TALLER DE SISTEMA DE GESTIÓN DE PROTECCIÓN

SOCIOS DE NEGOCIOS Y TERCERAS PARTES

Objetivos

- La seguridad de la información y la lucha contra el soborno son pilares fundamentales para la integridad y el éxito de la Administración Portuaria.
- La implementación de las normas ISO 27001 e ISO 37001 en un sistema de gestión integral consolida la confianza de las partes interesadas y protege los activos de ASIPONA.
- Este taller ofrece una introducción a los conceptos básicos de ambas normas y su aplicación en el contexto portuario

Seguridad de la información

Nos encanta compartir…

Religión

Nombre

Dirección

Mis rutas

Perro o Gato

Edad

Dónde comí

Cine

Hermanos

Sexo

Qué me gusta

Teléfono

Donde estoy

Qué escucho

HOY

El 70% de los incidentes de ciberseguridad en seguros son impulsados por la posibilidad de obtener una ganancia económica.

La mayoría de los hackers reconoce que el sector maritimo guarda un tesoro de empleados jóvenes que carecen de experiencia tecnológica.

Cuando acceden sus cuentas usando dispositivos conectados sin seguridad, exponen con frecuencia datos financieros sensibles tales como los números de seguro social, códigos de los cajeros automáticos y contraseñas de las computadoras.

El espionaje está en aumento.

Cuando la gente imagina casos de espionaje, por lo general, no piensa en los puertos, pero lo cierto es que se están convirtiendo en los objetivos principales de los hackers debido a que los datos personales y la información valiosa no están protegidas adecuadamente.

De hecho, una de las peores violaciones de datos que se dio a conocer el año pasado involucró a nueve hackers que supuestamente estaban lanzando una serie de ciberataques en contra de más de 100 puertos de todo el mundo.

Activos

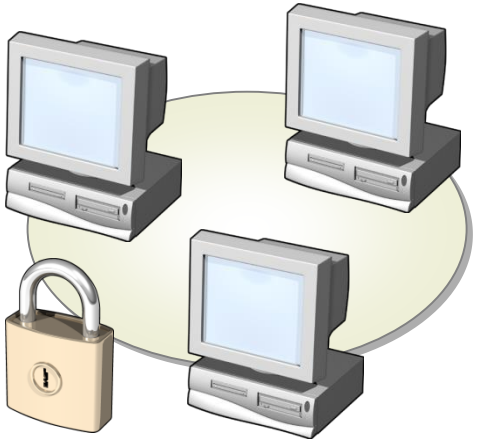
Cualquier elemento que tiene valor para ASIPONA

¿Qué es un activo de información?

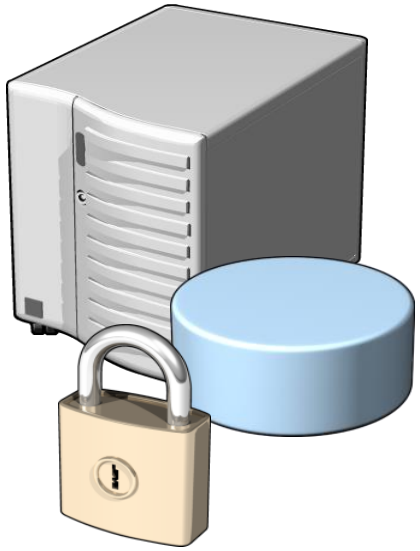
Todo aquello que tiene valor para la ASIPONA

Información

Redes de datos



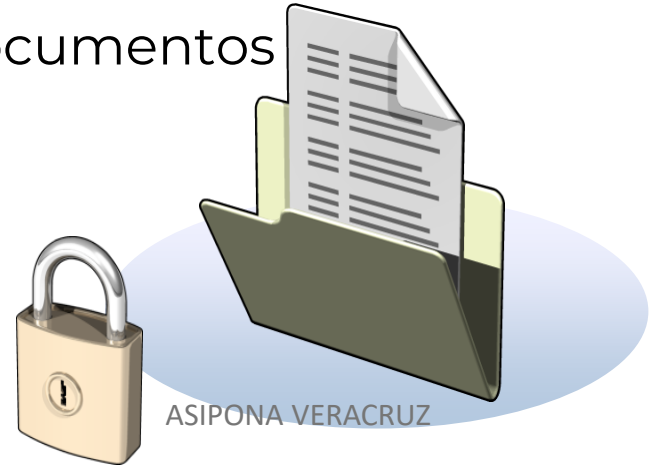
Aplicaciones y base de datos



Internet

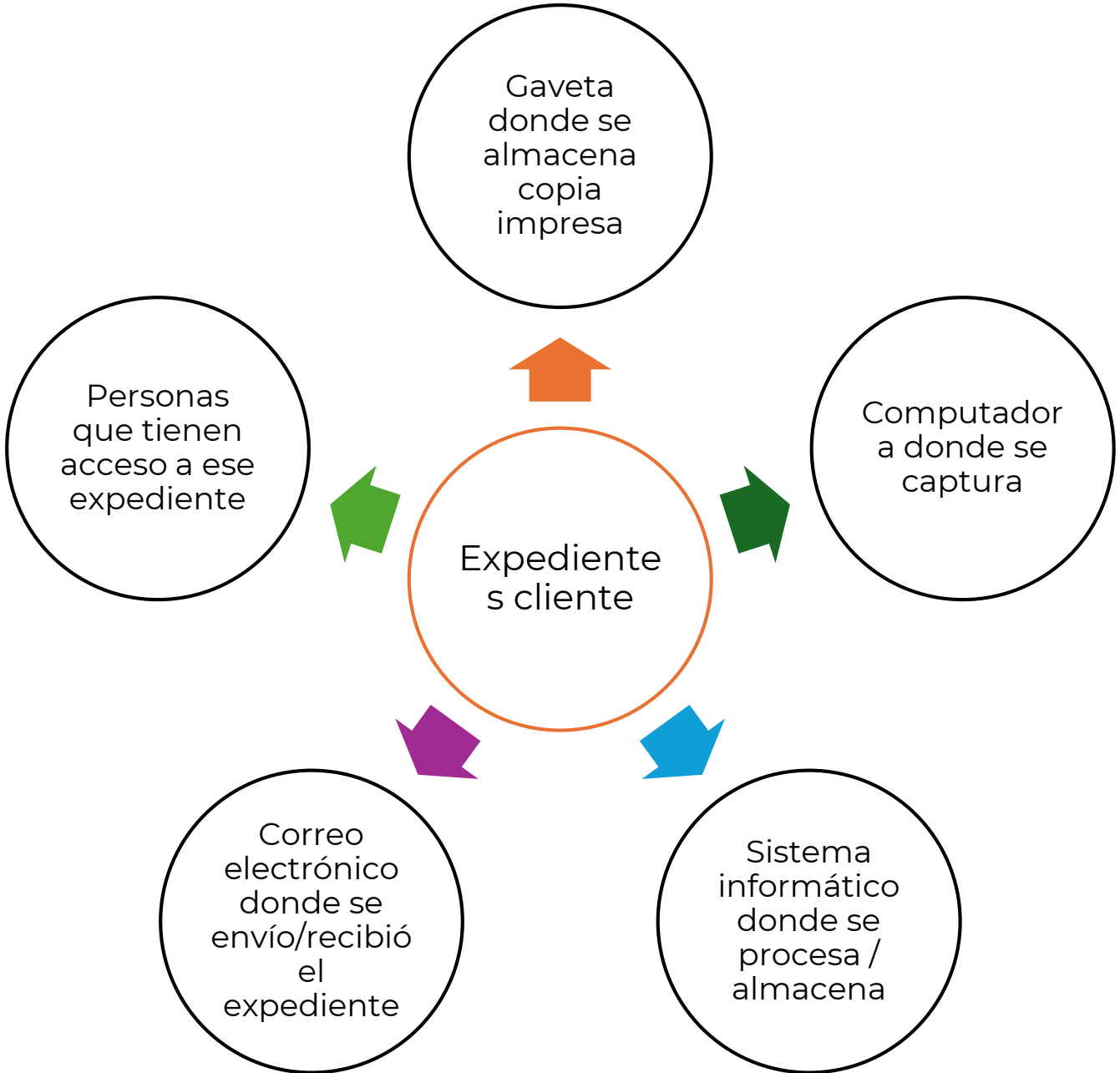
Usuarios

Documentos



Computación móvil

Cómo fluye el activo de información



¿Qué es Seguridad de la Información?

Es el conjunto de metodologías, prácticas y procedimientos que buscan proteger la información como activo valioso contra diferentes amenazas a las que está expuesta y asegurar la continuidad del negocio.

Tener la información justa en el momento oportuno ha significado ‘Poder’, protegerla depende de todos, no solo de las tecnologías de información

Principios de seguridad

¿Qué pasa si la información cae en manos de personas no autorizadas, como por ejemplo un delincuente, un reportero o un competidor?

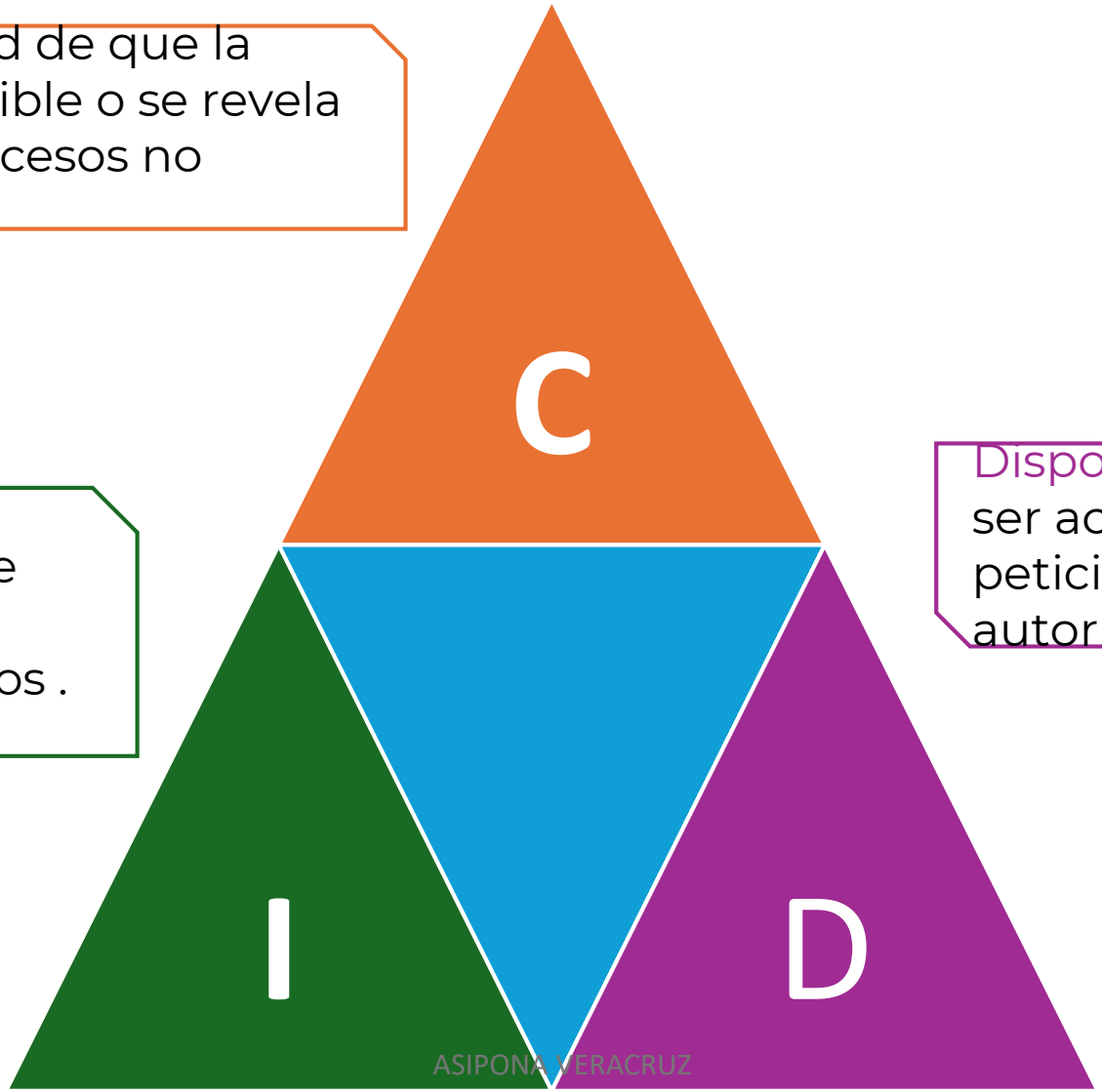
¿Qué pasa si la información se corrompe o se altera accidentalmente o intencionalmente?

¿Qué pasa si la información no está accesible por cierto tiempo?

Principios de Seguridad

Confidencialidad: Propiedad de que la información no esté disponible o se revela a personas, entidades o procesos no autorizados.

Integridad: Propiedad de proteger la exactitud y completitud de los activos .



Disponibilidad: Propiedad de ser accesible y utilizable a petición de una entidad autorizada.

QUE ES LA NORMA ISO 27001

Qué es ISO 27001:2022

- La norma ISO 27001 es como un manual para proteger la información de la ASIPONA. Te ayuda a:
- Organizar: Define cómo proteger la información, desde datos confidenciales hasta el conocimiento del personal.
- Controlar: Establece medidas para prevenir y detectar problemas de seguridad, como robos de datos o errores humanos.
- Mejorar: Te ayuda a identificar puntos débiles y mejorar continuamente la seguridad de la información

Tipos de controles

DOMINIOS DE CONTROLES	NÚMERO DE CONTROLES
A.5 Controles Organizacionales	37
A.6 Controles de personales	8
A.7 Controles físicos	14
A.8 Controles tecnológicos	34

Controles organizacionales

5.1 Políticas para la seguridad de la información

EJEMPLOS

Políticas normativas especificas de:
-General de Seguridad de la información
-Control de Acceso
-Clasificación y manejo de información
-Responsabilidad de usuarios
-Respaldos
-Transferencia de información
-Protección contra el malware
-Gestión de vulnerabilidades técnicas
-Controles criptográficos
-Seguridad en las comunicaciones
-Privacidad y protección de la información de Identificación personal
-Relación con proveedores

Política del SGP

- En la Administración del Sistema Portuario Nacional Veracruz, S. A de C. V. nos comprometemos a administrar, desarrollar, mantener y optimizar la infraestructura portuaria para la adecuada prestación de los servicio portuarios, quedando prohibida cualquier conducta que pueda considerarse un acto de soborno en todas sus formas, contando con la autoridad e independencia necesaria para asegurar el cumplimiento de la Gestión de la Protección del puerto, bajo un marco de trabajo que promueve una cultura ética y transparente enfocado en la mejora continua que facilite el logro de objetivos, metas y programas, que tengan como finalidad, prevenir las amenazas y riesgos que podrían afectar la confidencialidad, integridad, disponibilidad, relevancia y continuidad de los activos administrados.
- Así también, se trabaja en cumplimiento a la las leyes antisoborno y demás legislación aplicable y otros requisitos pertinentes a nuestro contexto organizacional,
- Esta política es de aplicación obligatoria para todos los empleados y partes interesadas relevantes de la ASIPONA VER, y será revisada anualmente para asegurar su pertinencia y efectividad en la consecución de nuestros objetivos de gestión y seguridad.
- Director General
- Rev. 02 23/02/2024

5. 2 Roles y responsabilidades de seguridad de la información

EJEMPLOS

-ROLES: Comité del SGP, Responsable del SGP, Propietario de activos y riesgos, Alta dirección
-MECANISMOS: Nombramientos, Matriz de roles y responsabilidades, Perfiles de puesto

5.12
Clasificación de información

EJEMPLOS

-Establecer reglas o criterios para clasificar la información de acuerdo a su importancia, requisitos legales, este mismo criterio puede utilizarse para los activos. Ejemplo: Sensible, Crítico / Confidencial , Uso interno, público.

5.13
Etiquetado de información

EJEMPLOS

-Procedimiento o guías que indique dónde y cómo se colocan las etiquetas, y excepciones, por ejemplo para información pública. Se recomienda un esquema que sea fácilmente reconocible únicamente por el personal autorizado por ejemplo un esquema de colores o claves . Los metadatos son una forma común de etiquetado de información técnica.

EJEMPLOS

-Procedimientos para proteger la información transferida de la intercepción, copia, modificación, mal enrutamiento y la destrucción-
-Procedimientos para la detección y protección contra software malicioso
-Procedimientos para la protección de la información sensible comunicada de manera electrónica
Los acuerdos deben incluir:
-Mecanismos el control y la notificación de la transmisión, envío y recepción
-Mecanismos para garantizar la trazabilidad y no repudio
-Técnicas de empaquetado
-Normas para la identificación del mensajero
-Proteger los mensajes del acceso no autorizado, modificación o denegación del servicio
-Aprobación para la utilización de servicios públicos, redes sociales, mensajería instantánea
-Protocolos que aseguren el correcto direccionamiento y transporte del mensaje

5.14
Transferencia de información

EJEMPLOS

-Política de acceso que incluya mecanismos para la asignación de privilegios, lineamientos respecto a las restricciones de acuerdo a los roles , requisitos de seguridad en aplicaciones , requisitos para las restricciones, asignación y cambio en permisos de acceso a personal externo, requisitos para la revisión periódica, incluir la premisa de “todo está generalmente prohibido a menos que esté expresamente prohibido”.
Política debe incluir información sobre:
-Redes a la que se va acceder
-Personal que puede acceder a las redes
-Mecanismos de protección
-Medios para acceder a las redes
-Requisitos de autenticación
-Medios para el monitoreo de red

5.15 Control de acceso

EJEMPLOS

Considerar lineamientos respecto a:
-Base de datos de proveedores
-Procedimiento para la gestión de proveedores
-Definición de tipos de acceso y otros requisitos de seguridad
-Contrato , acuerdos
-Evaluación de cumplimiento

5.19
Seguridad de la información en las relaciones con los proveedores

EJEMPLOS

El acuerdo debe contener:
-Descripción de la información que se va a proporcionar
-Incluir el esquema de clasificación
-Cumplimiento de regulaciones como protección de datos y derechos de autor y mecanismos para el cumplimiento
-Reglas para la uso y manejo de la información
-Gestión de incidentes
-Contactos principales
-Cumplimiento de políticas internas
-Disputas contractuales

5.20
Abordar la seguridad de la información dentro de los acuerdos con proveedores

EJEMPLOS

Considerar en los contratos :
-Requisitos de seguridad
-Responsabilidades para subcontratados por parte del proveedor
-Mecanismos monitoreo y validación de servicios críticos
-Obtención de garantías de componentes críticos
-Reglas para el intercambio de información, uso y tratamiento de información entre todas las partes

5.21
Gestión de la seguridad de la información en la cadena de suministro de las TIC

EJEMPLOS

Monitorear el cumplimiento de los acuerdos
-Revisar los informes de servicios
-Realizar auditorías a proveedores
-Revisar información sobre incidentes de seguridad
-Implementar mejoras parar resolver problemas de seguridad
Considerar :
-Cambios en los acuerdos
-Cambios en mejoras, desarrollo de proyectos
-Cambios internos
-Cambios en controles
-Cambios en tecnologías o infraestructura
-Cambios en subcontratación

5.22
Seguimiento, revisión y gestión del cambio de los servicios de los proveedores

5.24
Planificación y preparación de la gestión de incidentes de seguridad de la información

EJEMPLOS

Considerar:
-Planificación y preparación de respuesta a incidentes
-Monitoreo, detección, análisis y reporte de eventos e incidentes
-Manejo de evidencia forense
-Evaluación y decisiones sobre eventos de seguridad
-Escalación y recuperación de un incidente
Capacitación del personal sobre mecanismos para reportar un evento o incidente de seguridad y actividades de contención básicas
Referencia a Contacto con autoridades y grupos de especial interés y procedimiento disciplinario

5.31
Determinación de la legislación aplicable y requisitos contractuales

EJEMPLOS

Considerar:
-Identificarse, Registrarse y actualizarse la legislación aplicable y conocer sus requisitos.
Considerar:
-Restricciones sobre la importación y / o exportación de hardware y software para realizar funciones criptográficas, uso de cifrado
-Asesoramiento jurídico

5.32
Derechos de propiedad intelectual

EJEMPLOS

Mecanismos para proteger el material con propiedad intelectual
Implementar una política que defina su uso
Registrar la información y cumplimiento de los requisitos de propiedad intelectual
Realizar revisiones al licenciamiento y material
Concientizar al personal sobre las políticas

5.36
Cumplimiento de las políticas y normas de seguridad

EJEMPLOS

Considerar:
-Identificar las causas de incumplimiento
-Acciones correctivas apropiadas
-Revisar y verificar las acciones para identificar en cualquier deficiencia o debilidades

5.37
Procedimientos operativos documentados

EJEMPLOS
Procedimientos de: Instalación y configuración de los sistemas Respaldos y monitoreo Procesamiento y manejo de información automatizada y manual Procedimientos de reinicio y recuperación del sistema Incidentes Instrucciones para el manejo de errores

Controles personales

EJEMPLOS

-Programa de concientización se sugiere incluya una serie de actividades de concientización, tales como campañas (por ejemplo, un “día de seguridad de la información”) y emisión de folletos y boletines
-Capacitación que incluya políticas, reglas de seguridad, proceso disciplinario, qué hacer en caso de incidentes de seguridad y contingencias
-Evaluación del conocimiento adquirido

6.3 Concientización, educación y capacitación en seguridad de la información

6.8
Reporte de eventos de seguridad de la información

EJEMPLOS

Eventos referentes a control de seguridad ineficaz, violaciones de seguridad, errores humanos, incumplimientos de políticas o lineamientos, daño a medidas físicas, cambios no controlados, mal funcionamiento de SW HW, violaciones de acceso
Informar sobre posibles brechas de seguridad física o lógica, como un mal procesamiento de datos, o información el mal funcionamiento de controles de acceso.
El personal necesita ser consiente respecto a no intentar probar presuntas debilidades de seguridad

Controles de Seguridad Física

EJEMPLOS

-Reforzar perímetros de construcción solidas con barras, alarmas, cerraduras, contar un área de recepción, instalar sistemas adecuados de detección de intrusos

7.1
Perímetro de Seguridad física

EJEMPLOS

-Bitácora de visitantes
-Tarjetas de proximidad, biométricos, tarjeta de acceso y el PIN secreto
-Gafetes
Revisión y actualización periódica de los controles
-Identificar una zona de área de entrega y carga aislada de otras áreas
-Identificar y registrar al personal autorizado a esa zona y material entrante
-Inspeccionar el material entrante

7.2
Controles físico de entrada

EJEMPLOS

-Sin señalamientos obvios
-Instalaciones donde no sea visible las actividades realizadas
-No tener accesible los directorios y guías telefónicas internas

7.3
Aseguramiento de oficinas, salas e instalaciones

EJEMPLOS

-Extintores de humo
-Aspersores de humo
-Hidrantes
-Alarmas contra incendio
-Válvulas de Corte de Gas y electricidad

7.5
Protección contra amenazas externas y ambientales

7. 7 Escritorio limpio y pantalla limpia

EJEMPLOS

-Mantener guardada información sensible o crítica
-Desconectar o proteger los equipos y terminales con un protector pantalla y un mecanismo de bloqueo
-Proteger escáneres, copiadoras impresoras contra acceso no autorizado
-Retirar inmediatamente documentos de estos periféricos

EJEMPLOS

-Lugares que no bloquee pasillos o cableado
-Salvaguardar los elementos que requieren protección especial
-Alarmas que permitan prevenir cualquier eventualidad
-Establecer lineamientos para comer, beber y fumar
-Candados para laptops
-UPS, planta de emergencia

7.8
Ubicación y protección del equipo

EJEMPLOS

-No dejar desatendido el equipo y medios
-Controles de acceso físicos y lógicos
-Registro de activos móviles o autorizados para sacar fuera de las instalaciones

7.9
Seguridad de los equipos y activos fuera de las instalaciones

Controles Tecnológicos

8.1
Política de dispositivos móviles

EJEMPLOS

DISPOSITIVOS: Celulares, laptops, tabletas
La política debería considerar: el registro de dispositivos móviles, los requisitos de protección física, la restricción de la instalación de software, los requisitos para las versiones de software de dispositivos móviles y la aplicación de parches, la restricción de la conexión a los servicios de información, los controles de acceso, las técnicas criptográficas, la protección contra el malware, la desactivación, borrado o bloqueo remoto, los respaldos, el uso de los servicios y aplicaciones web.
-Bloqueo automático de sesiones
-Cierre de sesiones automático en aplicaciones
-Protector de pantalla
-Terminar las sesiones activas cuando hayan terminado

8.10 Eliminación de información

EJEMPLOS

a) seleccionar un método de eliminación (por ejemplo, sobreescritura electrónica o
borrado criptográfico) de conformidad con los requisitos empresariales y
teniendo en cuenta las leyes y reglamentos pertinentes;
b) registrar los resultados de la supresión como prueba;
c) cuando se utilicen proveedores de servicios de eliminación de información,
obteniendo evidencia de eliminación de información de ellos.
Cuando terceros almacenen la información de la ASIPONA en su nombre, se sugiere
que la ASIPONA considere la inclusión de requisitos sobre la eliminación de
información en los acuerdos de terceros para hacerla cumplir durante y después de la terminación de dichos servicios

8.30
Desarrollo de sistemas subcontratado

EJEMPLOS
Acuerdos de propiedad y derechos de código, licenciamiento Requisitos respecto a desarrollo seguro Pruebas de aceptación sobre la calidad y precisión Derecho a auditar los procesos y controles

ISO 37001:2016

Qué es la ISO 37001:2016

- La ISO 37001 es una norma internacional que proporciona un marco para prevenir y detectar el soborno.
- La norma establece los requisitos para un sistema de gestión antisoborno (SGAS).

Tipos de controles

- El SGAS incluye medidas como:
  - Política antisoborno
  - Evaluación de riesgos
  - Controles de soborno
  - Capacitación
  - Monitoreo y revisión
  - Comunicación

Que es el soborno

- El soborno es un delito grave que puede tener consecuencias devastadoras para las empresas y las personas.
- La industria portuaria es particularmente vulnerable al soborno debido a la naturaleza compleja de las operaciones y la gran cantidad de actores involucrados.
- La norma ISO 37001 proporciona un marco para prevenir y detectar el soborno en cualquier ASIPONA.

Definición

- El soborno es ofrecer, dar o prometer algo de valor a un funcionario público con la intención de influir en su comportamiento.
- El soborno puede tomar muchas formas, incluyendo dinero, regalos, favores o promesas de empleo.
- Tanto el que ofrece el soborno como el que lo recibe son responsables del delito.

Ejemplos

- Soborno a funcionarios públicos: Para obtener permisos, licencias o contratos.
- Soborno a empleados: Para agilizar el despacho de aduanas, la carga o la descarga de barcos.

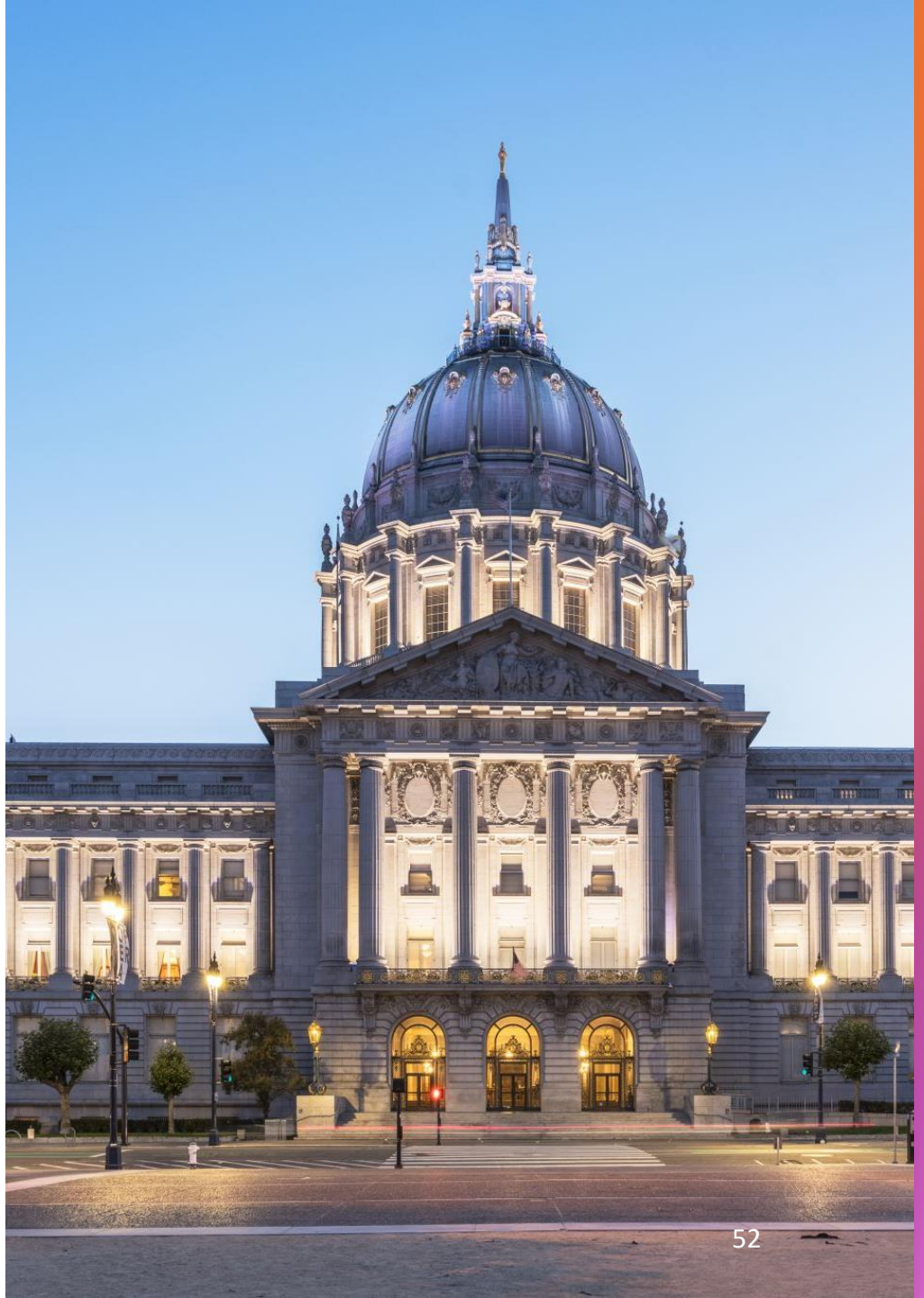
Ejemplos

- Soborno a proveedores: Para obtener contratos o favores.
- Soborno a otros actores: Como agentes marítimos, estibadores o empresas de transporte.

Definiciones

funcionario público

- toda persona que ocupe un cargo legislativo, administrativo o judicial, por designación, elección o como sucesor, o cualquier persona que ejerza una función pública, incluso para un organismo público o una empresa pública, o cualquier funcionario o agente de una organización pública local o internacional, o cualquier candidato a un cargo público

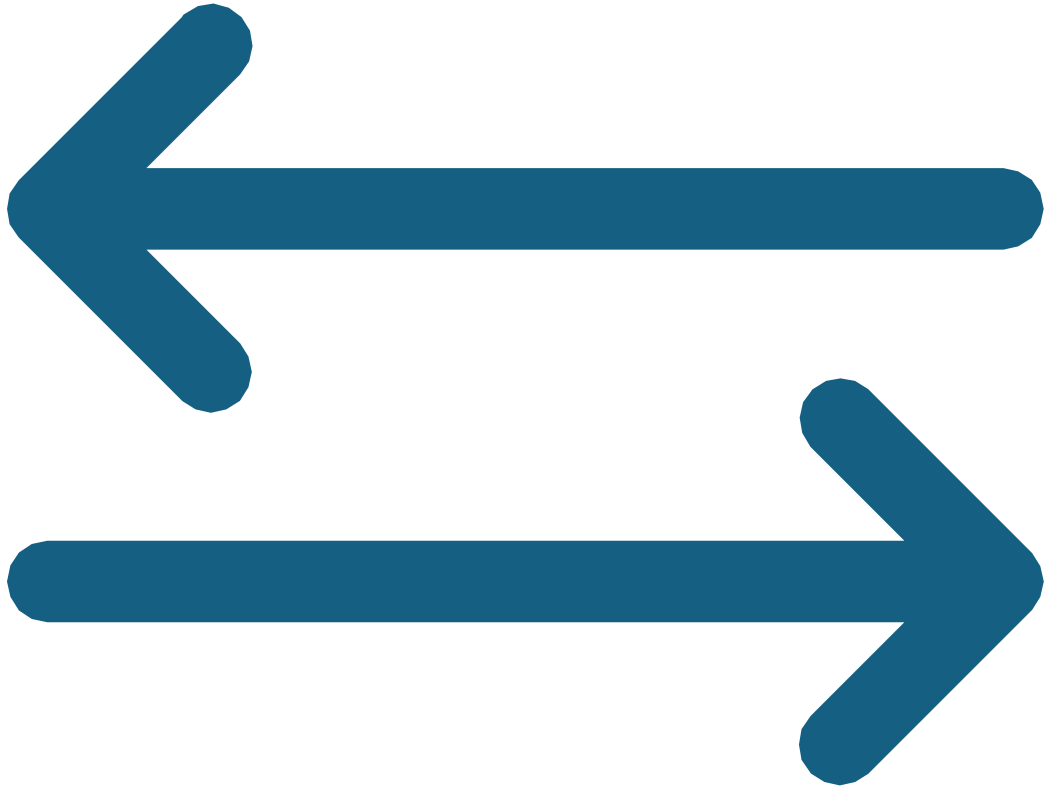


conflicto de intereses

- Situación donde los intereses de negocios, financieros, familiares, políticos o personales podrían interferir con el juicio de valor del personal en el desempeño de sus obligaciones hacia la organización.

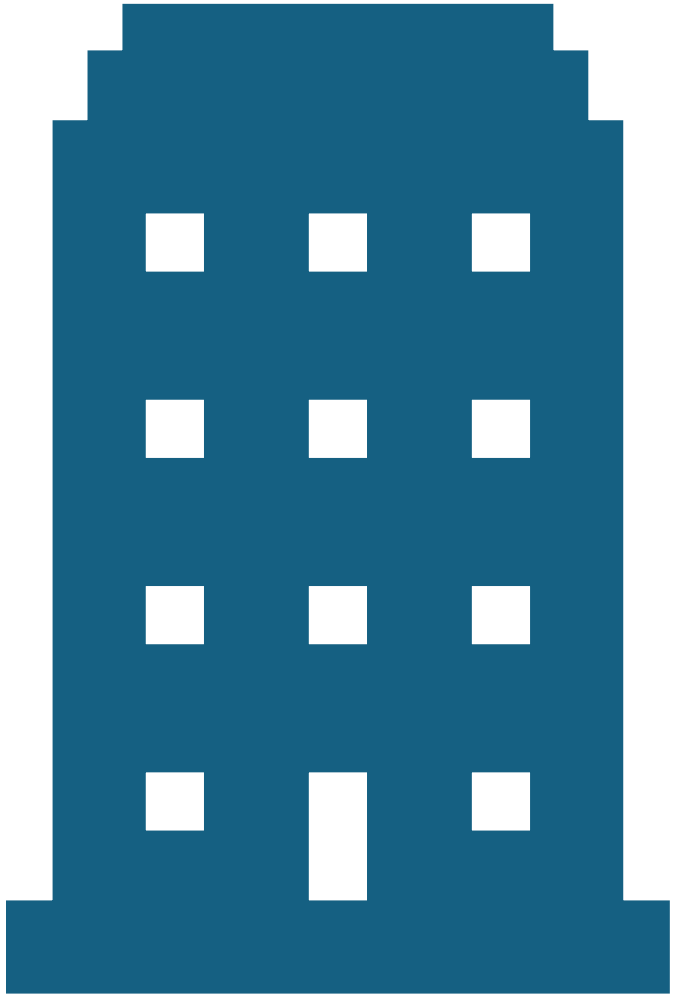
Socio de negocios

- Parte externa con la que la organización tiene, o planifica establecer, algún tipo de relación comercial



Socio de negocios

- Nota 1a la entrada: Socio de negocios incluye pero no se limita a los clientes, consumidores, "alianza empresarial", socios de alianzas empresariales, miembros de un consorcio, proveedores externos, contratistas, consultores, subcontratistas, proveedores, vendedores, asesores, agentes, distribuidores, representantes, intermediarios e inversores.

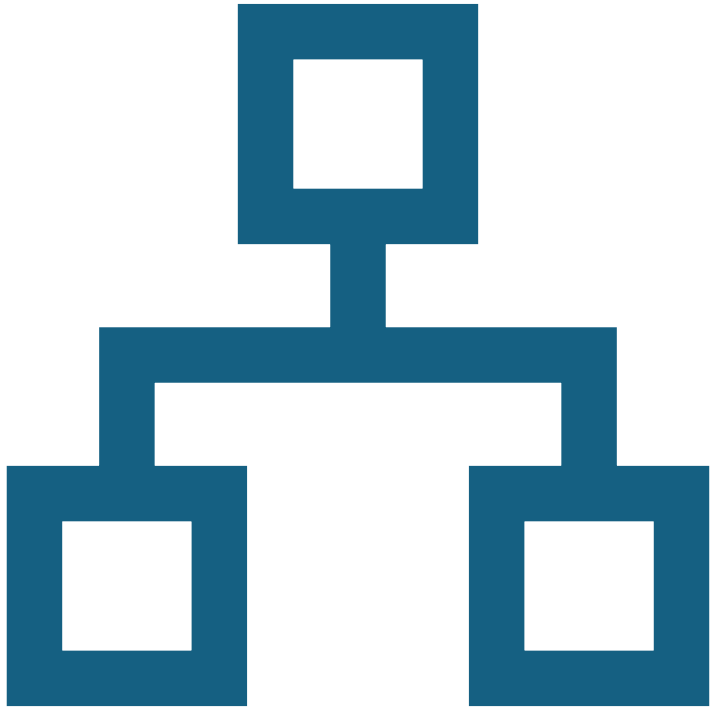


Socio de negocios

- Esta definición es deliberadamente amplia y debería interpretarse de acuerdo con el perfil de riesgo de soborno de la organización, para que se aplique a los socios de negocios que razonablemente se entienda que pueden exponer a la organización a riesgos de soborno.

Socio de negocios

- Nota 2 a la entrada: Diferentes tipos de socio de negocios plantean diferentes tipos y grados de riesgo de soborno, y una organización tendrá diferentes grados de capacidad para influir en diferentes tipos de socio de negocios.



Tercera parte

- Persona u organismo que es independiente de la organización
- Nota 1 a la entrada: Todos los socios de negocios son tercera parte, pero no todas las terceras partes son socios de negocios.

Controles Antisoborno

- Debida diligencia
- Controles Financieros
- Controles NO Financieros

Ejemplos de controles

- Código de conducta: Establece los principios y valores que deben seguir los empleados en relación con el soborno.
- Capacitación: Se debe brindar capacitación a los empleados sobre la política antisoborno y cómo identificar y reportar el soborno.
- Evaluación de riesgos: Se debe realizar una evaluación de riesgos para identificar las áreas donde existe un mayor riesgo de soborno.

Controles

- Controles de soborno: Se deben implementar medidas para prevenir el soborno en las áreas de mayor riesgo, como:
  - Procedimientos de licitación transparentes: Asegurar que todos los proveedores tengan la misma oportunidad de competir por contratos.
  - Regalos y hospitalidad: Establecer una política clara sobre la aceptación de regalos y hospitalidad.
  - Conflictos de interés: Implementar medidas para prevenir y detectar los conflictos de interés.

Ejemplo de reporte

- Es importante tener un proceso claro para reportar el soborno.
- Los empleados deben poder reportar el soborno sin temor a represalias.
- Se deben investigar todas las denuncias de soborno de manera justa y transparente

Ejemplo

Involúcrado	Ejemplo	Responsabilidad
Funcionario público	Oficial de aduanas que acepta un soborno para agilizar el despacho de aduanas.	Solicitar o aceptar el soborno.
Empleado de la administración portuaria	Estibador que acepta un soborno para cargar o descargar un barco de manera preferencial.	Solicitar o aceptar el soborno.
Persona que ofrece el soborno	Representante de una empresa naviera que ofrece un soborno para obtener un contrato.	Ofrecer o prometer el soborno.
Intermediario	Agente marítimo que actúa como intermediario para facilitar el soborno.	Facilitar el soborno entre las dos partes.

Ejemplo

Rol	Ejemplo de Nombre/Posición	Descripción
Autoridad Portuaria	Juan Pérez, Director de la Administración Portuaria	La autoridad máxima responsable de la gestión del puerto.
Funcionario Corrupto	María García, Jefa de Inspección Aduanera	Persona dentro de la administración que acepta sobornos para agilizar procesos o ignorar irregularidades.
Empresa Sobornadora	XYZ Importaciones S.A.	Empresa que busca ventajas ilegítimas a través del soborno en la administración portuaria.
Intermediario	Luis Ramírez, Consultor de Logística	Individuo que actúa como enlace entre la empresa sobornadora y el funcionario corrupto.
Testigo	Roberto Torres, Empleado descontento	Persona que, consciente o no, puede proporcionar información sobre el soborno y sus participantes.

Como contribuyes TU a que el SGP tenga éxito

- Atendiendo las políticas y lineamientos del SGP
- Cuidando tu información y la información de la ASIPONA
- Evitando caer en algún escenario de SOBORNO
- Reportando cualquier irregularidad