HAGAMOS UN TRUEQUE
TLC MAGAZINE MÉXICO

TRADE LAW & CUSTOMS magazine
arquitectura aduanera
TLC ASOCIADOS

6 DE MAYO DEL 2021

Recomendaciones CTPAT sobre ciberseguridad

Lic. Karen Anaya Mendoza

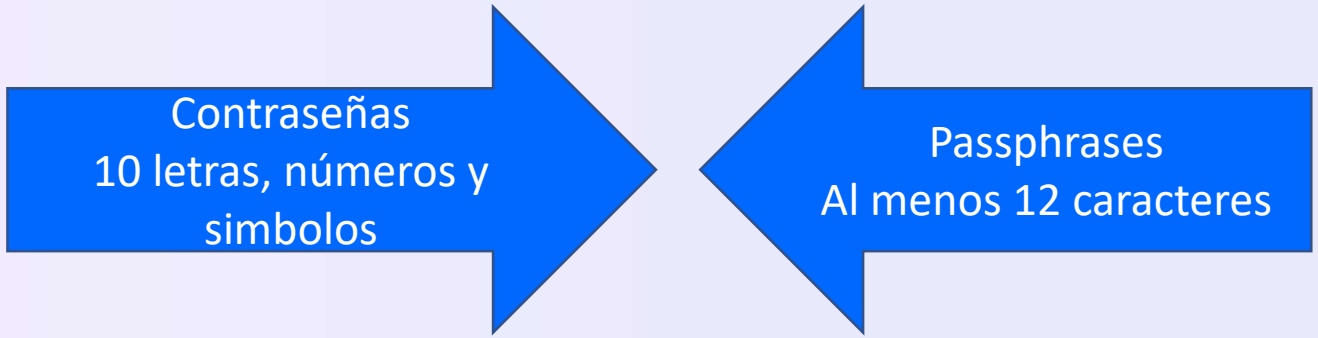
Boletín CTPAT

Mayo 2020

Passwords, passphrases

Criterio 4.8 de los MSC

Recomienda el uso de la autenticación multifactor, uso de passphrases o contraseñas más fuertes.



- No utilizar contraseñas basadas en información personal.
- Las contraseñas no deben incluir palabras del diccionario
- Tener un procedimiento documentado en caso de una contraseña comprometida.
- Utilizar contraseñas diferentes para diferentes cuentas.
- No permitir a los usuarios elegir una contraseña que se haya utilizado en las últimas cuatro ocasiones.
- Concientizar a los empleados acerca del uso correcto y protección de las contraseñas

ALERTA CTPAT

Octubre 2020

Ciberseguridad:

Como detectar un phish.

Ataques de Phishing utilizan emails o paginas web maliciosas para infectar los equipos con malware y virus para obtener información personal, empresarial o financiera. Los cibercriminales intentan atraer a los usuarios a hacer clic en un link o abrir un adjunto que infecta las computadoras.

A. Ser cauteloso

B. Verificar uno de los indicadores:

1. Asuntos genéricos
2. URLs sospechosos
3. Uso incorrecto de copyright
4. Mala ortografía o redacción
5. Urgencia innecesaria

C. Practicar buenos ciber hábitos

Responder | Reenviar | Archivar | No deseado | Eliminar | Más

De: Online Bbva.es <info@graexcon.com>
Asunto: **Bbva(es): verifique su cuenta introduciendo...** 29/07/2019 18:39
A: undisclosed-recipients:;

BBVA

Hola, su cuenta en línea ha sido suspendida temporalmente.

Necesitamos que verifique su cuenta introduciendo sus credenciales y SMS verificacion .

Asegurese de introducir sus datos correctamente y su numero de telefono esta cerca de usted para verificar su identidad por el telefono adormecer: .

1- Acceder a mi

2- Ingrese el codigo de verificacion de SMS en la pagina de verificacion

3- inicie sesion y siga los pasos haciendo clic a continuacion:

Acceder a mi

Nota: Si usted no activa su cuenta en el próximo 24Hours usted será suspendido de nuestros servicios bancarios.

BBVA Espana Merchant Services, Entidad de Pago S.L.U., Calle Isla Graciosa 5, 28703 San SebastiÃ¡n de los Reyes, Madrid, Espana.

http://fortyone.web.id/dist/re/

De: Agencia Tributaria 13:00 <gestion.32@agenciatributaria.net>
Para: [redacted]
CC:
Asunto: Denuncia - factura no declarada - 2019 13:00

Mensaje | Denuncia - factura no declarada - 2019.xls (41 KB)

Se ha presentado una denuncia contra su empresa con respecto a una factura no declarada.

Un representante de la Agencia Tributaria se pondrá en contacto con usted en los próximos 3 días laborales para planificar una reunión y una respuesta oficial.

La queja ha sido presentada por una empresa con sede en Madrid con respecto a una factura emitida y pagada **en noviembre de 2019**.

También tenemos en consideración que puede ser una queja falsa o realizada de manera incorrecta.

Puede encontrar más información sobre la empresa que presentó la queja y la factura en el archivo adjunto.

Por favor, consulte el archivo y verifique la información.
La denuncia recibida y la factura se adjuntan a este mensaje.

Según su respuesta, consideraremos las medidas adicionales que debe tomar (Agencia Tributaria).

EA37

Por favor, no responda a este correo. Este es un correo automatizado sólo utilizado para enviarle avisos por correo electrónico.
Si tiene cualquier pregunta utilice nuestros servicios de información y asistencia tributaria que encontrará en www.agenciatributaria.es

Atentamente
Agencia Estatal de Administración Tributaria

La información incluida en el presente correo electrónico es SECRETO PROFESIONAL Y CONFIDENCIAL, siendo para el uso exclusivo de su destinatario.Si usted no es el destinatario del mensaje o ha recibido esta comu
prohibida cualquier divulgación, distribución o reproducción de esta comunicación

Alerta CTPAT

Enero 2021

Cyberamenazas: La nube y conexiones remotas

Debido a la pandemia muchos ciberdelincuentes han explotado los puntos débiles relacionados a las configuraciones de trabajo remoto. Se ha reportado un aumento de intrusiones a las redes, pérdida de datos o ransomware.

Las empresas han mudado sus operaciones a soluciones en la nube.

- Implementar autenticación Multifactor
- Políticas para prohibir uso de dispositivos personales
- Restringir usuarios de reenviar correos fuera del dominio de la empresa
- Restringir descarga de programas y apps sin autorización
- Reforzar concientización y entrenamiento
- Establecer herramientas de reporte de sospechas

Alerta CTPAT

Marzo 2021

Cyberamenazas: Vulnerabilidades de Microsoft Exchange

El Microsoft Exchange Server es un software propietario de colaboración entre usuarios, desarrollado por Microsoft. Es parte de la familia Microsoft Server ya que es una de las aplicaciones destinadas para el uso de servidores.

- La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) y la Oficina Federal de Investigaciones (FBI) publicaron una alerta conjunta relevante para la amenaza cibernética asociada con la explotación activa de vulnerabilidades en los productos locales de Microsoft Exchange. La alerta conjunta indica que varios grupos de amenazas persistentes avanzadas (APT, por sus siglas en inglés) están intentando explotar esta vulnerabilidad y apuntar a agencias del Poder Ejecutivo Civil Federal, así como a empresas privadas e instituciones académicas. Se recomienda encarecidamente a los miembros de CTPAT que se tomen en serio esta amenaza y verifiquen si esta alerta es aplicable a su empresa. Si la alerta es relevante para la empresa de un Miembro, el personal de TI debe comenzar a seguir todos los pasos aplicables para mitigar las amenazas asociadas con las vulnerabilidades establecidas en la alerta y sus documentos correspondientes.

https://www.ic3.gov/Media/News/2021/210310.pdf

National Institute of Standards and Technology

- **Identificar**

Identificar y controlar quien tiene acceso a la información de la empresa

- **Proteger**

Funciones para prevenir, limitar y contener riesgos a los sistemas de ciberseguridad

- **Detectar**

Contar con herramientas que permitan descubrir anomalías en tiempo

- **Responder**

Contar con un plan de contingencia y acciones de respuesta

- **Recuperar**

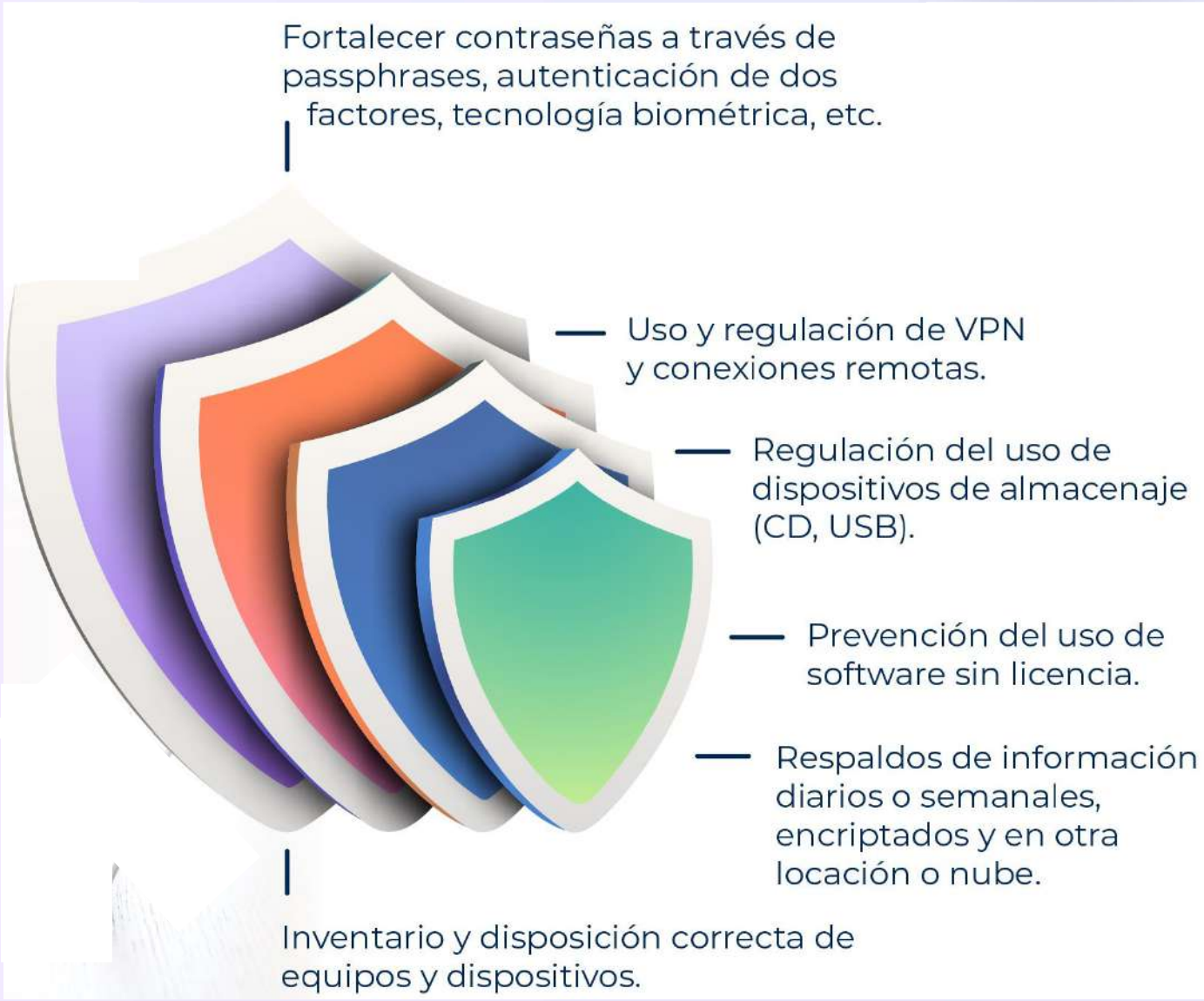
Contar con planes de resiliencia después de un incidente de ciberseguridad
Regla 3-2-1

Criterios mínimos de seguridad CTPAT

Ciberseguridad

Criterios mínimos de seguridad CTPAT

Ciberseguridad



Recomendaciones

- Establecer un equipo IT a la altura de la organización
- Realizar análisis de vulnerabilidades periódicamente
- Establecer políticas y procedimientos documentados
- Mantenerse al tanto de alertas y nueva información
- Reforzar las capacitaciones y concientizaciones a los usuarios
- Realizar auditorías y verificaciones periódicas a los usuarios y las redes de la empresa
- Transmitir concientización a los socios comerciales
- Ante cualquier duda, sospechar y reportar

TRADE LAW & CUSTOMS magazine

TLC MAGAZINE MÉXICO

HAGAMOS UN TRUEQUE

PODCAST DE TLC MAGAZINE MÉXICO

Escúchanos en:

Spotify®

Apple Podcasts

www.tlcmagazinemexico.com.mx

contacto@tlcmagazinemexico.com.mx

SERVICIOS
TLC ASOCIADOS

- Soluciones legales especializadas.
- Acompañamiento en visita domiciliaria y revisiones de gabinete.
- Mantenimiento para empresas IMMEX.
  - NANO FIT
  - IMMEX 360°
- Mantenimiento a empresas PYMEs.
- Certificación y mantenimiento de OEA y CTPAT.
- Cumplimiento de Anexo 24 y Anexo 31.
- Auditorías preventivas y de cumplimiento.
- Certificación IVA e IEPS.
- Trámites y gestiones en comercio exterior.
- Consultoría fiscal y de comercio exterior.
- Clasificación arancelaria.
- Capacitaciones especializadas.
- Impuestos corporativos.
- Arquitectura aduanera.
- Auditoría de cumplimiento T-MEC.
- Biblioteca virtual TLC INFINITI.