El objetivo es reducir el impacto de un potencial incidente de seguridad informática.



Procesos y procedimientos de respuesta para lograr una respuesta oportuna ante un incidente.

Incorporación de lecciones aprendidas.

Se coordinan acciones con las partes interesadas internas y externas, según corresponda

Prevenir la expansión de un evento, mitigar sus efectos y erradicar el incidente

Asegurar una respuesta adecuada y dar soporte a las actividades de recuperación.

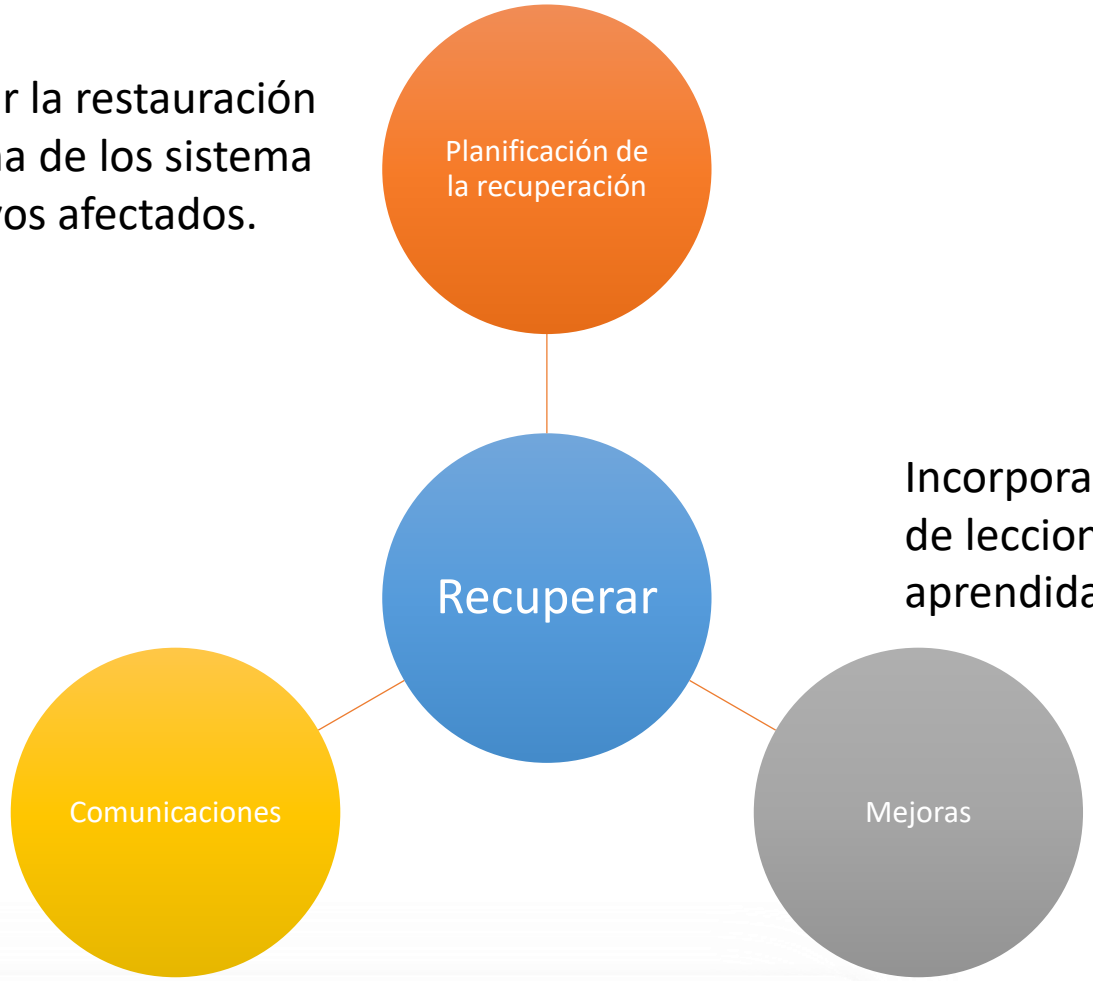
Requisitos OEC - Cibserseguridad

5.Recuperar

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas

Gestión de los planes y actividades para restaurar los procesos y servicios deficientes debido a un incidente de seguridad

Asegurar la restauración oportuna de los sistema s o activos afectados.



Incorporación de lecciones aprendidas.

Se coordinan acciones con las partes interesadas internas y externas, según corresponda

Requisitos OEC - Cibserseguridad

Identificar / Proteger / Detectar /Responder / Recuperar

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas

Comprender el contexto. Conocer los activos y los riesgos

IDENTIFICAR	1) Procedimientos con medidas de seguridad de la información
	2) Clasificar la información
	10) Revisar los procedimientos
	13) Inventariar regularmente todos los medios de TI que contenga información confidencial
	14) Licenciamiento adecuado

Requisitos OEC - Cibserseguridad

Identificar / Proteger / Detectar /Responder / Recuperar

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas

Aplicación de controles (técnicos, políticas, procesos) para mitigar riesgos

PROTEGER	3) Establecer los niveles y controles de acceso
	4) Usuarios asignados individualmente
	7) Uso de contraseñas seguras
	12) Realizar copias de seguridad de los datos
	14) Almacenar los datos sensibles y confidenciales en un formato cifrado.

Requisitos OEC - Ciberseguridad

Identificar / Proteger / Detectar /Responder / Recuperar

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas

	Control y Monitoreo
DETECTAR 	6) Sistemas para identificar accesos no autorizados
	9) Protección software/hardware contra malware (antivirus)
	11) Software de seguridad actualizado para maximizar la detección de vulnerabilidades
	18) Probar periódicamente la seguridad de su infraestructura de TI

Requisitos OEC - Ciberseguridad

Identificar / Proteger / Detectar /Responder / Recuperar

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas

Reducir el impacto de un potencial incidente

RESPONDER

16) Planes de respuesta antes ataques

17) Procedimientos de cómo la organización comparte información sobre amenazas de ciberseguridad

Resiliencia y recuperación ante incidentes

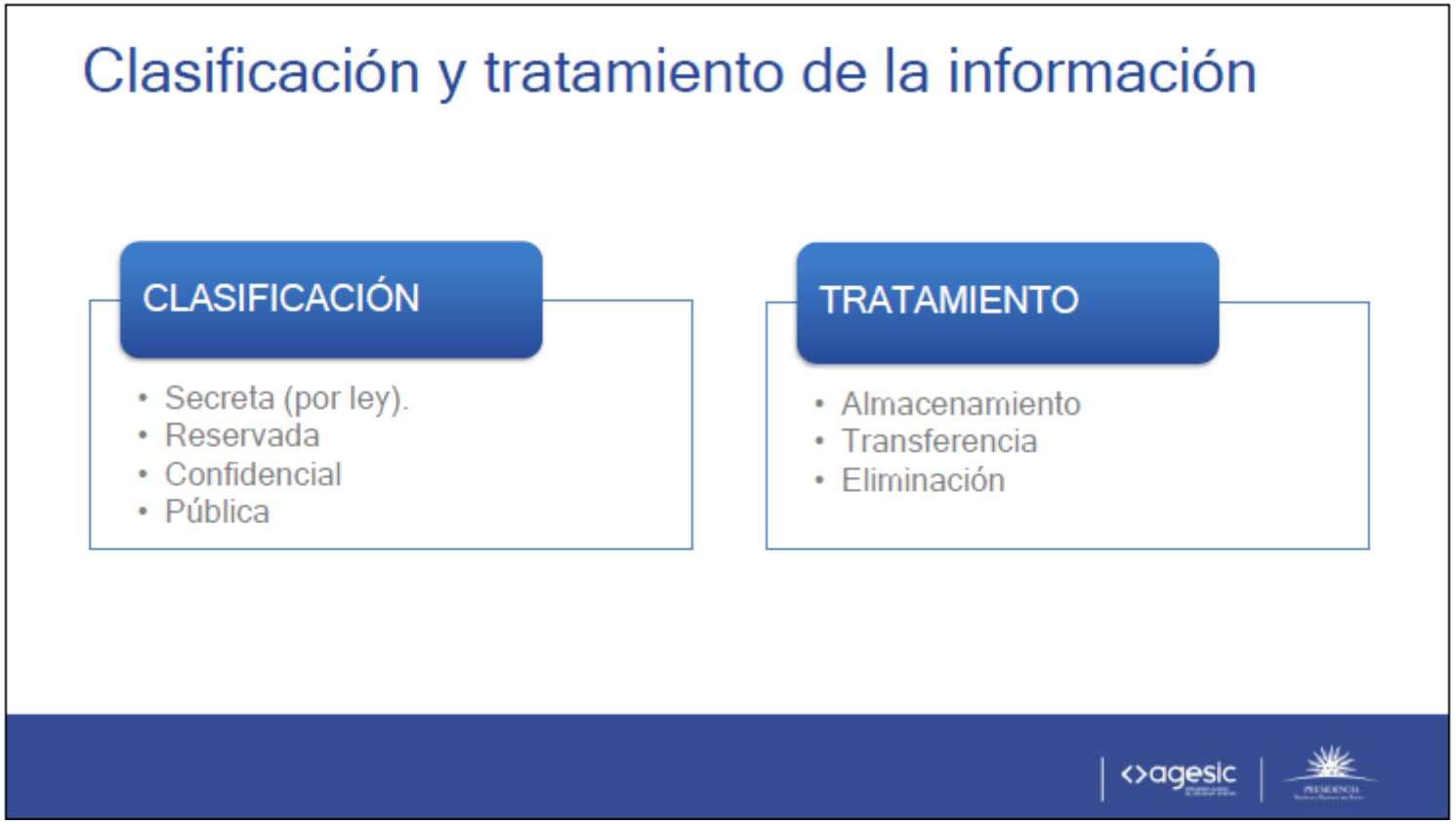
RECUPERAR

22) Contar con un plan de continuidad del negocio frente a fallas de los sistemas informáticos.

Requisitos OEC - Cibserseguridad

Buenas practicas (1/5)

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas



Requisitos OEC - Cibserseguridad

Buenas practicas (2/5)

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas

Bloquear sesión

› Recordá bloquear sesión en tu computadora cuando no la utilices, de esta manera nadie podrá acceder a tu información.

agesic

Requisitos OEC - Cibserseguridad

Buenas practicas (3/5)

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas

Escritorios limpios

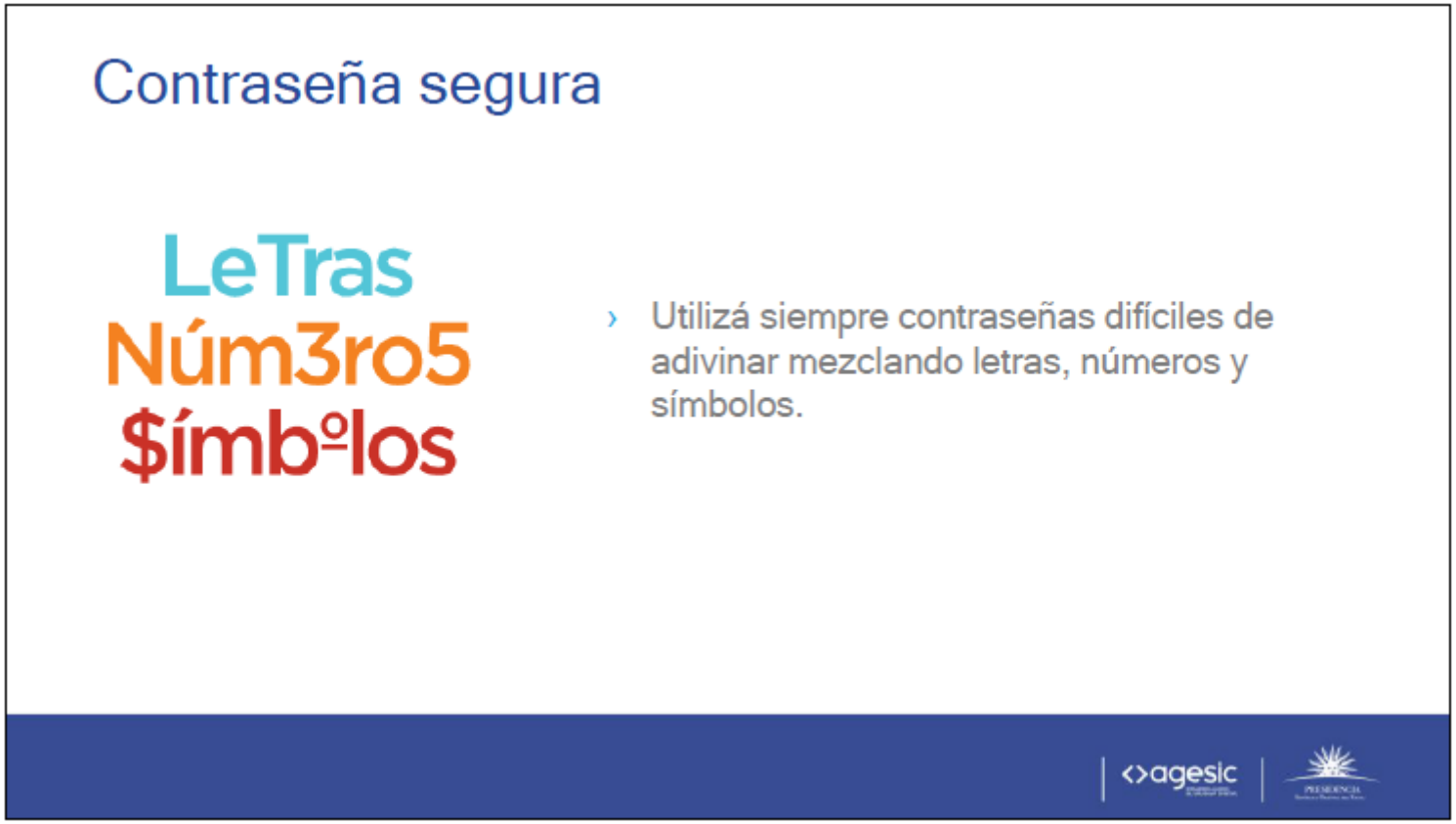
- Guarda bajo llave la información confidencial.
- Retira, sin demora, los documentos de las impresoras.

agesic

Requisitos OEC - Cibserseguridad

Buenas practicas (4/5)

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas



Requisitos OEC - Cibserseguridad

Buenas practicas (5/5)

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas

¿Llegaste a la oficina y no pudiste acceder a tus datos?

› Respaldá siempre tu información en forma periódica. Su resguardo y periodicidad deberá estar alineado con su valor para el organismo.

Informate sobre la política de respaldos de tu organización

agesic

Requisitos OEC - Cibserseguridad

Ingeniería social (o phishing)

Ministerio de Economía y Finanzas
Dirección Nacional de Aduanas

Ingeniería social

- ¿A quien estamos avisando por redes sociales cuando nos vamos de licencia?
- ¿Qué haríamos si encontramos un pen drive en la calle?
- No respondas correos sospechosos ni ingreses a sus enlaces.
- ¿Cómo actuamos ante un pedido de información realizado por teléfono?

Aduana alerta ante dos nuevas modalidades de estafa vinculadas a envíos del exterior

Fecha: 31/01/2023

La Dirección Nacional de Aduanas alerta a la población ante dos nuevas modalidades de estafas que, a través de notificaciones apócrifas, se envía a diferentes personas intentando cobrar un supuesto impuesto por parte de la DNA, ante la presunta llegada de "dinero o paquete con obsequio" del exterior del país.

Modalidad I

En la primera modalidad, la persona recibe el aviso que tiene un paquete con dinero a su nombre y se le solicita cancelar los impuestos relativos al tránsito libre del dinero.

Se le brinda documentación, Resoluciones Generales apócrifas y se le pide realizar el pago de ajuste de impuestos por el 2% del monto enviado más gastos administrativos y de representación.

Modalidad II:

En la segunda modalidad, se comunica desde el exterior un "amigo o familiar" a través de WhatsApp o Facebook, solicitando que le ayude a gestionar un paquete con obsequios. Se le dice a la persona que se le enviará la plata de los costos y Resolución o documento de Aduana donde se informa los costos y penalidades que debe abonar, a través de la cuenta que se le remite.

Muchas gracias

Ministerio
de Economía
y Finanzas

Dirección Nacional de Aduanas