URIBE · YÁÑEZ

Asesores Legales

CIBERSEGURIDAD


The Data Dollar Store - A Data Shopping Social Experi...
Copy link
Watch on YouTube
"¿Qué me darías por un grabado?"

Tap Here


Why would a fly land on something like this?
Rats should be ashamed for falling in this trap
BEARS!! This is ridiculous!
This must be fun!
Investment banking

URIBE · YÁÑEZ

¿CÓMO PREVENIR ATAQUES CIBERNÉTICOS?

¿POR QUÉ ES IMPORTANTE PREVENIRLOS?

URIBE · YÁÑEZ

1

¿QUÉ ES LA CIBERSEGURIDAD?

URIBE · YÁÑEZ

¿Qué es la Ciberseguridad?

"La ciberseguridad es la protección de sistemas informáticos, redes y dispositivos electrónicos contra ataques maliciosos, robo de información y daños a la propiedad. La ciberseguridad abarca una variedad de medidas de seguridad informática, incluyendo la protección de datos, la autenticación de usuarios, la prevención de intrusiones y la detección de malware."

Stallings, W., Brown, L., Bauer, M., & Van Duyne, D. (2019). Computer Security: Principles and Practice. Pearson Education.

URIBE · YÁÑEZ

Tap Here

URIBE · YÁÑEZ

Principios de la Información

Integridad

No alteración de la información sin autorización.

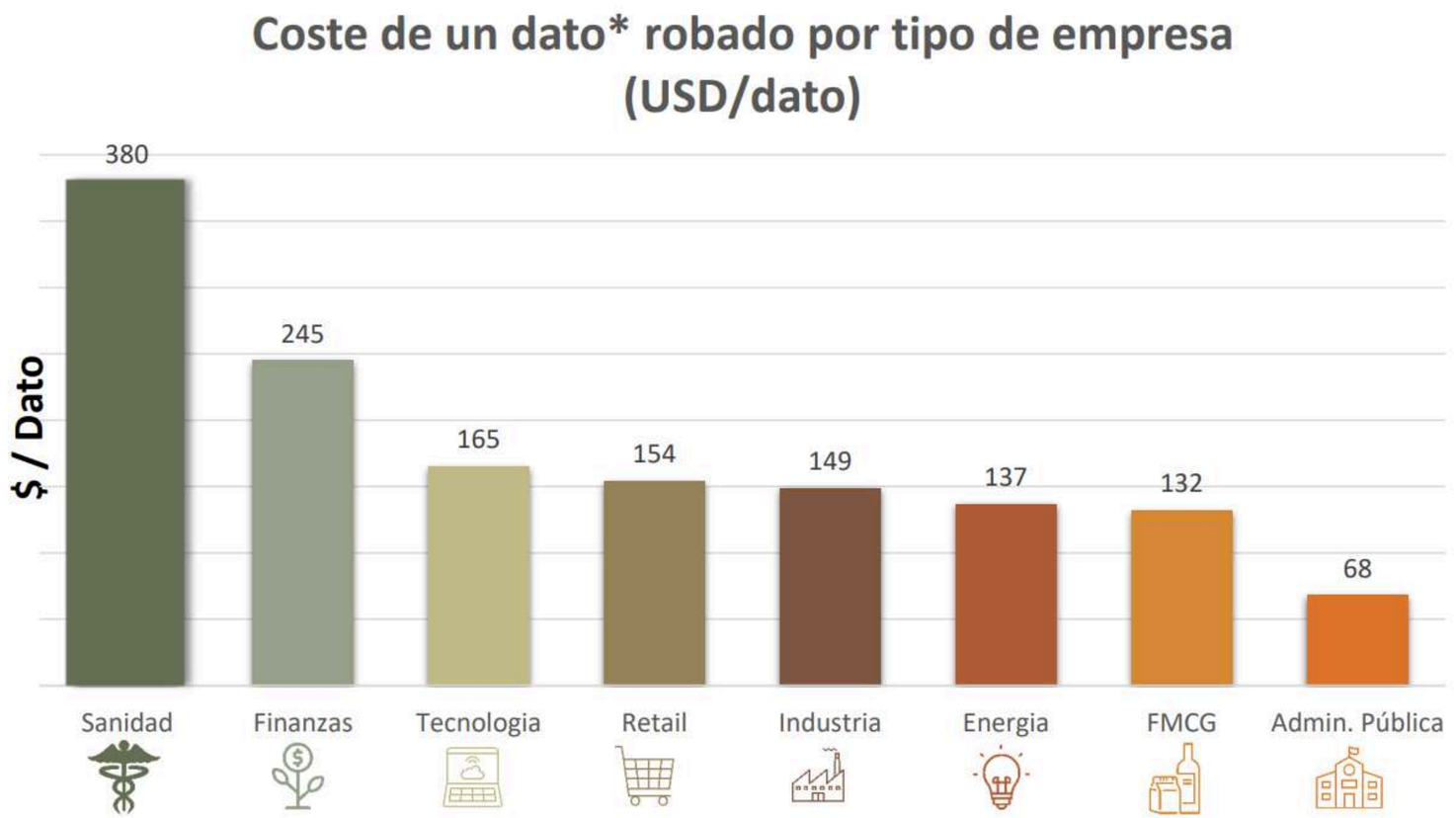
Confidencialidad

No visualización de los datos por personas no autorizados.

Disponibilidad

Cuando se necesiten hacer operaciones con los datos, deben estar disponibles.

¿Qué Daños Generan los Ciberataques a las Empresas?



*Información que contenga datos sensibles (ficha médica, datos de productos financieros, etc.) https://www.varonis.com/blog/cybersecurity-statistics

ERRORES HUMANOS

Imagen adaptada al español. Autor desconocido.

¿De qué sirve tener sistemas perfectamente diseñados para contrarrestar amenazas cuando el usuario no está capacitado?

URIBE · YÁÑEZ

National Cyber Security Centre
a part of GCHQ

10 Pasos de la Ciberseguridad

Colección diseñada para medianas y grandes empresas. Se recomienda revisar su enfoque de gestión de riesgos junto con estos 10 consejos para alcanzar sus objetivos comeciales.

Manejo de Riesgos

Adopte un enfoque basado en el riesgo para proteger sus datos y sistemas.

Compromiso y Formación

Construya seguridad de forma colaborativa

Gestión de activos

Sepa qué datos y sistemas tienes y obtenga su mayor provecho.

Arquitectura y Configuración

Diseñe, construya, mantenga y administre sistemas de manera segura.

Gestión de Vulnerablidades

Mantenga sus sistemas protegidos durante su ciclo de vida.

Manejo de identidad y acceso

Controle quién y qué puede acceder a sus datos y sistemas

Seguridad de datos

Proteja la información que pueda ser objeto de vulneración.

Registro y Monitoreo

Programe sus sistemas para que detecten y erradiquen amenazas.

Manejo de Incidentes

Establezca un protocolo para el manejo de incidentes de seguridad.

Colaborar con una cadena de seguridad

Colabore con sus proveedores y amigos.

www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq

Vectores de Ataque

33%

Servicios Cloud

32%

Insiders

Con o sin intención

19%

Software Malicioso

Para todo tipo de dispositivos

16%

Fuerza Bruta

Obtención de contraseñas

URIBE · YÁÑEZ

Vectores de ataque más utilizados por los ciberdelincuentes

1 **Ataques dirigidos**
Phishing - MSM

2 **Navegación Web**
Drive-by download
Browser in the browser

3 **Endpoints**
Terminales – IoT - Teletrabajo

4 **Aplicaciones web**
Portales corporativos - Intranet

5 **Software**
Mal Configurado, desactualizado, no parcheado

6 **Credenciales**
Fuga de datos o ingeniería social

6 **Credenciales/Contraseñas**
Predecibles, por defecto, filtradas

7 **Insiders**
Personal con acceso insatisfecho o accidental

8 **Carencia de cifrado**
Débil, sin políticas, protocolos obsoletos

9 **Cadena de suministro**

Tomado de : https://cutt.ly/RMIK

Vectores de ataque

La mayor cantidad de delitos informáticos que se realiza por parte de delincuentes a través de técnicas básicas buscan por parte de la víctima que ella realice estas tres acciones principales:

Link´s

Apertura de enlaces engañosos que llevan a los siguientes puntos.

Visitar páginas falsas o con contenido de descarga que puede comprometer la información y/o los dispositivos del usuario.

Malware

Descargar aplicaciones maliciosas.

Contraseña y correo electrónico

Ejercicio practico

1

¿Qué tan segura es mi contraseña?

http://www.security.org/how-secure-is-my-password/

2

¿Me han engañado? compruebe si su dirección de correo electrónico ha sido victima de una fuga de datos

http://haveibeenpwed.com/

URIBE · YÁÑEZ

2

TIPOS DE MALWARES

Malware: Definición y Tipos

¿Qué es un Malware?

El malware, o software malicioso, es un programa o aplicación que se instala en un dispositivo sin el consentimiento del usuario y que tiene como objetivo dañar el sistema o robar información.

"Programa informático o virus específicamente diseñado para perturbar o dañar un sistema" (Fundéu).

- Es incorrecto llamar virus a un malware (o programa malicioso). El virus es solo un tipo de malware.
- Está diseñado para dañar, alterar, robar información o tomar el control de un sistema informático sin el consentimiento del usuario.

Purtilo, J. (2017). Cyber Ethics 4.0).

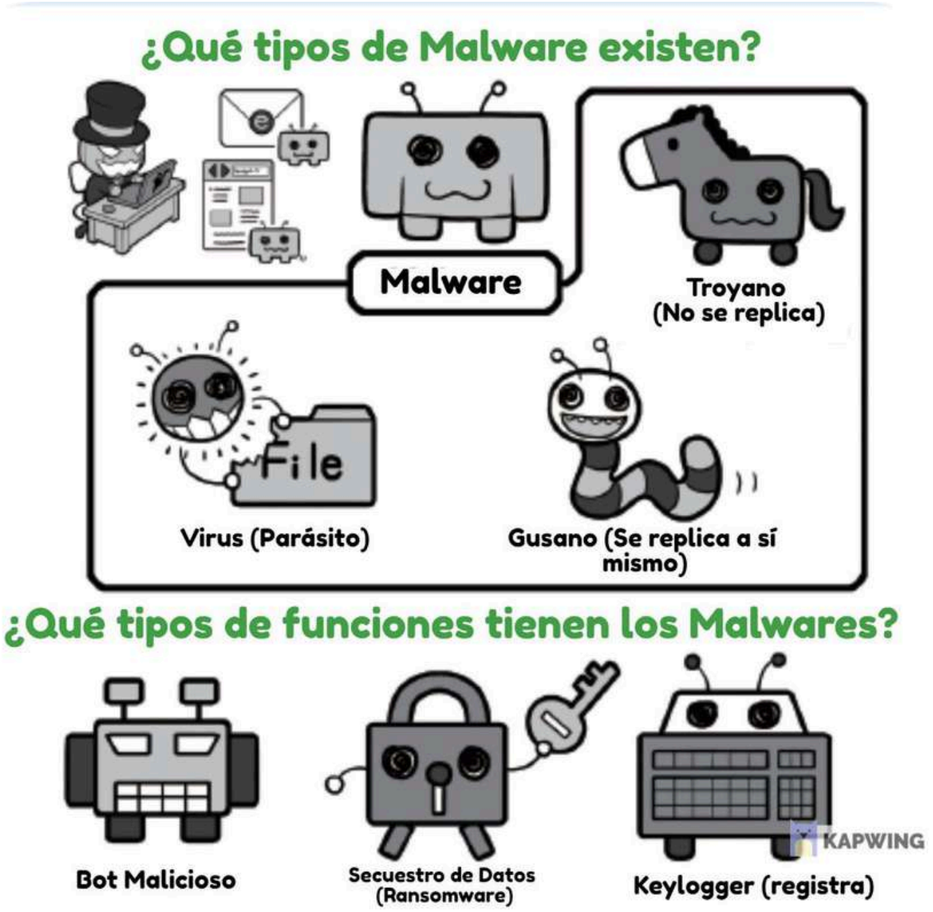


Imagen adaptada al español. Tomado de NISC

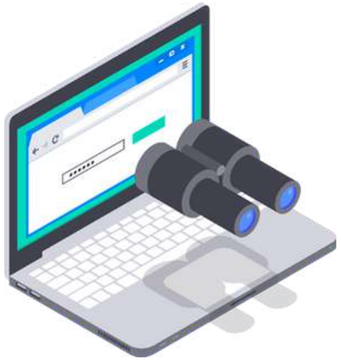
URIBE · YÁÑEZ

Tipos de Malwares

Virus

Gusano (Duplicar)

Troyano



Spyware

Adware

Ransomware

URIBE · YÁÑEZ

Ransomwares (Secuestro/Extorción)

Tomado de Incibe

Tomado de WeLiveSecurity

URIBE · YÁÑEZ

Botnet

¿Qué es?

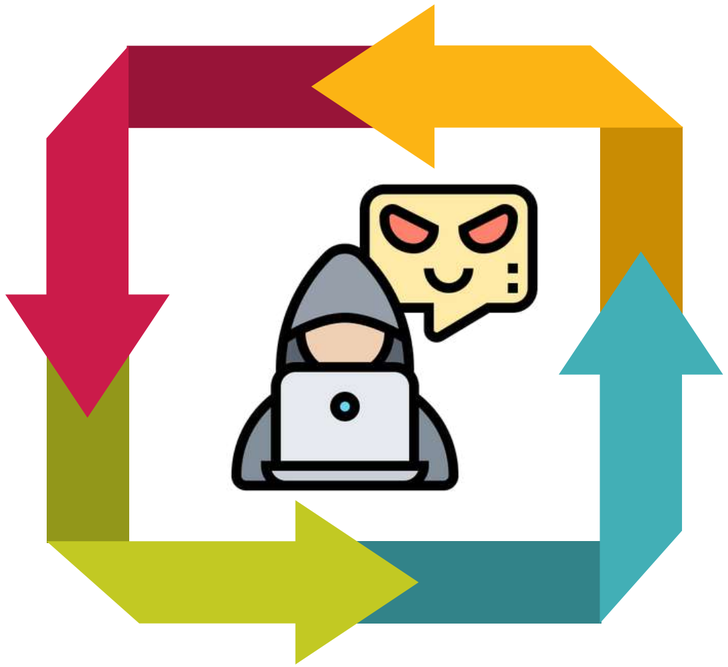
1

"Red de equipos infectados con software malicioso que permite su control remoto, obligándoles a enviar spam, propagar virus o realizar ataques" (Avast).

Modus Operandi

2

El atacante introduce malwares dentro de archivos "inofensivos", para luego poseer el control del equipo.



Ataque DDOS

3

Ataque distribuido de denegación de servicio. Múltiples dispositivos atacan un servidor para incapacitarlo.

¿Cuál es el Peligro?

4

Ralentizan el funcionamiento de nuestro dispositivo, así como amenazan contra servicios que usamos.

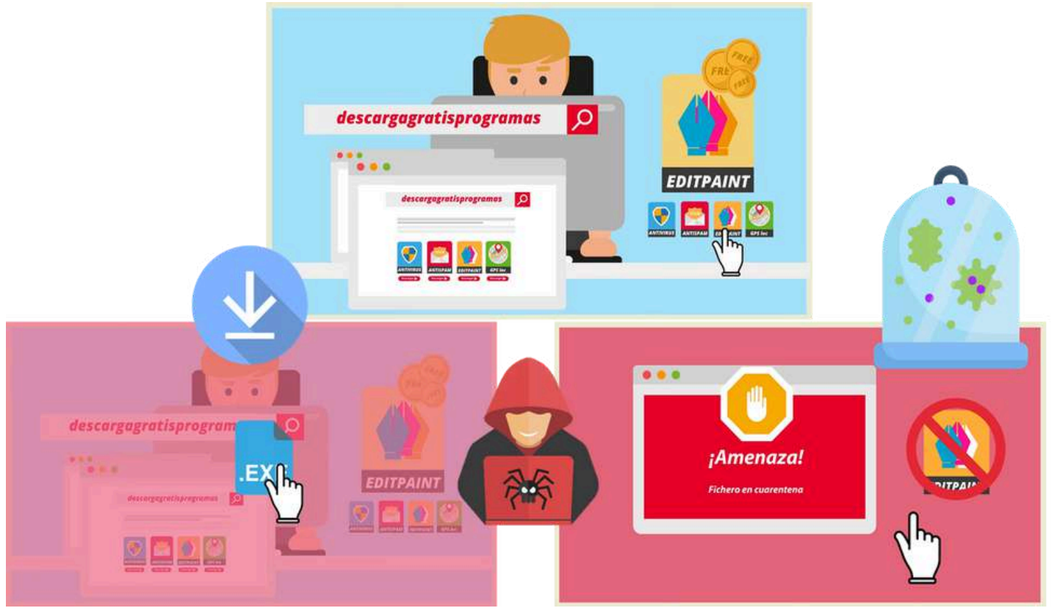
URIBE · YÁÑEZ

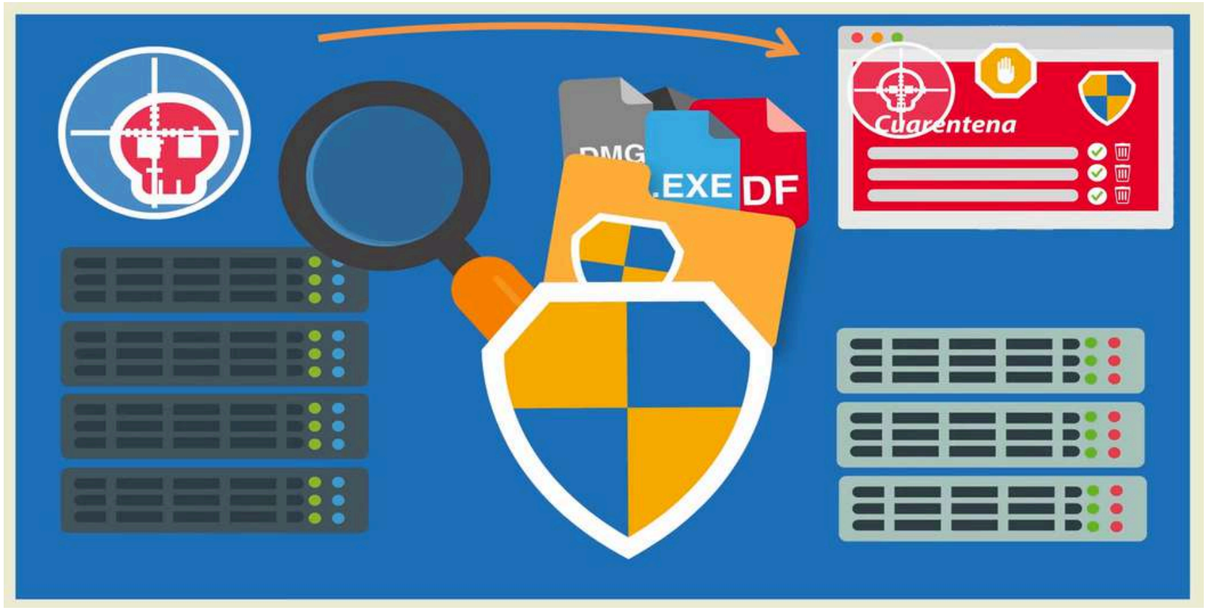
POSIBLES SOLUCIONES

¿Qué es un Antimalware?

Es la herramienta principal con la que contamos para defendernos de una gran variedad de amenazas. Su función principal es detectar y eliminar virus, troyanos y otras clases de malware, evitando el robo de información y protegiéndonos de todo tipo de amenazas que traten de ingresar a nuestro sistema

¿Cómo funciona un antimalware?



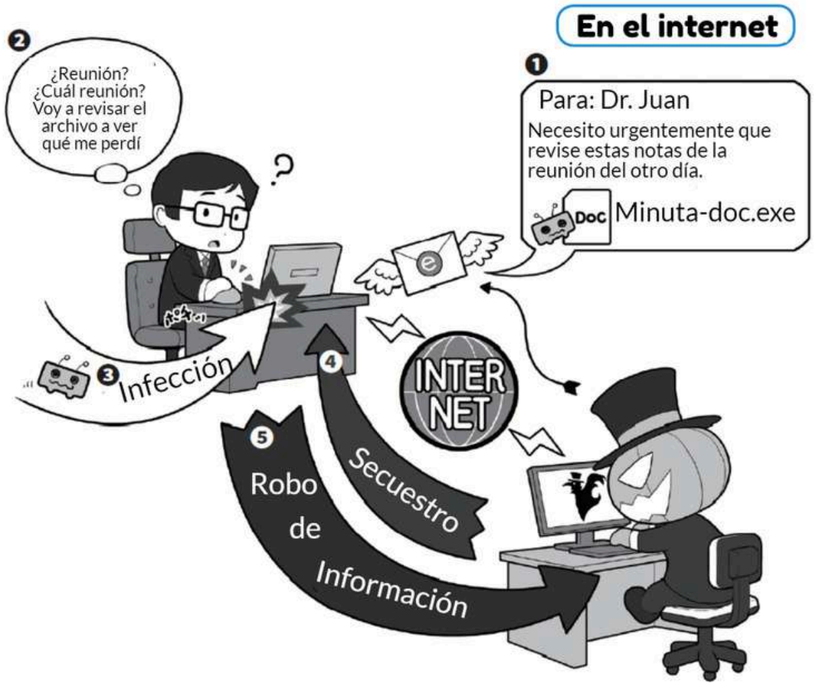


URIBE · YÁÑEZ

Agujeros Psicológicos de Seguridad en Nuestro Día a Día

Suplantación de Identidad

Netbots y Ramsomware



Ilustraciones tomadas de NISC

Infecciones y Agujeros de Seguridad

1. Agujero de Seguridad: “fallo de un programa que permite mediante su explotación violar la seguridad informática de un sistema” (Ecured).

2. Normalmente, los agujeros de seguridad de un software son solucionados con actualizaciones. Ej: Windows Update.

3. Agujero Psicológico de Seguridad: El atacante induce al usuario a darle acceso sin ninguna agresividad.

4. El ladrón crea un “ambiente” o software falso para hacer creer al usuario que es legítimo un link, archivo dato, etc.


Desde la cárcel llamaba a hacer estafa pero resultó lla...
Share
Watch on YouTube

Tap Here

URIBE · YÁÑEZ

3

PHISHING: ¿CÓMO DETECTARLO EN CORREOS ELECTRÓNICOS?

Phishing y Spear Phishing

Técnica que permite obtener credenciales de acceso (Usuario- Contraseña) a través del engaño visual, los sitios Web suplantados e ven muy similares a los originales.

Spear phishing, más personalizado, dirigido a organizaciones.

URIBE · YÁÑEZ

El Phishing a Través de Correo Electrónico

Tomado de Oficina de Seguridad del Internauta

1. Remitente: ¿Esperaba un email de esta persona/entidad?
2. Asunto: ¿Es llamativo el asunto del correo?
3. Objetivo del Correo: ¿Es un fin concreto o le están pidiendo ingresar a links o introducir sus datos personales?

URIBE · YÁÑEZ

El Phishing a Través de Correo Electrónico

Tomado de Oficina de Seguridad del Internauta

4 Ortografía: ¿Tiene errores ortográficos o parece una traducción de otro idioma mal hecha?

5 Enlaces: Si contiene enlaces, coloque el cursor sobre este y verá realmente a dónde lo dirige.

6 Adjuntos: Si contiene archivos no esperados, analizarlos con antivirus siempre será nuestro blindaje.

URIBE · YÁÑEZ

Ejemplos de Phishing

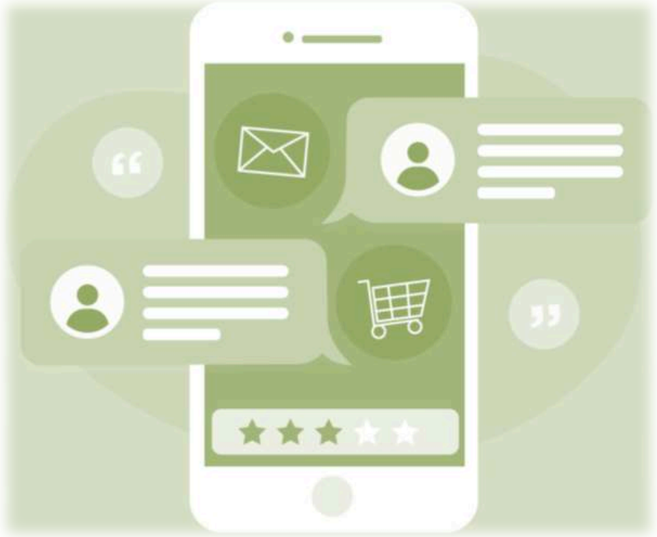
Tomado de GoDaddy ES

Tomado de Líder Empresarial

URIBE · YÁÑEZ

Smishing – Vishing / Engaño

Mensajes SMS / MSM / Voz



SPOOFING

Suplantación

Modalidad en la que personas malintencionadas suplantan a personas naturales o jurídicas para ejecutar acciones fraudulentas.

Estafas Online

Variantes de la estafa:

- Herencia
- Loterías
- Lazos afectivos
- Paquetes

URIBE · YÁÑEZ

BEC / SUPLANTACIÓN

Business Email Compromise

Fraude del CEO / ¿Como lo pueden engañar?
Envían un correo haciéndose pasar por uno de los directivos de su empresa.
Un empleado autorizado para realizar pagos es engañado para que pague una factura falsa o haga una transferencia no autorizada desde una cuenta de la compañía.

Ingeniería social
Insider
Phishing
Suplantación dominio correo
Malware
Transferencias electrónicas a entidades financieras en el extranjero

¿Cómo reconocer un mensaje tipo phishing en el correo electrónico?

¿Quién envía el correo? ¿es fiable o no?
Debes sospechar si el remitente es una dirección de correo desconocida o que no pertenece a una entidad oficial.

¿El contenido es sospechoso?
El objetivo es intentar asustarte para que actúes según las indicaciones del mensaje. Siempre añaden una excusa, como por ejemplo "problemas técnicos o de seguridad", y proporcionan una solución sencilla del tipo "accede utilizando este enlace". Además, es muy habitual que te soliciten nombre de usuario, claves y otros datos.

¿Pide hacer algo de manera urgente?
Con esta urgencia, los delincuentes intentan que tomes una decisión precipitada y caigas en la trampa, que incluye visitar un enlace e indicar datos personales y/o contraseñas.

¿A quién va dirigido el correo?
Si un ciberdelincuente quiere estafar a cientos de personas, es muy complicado saber el nombre de todas. Por ello, utilizan "Estimado cliente", "Hola", "Hola amigo", etc. Para evitar decir un nombre.

¿El enlace es fiable?
La intención de los ciberdelincuentes es que hagas clic en un enlace. En el texto del mensaje hay un enlace que en lugar de llevarte a la página web legítima, te lleva a otra fraudulenta que estéticamente es igual o muy parecida a la oficial.

URIBE · YÁÑEZ

4

CIBERSEGURIDAD EN LA PRÁCTICA

URIBE · YÁÑEZ

EXPAND-URL

ExpandURL

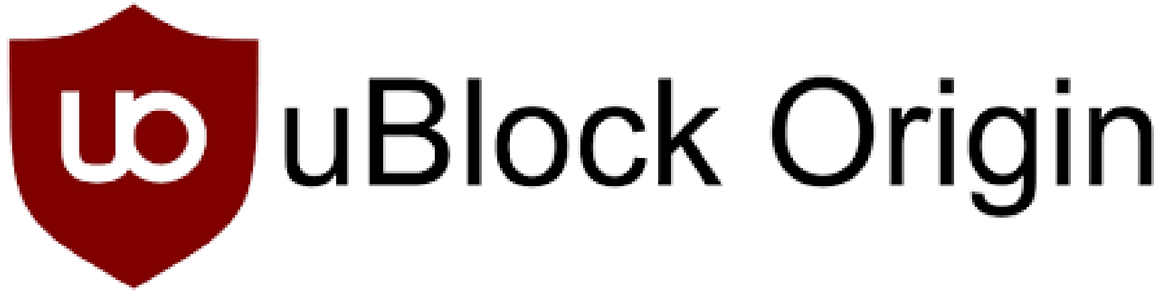
bitly

¿Qué hacer si me envían un enlace “recortado”?

EJEMPLO: https://bit.ly/3KvozRV

URIBE · YÁÑEZ

Extensiones para el Navegador



¿Cómo bloquear anuncios no deseados?

URIBE · YÁÑEZ

Tecnotips

Actualización de los equipos de cómputo

Recuerda que para garantizar el correcto funcionamiento de tu equipo y prevenir posibles intrusiones no autorizadas, **es necesario aplicar las actualizaciones del sistema operativo y reiniciar el equipo periódicamente.**

Para validar las actualizaciones, debes ir al menú de **"Configuración"**, haciendo clic en el botón de inicio y luego seleccionar **"Windows Update"**.

En la sección **"Configuración"**, selecciona el ícono de **"Actualización y seguridad".**

Valida que el equipo esté al día en actualizaciones; de lo contrario, realiza la instalación de las mismas.

Una vez realices las actualizaciones, **reinicia el equipo.**

Recuerda: puedes realizar estos pasos de manera remota en tu casa, en el campus o desde cualquier lugar.

Dirección de Tecnología y Transformación Digital
Contáctanos en: service.desk@unisabana.edu.co
(601) 861 5555 / 861 6666 - ext. 34444

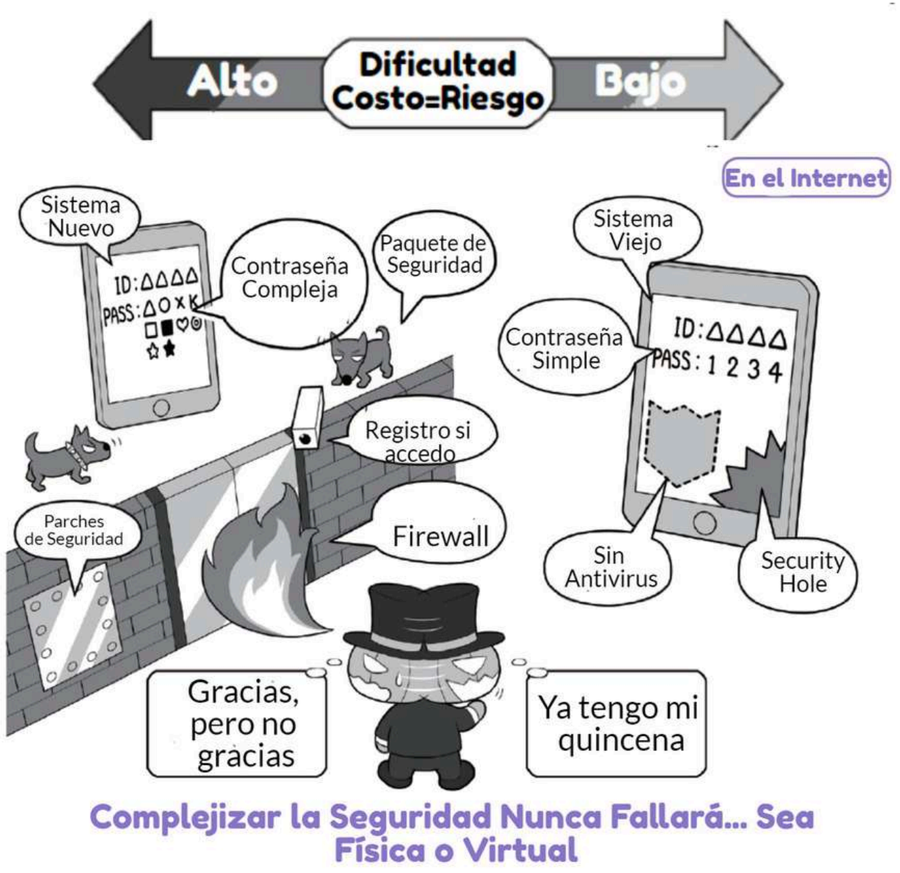
Universidad de La Sabana

URIBE · YÁÑEZ

5

SEGURIDAD: MECANISMO PARA DETENER A CIBERATACANTES

¿Es Ventajoso Estar Seguro de mi Protección Cibernética?



Adaptación a partir de NISC

Ciberataques por Falencias Propias

- No actualizar nuestra clave.
- Usar la misma clave para todas las cuentas.
- No actualizar el firmware de nuestro equipo.
- Evitar el uso de softwares por “pereza” o no tener el conocimiento suficiente.

URIBE · YÁÑEZ

Mecanismos

- Capacitaciones.
- Perfiles de acceso y manejado de la información.
- Respaldo periódico.
- Actualizar software y firmware.
- Cierre de sesión de los equipos.
- Cierre físico de las oficinas.
- Durante el mantenimiento de los sistemas.
- Al cambiar un sistema.
- Controlar a los terceros que se les entrega información.
- Contraseña segura
- Doble Factor de Autenticación

URIBE · YÁÑEZ

Navegación en Modo Incógnito

El modo incógnito es una función de privacidad en línea que crea una sesión paralela y temporal en el navegador y está aislada de los datos y sesión principal del usuario.

1. **Borrar cookies**
2. **No almacena el historial**
3. **Múltiples sesiones**

Contraseñas

Configuración / Creación

TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

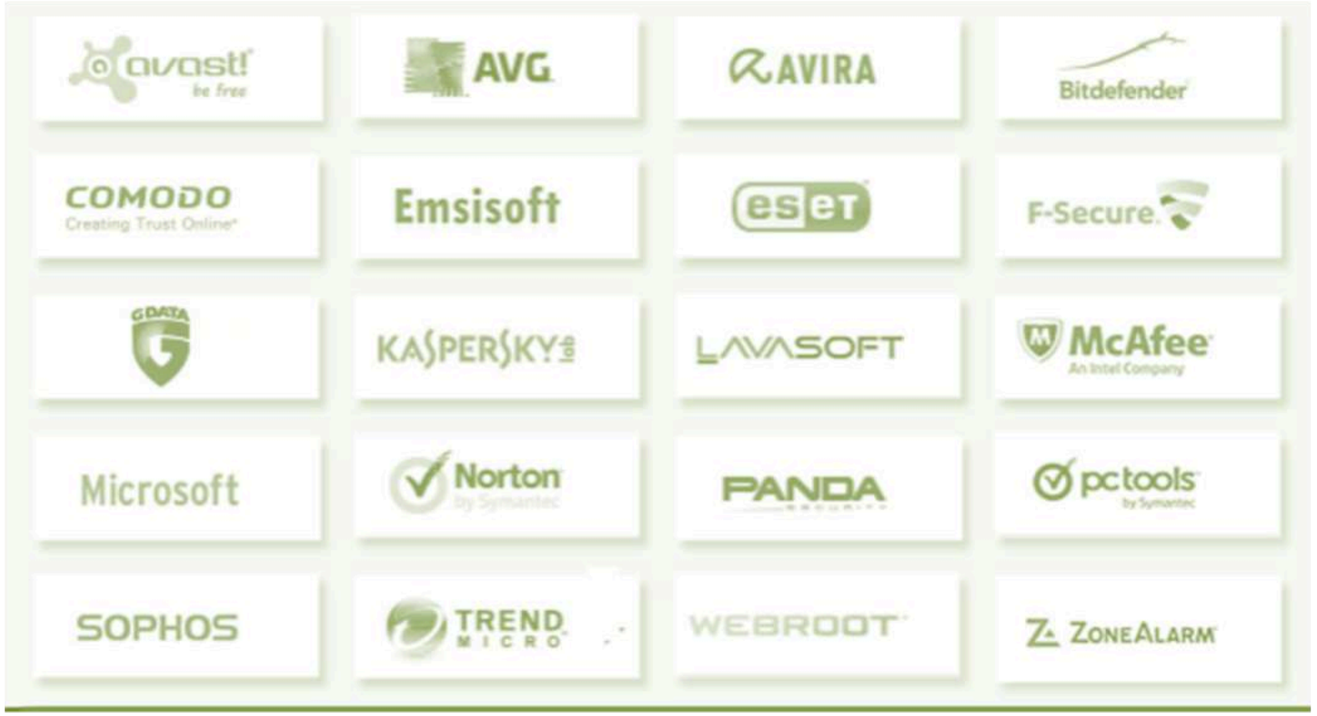
HIVE SYSTEMS

Cybersecurity that's approachable.
Find out more at hivesystems.io

Las contraseñas que tienen entre 4 y 7 caracteres son las más débiles, no son muy recomendables de utilizar.

- Morado: para aquellas contraseñas que se pueden obtener de forma instantánea.
- Rojo: para las password que se descifran en unos pocos segundos hasta unas cuantas horas sin sobrepasar un día.
- Naranja oscuro: se necesitaría un tiempo desde los 3 días hasta los 5 años para poder crackearlas.
- Naranja claro: para las que tardaríamos desde un año a mil años para que se averiguara nuestra contraseña.
- Verde: sin duda son las más complejas y robustas, se tardarían en descifrar más de mil años.

Instalación de aplicaciones



Se deben instalar las aplicaciones que sean necesarias y sólo aquellas que gocen de buena reputación o puntaje. Entre más aplicaciones se instalen más vulnerable es un sistema, asimismo hay que tener en cuenta que los delincuentes crean APPS (aplicaciones) maliciosas para infectar los equipos móviles.

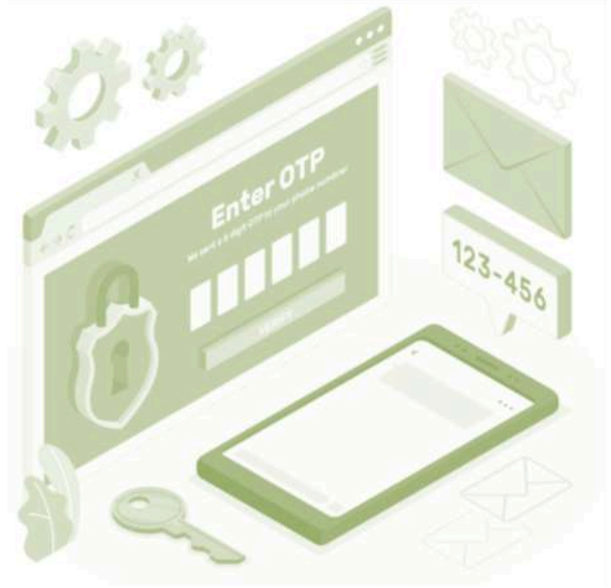
Backup – Respaldo

La Regla 3-2-1 recomienda que debe haber al menos tres copias de datos importantes, en al menos dos tipos de medios diferentes, con al menos una de estas copias en un almacenamiento externo (offsite). La Regla 3-2-1 no exige o requiere ningún tipo de hardware en especial y es lo suficientemente versátil como para abordar casi cualquier escenario de fallo.

URIBE · YÁÑEZ

Doble Factor o Múltiple Factor de Autenticación

2FA / MFA



Los autenticadores y los tokens abarcan cuatro categorías principales: algo que tienes, algo que sabes, algo que eres o donde estás.

Algo que tienes: Una tarjeta de acceso física, un teléfono inteligente u otro dispositivo o un certificado digital

Algo que sabes: Un código PIN o una contraseña

Algo que eres: Datos biométricos, como huellas dactilares o escáneres de retina

URIBE · YÁÑEZ

PASO A PASO PARA ACTIVAR EL FACTOR MÚLTIPLE DE AUTENTICACIÓN

UNA DE LAS MEJORES MANERAS DE MANTENER TUS CUENTAS A SALVO

www.uribeyanez.com

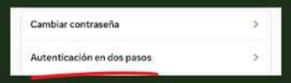
INSTAGRAM

1 Ve a tu perfil y toca el **menú de tres líneas.**

2 Selecciona **"Centro de cuentas".**

3 Toca **"Contraseña y seguridad".**

4 Selecciona **"Autenticación en dos pasos"** y sigue las instrucciones.



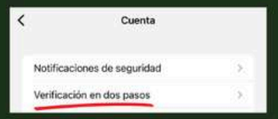
www.uribeyanez.com

WHATSAPP

1 Abre WhatsApp y ve a **"Configuración"**

2 Selecciona **"Cuenta".**

3 Toca **"Verificación en dos pasos"** y activa la función **e ingresa un PIN de seis dígitos y un correo electrónico de recuperación.**

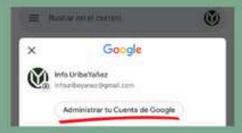


www.uribeyanez.com

GMAIL

1 Selecciona **tu cuenta** en la parte superior izquierda.

2 Toca **"Administrar tu cuenta de Google ".**



3 Toca **"Seguridad".**

4 Selecciona **"Autenticación en dos pasos"** y sigue las instrucciones.

Una contraseña fuerte es el primer paso, pero el MFA es tu mejor escudo contra ciberataques

URIBE · YÁÑEZ

6

ADOPCIÓN DEL MODELO DE SEGURIDAD CONFIANZA CERO:

INTRODUCCIÓN

El Modelo Zero Trust, en adelante ZT, o de confianza cero, parte de la premisa de que cada conexión y punto final se consideran una amenaza.

El modelo ZT cambió radicalmente el enfoque tradicional de seguridad al pasar de "confiar, pero verificar" a **"nunca confiar y siempre verificar**".

El principio base del modelo es el del mínimo privilegio, en el que los usuarios tienen acceso únicamente a lo que es esencial para realizar su trabajo.

Premisas del modelo:

✓ Autenticación y autorización continua.

✓ Confidencialidad y protección de los datos

Tomado de PUJ Diana Baquero et al.

URIBE · YÁÑEZ

Historia del Modelo

Arquitectura de Seguridad Tradicional

Perímetros estáticos de red

Foro de Jericó - 2004
Desperimetralización

David Lacey del Royal Mail y un grupo de CISO's a nivel mundial

DISA y Dpto defensa EEUU
SDP Group – Iniciativa Núcleo Negro

John Kindervag, 2010
Creó el modelo mientras trabajaba como analista principal en Forrester Research

HOY

Usuarios, activos y recursos
APIs

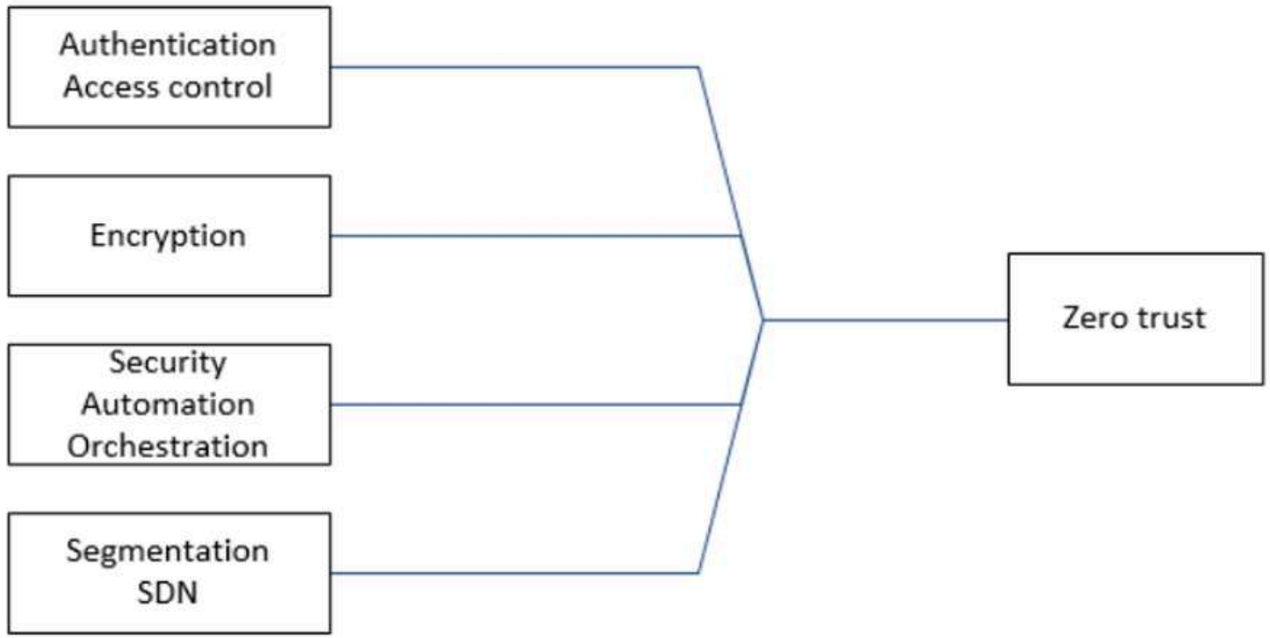
Tomado de PUJ Diana Baquero et al.


La señorial reacción de Federer al no poder entrar en vestuarios por olvidarse la acredi...
Copy link
Watch on YouTube

Tap Here

Características mínimas

Las características mínimas con las que debe contar una arquitectura Zero trust están regidas bajo la premisa de la noción en la que ningún usuario o dispositivo es considerado confiable, por lo que su implementación será a través de una postura del menor privilegio.



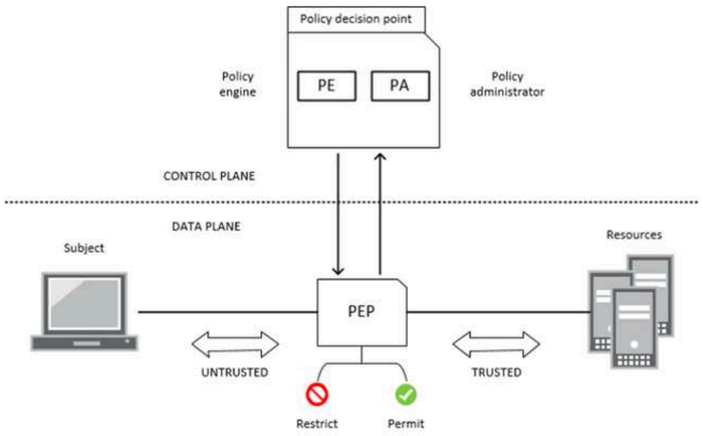
Naeem Firdous Syed, Syed W. Shah, Arash Shaghaghi, Anan Anwar, Zubair Baig, Robin Doss: Zero Trust Architecture (ZTA): A Comprehensive Survey. 2022 (P2)

Tomado de PUJ Diana Baquero et al.

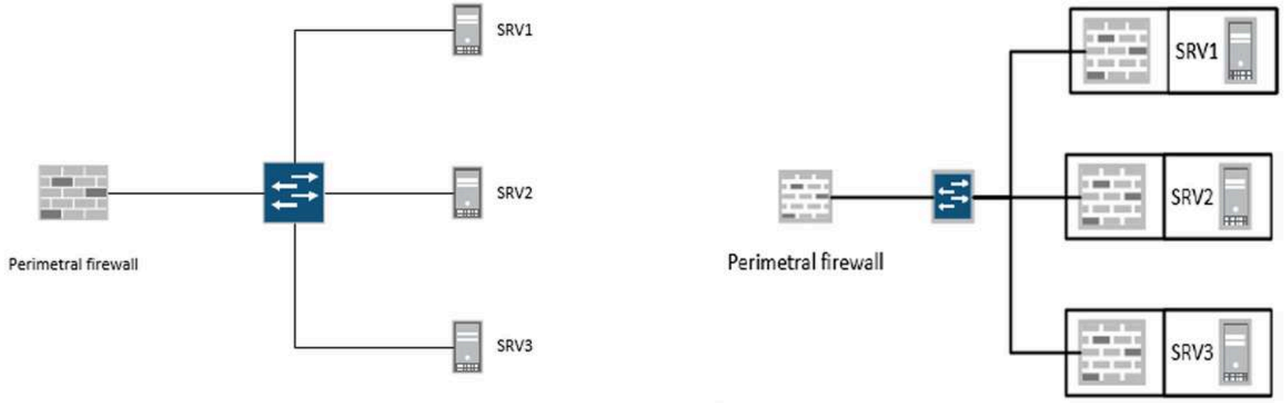
Representación lógica de infraestructura ZT

Modelo para la representación lógica de una infraestructura ZTA e insumos de decisión para el algortimo de confianza.

Diferencias de un aprovisionamiento de una infraestructura LAN tradicional vs LAN ZTA con la implementación de la microsegmentación (nativa, third-party u overlay) como mecanismo para prevenir movimientos laterales.



Naeem Firdous Syed, Syed W. Shah, Arash Shaghaghi, Anan Anwar, Zubair Baig, Robin Doss: Zero Trust Architecture (ZTA): A Comprehensive Survey. 2022 (P4)

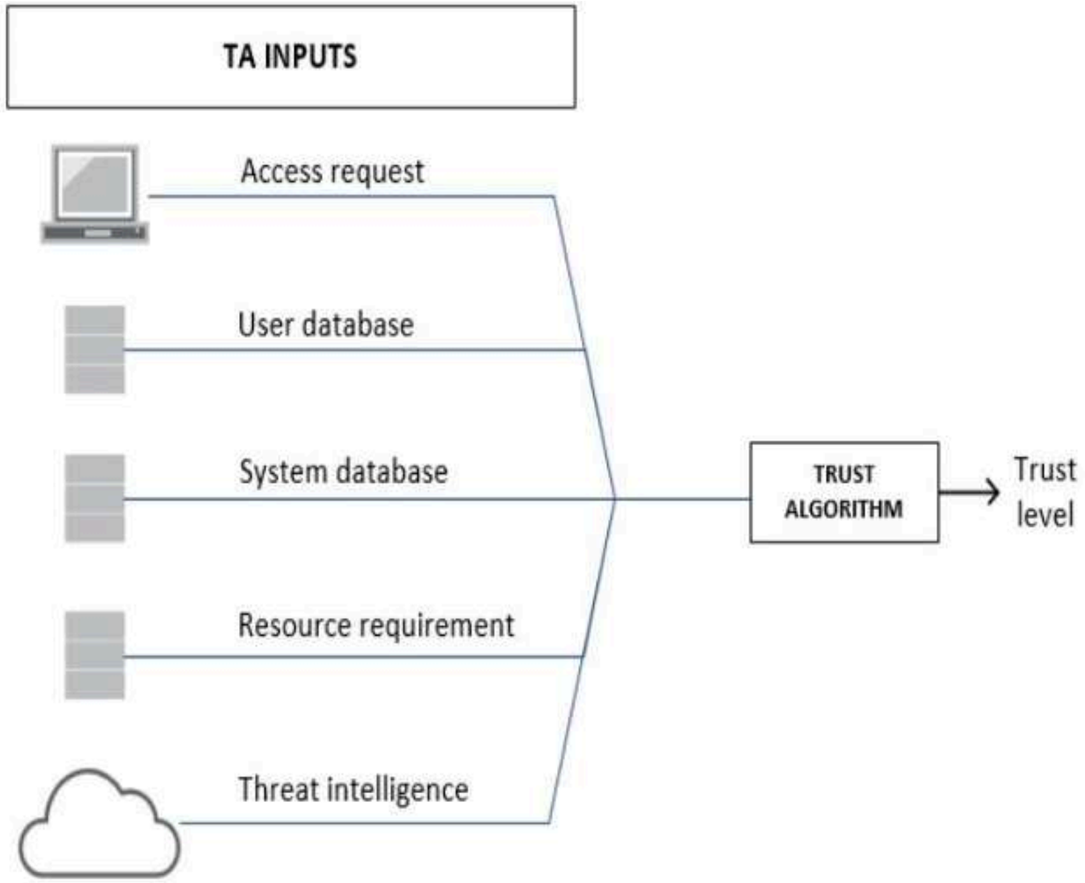


Naeem Firdous Syed, Syed W. Shah, Arash Shaghaghi, Anan Anwar, Zubair Baig, Robin Doss: Zero Trust Architecture (ZTA): A Comprehensive Survey. 2022 (P20)

Tomado de PUJ Diana Baquero et al.

URIBE · YÁÑEZ

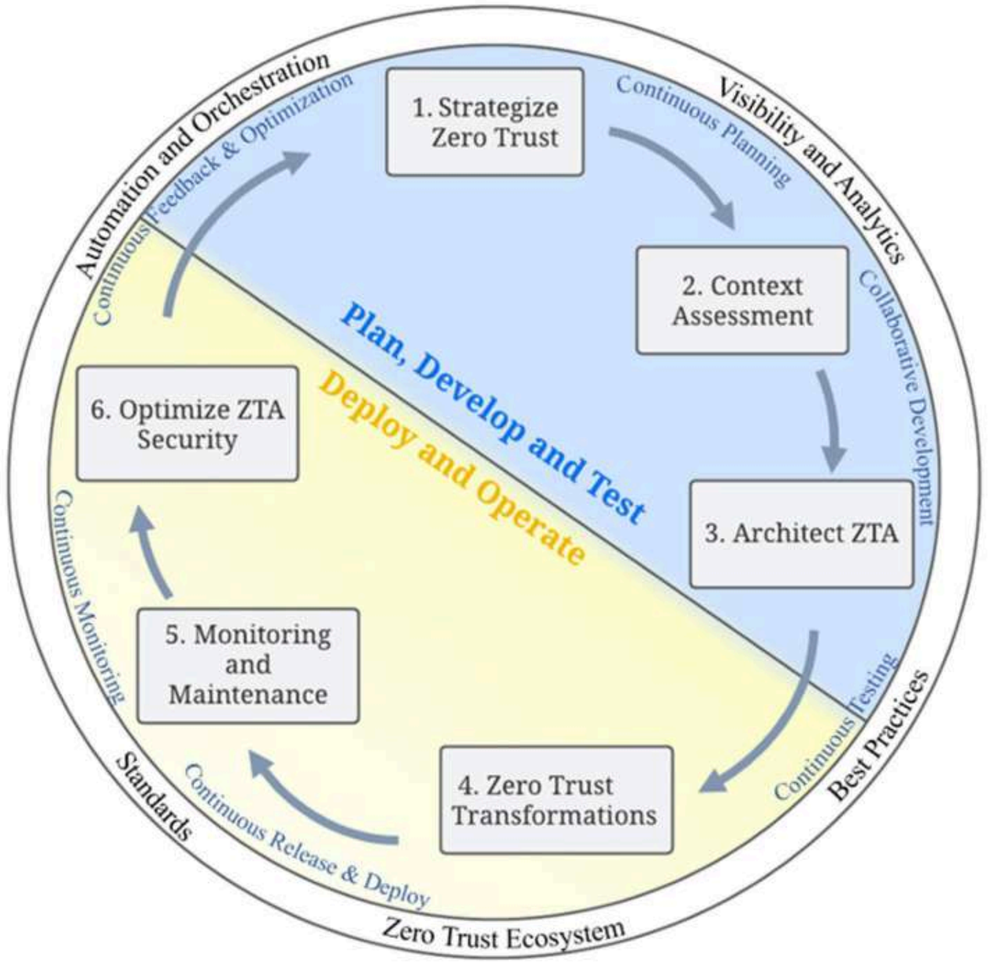
Representación lógica de infraestructura ZT



Naeem Firdous Syed, Syed W. Shah, Arash Shaghaghi, Anan Anwar, Zubair Baig, Robin Doss: Zero Trust Architecture (ZTA): A Comprehensive Survey. 2022 (P5)

Tomado de PUJ Diana Baquero et al.

¿CÓMO IMPLEMENTAR ZERO TRUST?



Framework para la migración a una arquitectura ZT (Tomado de: Phiayura & Songpon, 2023).

URIBE · YÁÑEZ

PERSPECTIVA LEGAL DE LA CIBERSEGURIDAD

URIBE · YÁÑEZ

INFORMACIÓN PRIVILEGIADA:

¿QUÉ TENER EN CUENTA?

¿CÓMO SE CLASIFICA LA INFORMACIÓN?

Tiempo

Transparencia

Totalidad

Tipo

¿QUÉ CONSECUENCIAS NEGATIVAS TRAE COMPARTIR INFORMACIÓN PRIVILEGIADA?

- Daños reputacionales.
- Órdenes de autoridades administrativas.
- Multas (Personas Jurídicas y Personas Naturales).
- Penas privativas de la libertad.
- **El estrés, la salud, el sueño.**

URIBE · YÁÑEZ

7 PROPIEDAD INDUSTRIAL

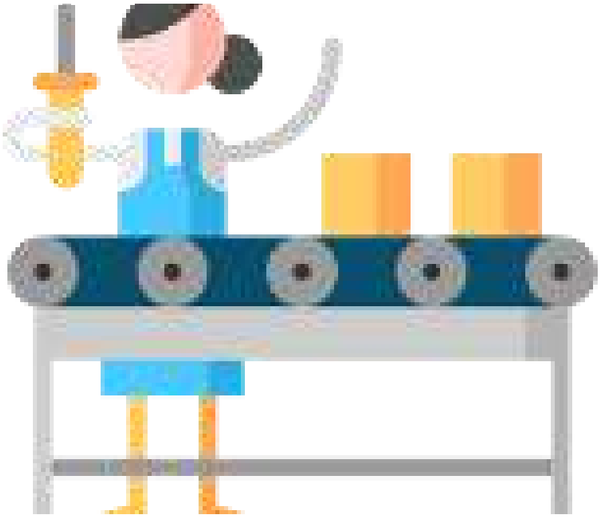
¿QUÉ INFORMACIÓN SE PROTEGE COMO SECRETO EMPRESARIAL?

Art. 260 Decisión 486: Cualquier información no divulgada que una persona natural o jurídica legítimamente posea, que pueda usarse en alguna actividad productiva, industrial o comercial, y que sea susceptible de transmitirse a un tercero, en la medida que dicha información:

- Sea secreta.
- Tenga valor comercial por ser secreta.
- Sea objeto de medidas razonables destinadas a mantenerla secreta.

¿QUÉ INFORMACIÓN SE CONSIDERA “SECRETO EMPRESARIAL”?

Producto o servicio



Métodos o procesos de producción.

Distribución o comercialización

RÉGIMEN MARCARIO

Artículo 134. Decisión 486. (...) constituirá marca cualquier signo que sea apto para distinguir productos o servicios en el mercado. Podrán registrarse como marcas los signos susceptibles de representación gráfica. La naturaleza del producto o servicio al cual se ha de aplicar una marca en ningún caso será obstáculo para su registro.

¿Será posible registrar dominios de internet como “marca”?

https://sipi.sic.gov.co/sipi/Extra/IP/TM/Qbe.aspx?sid=638427434682585088

05129937	317844	WWW.ALFAINMO.COM		18 jul. 2026	Registrada	INMOBILIARIA DE ADMINISTRADORES ALFA, S.A.	36	561
06006521	321429	WWW.SUMANDOOPORTUNIDADES.COM		10 ago. 2026	Registrada	BANCO DAVIVIENDA S.A.	38	561
06015449	321876	WWW.INDUSS.NET		08 sept. 2016	Caducado	INDUSS NET LTDA	35	562
06015708		WWW. CONSTITUCIONALDIA.COM			Negada	CHARRY MOSQUERA ASOCIADOS & CIA. LTDA ABOGADOS	42	562
06037022	323428	WWW.GRUPOAVAL.COM		14 nov. 2026	Registrada	GRUPO AVAL ACCIONES Y VALORES S.A.	36	564
06037025	323427	WWW.GRUPOAVAL.COM		14 nov. 2026	Registrada	GRUPO AVAL ACCIONES Y VALORES S.A.	35	564
06110940		WWW.CO			Negada	MAURICIO PINZÓN PINZÓN	38	570
06112812	343013	WWW.IT		24 oct. 2017	Caducado	VALTER DAL CORTILE	25	579
06115480	337564	WWW.UNILAGO.COM.CO		26 jun. 2017	Caducado	CENTRO COMERCIAL UNILAGO	35	575
06124177	336045	WWW.CHUBB-CARGA.COM		28 jun. 2027	Registrada	CHUBB INA HOLDINGS INC.	38	572

URIBE Y YÁÑEZ

8 COMPETENCIA DESLEAL

URIBE · YÁÑEZ

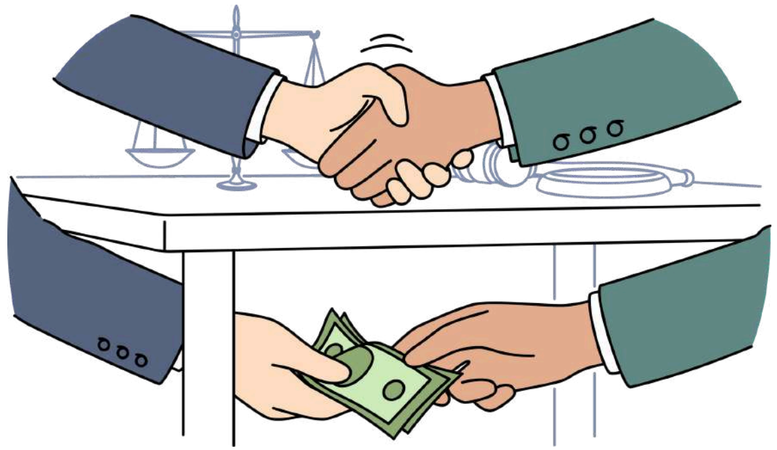
POSIBLES CONDUCTAS

- Violación de secretos empresariales.
- Prohibición general (Art 1 Ley 155/59)
- Desviación de clientela.
- Desorganización.
- Imitación.

URIBE · YÁÑEZ

CONSECUENCIAS

- Investigaciones/Multas.
- Demandas/condenas.
- **Estrés, pérdida de sueño.**



URIBE Y YÁÑEZ

9

PRÁCTICAS RESTRICTIVAS DE LA COMPETENCIA

POSIBLES CONDUCTAS

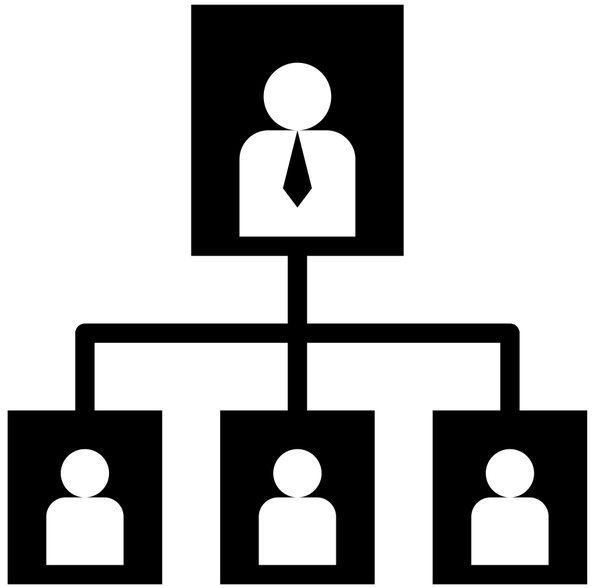
- Infracción de la cláusula de prohibición general (Art. 1 Ley 155 de 1959).
- Abuso de posición dominante.

URIBE Y YÁÑEZ

10

ÁMBITO CORPORATIVO

¿QUIÉNES HACEN PARTE?



- Gerente.
- Miembro de junta directiva.
- Asesor.
- Empleado.

¿POR QUÉ SON IMPORTANTES?

Tienen acceso a información privilegiada o constitutiva de secreto empresarial de la compañía.

URIBE Y YÁÑEZ

11 ÁMBITO BURSÁTIL

¿QUÉ INFORMACIÓN SE CONSIDERA PRIVILEGIADA?

- Información de carácter concreto.
- No conocida por el público.
- La habría tenido en cuenta un inversionista medianamente diligente y prudente al negociar los respectivos valores.

URIBE · YÁÑEZ

12 DATOS PERSONALES

URIBE · YÁÑEZ

TRATAMIENTO DE LOS DATOS PERSONALES

- Principio de responsabilidad demostrada. (carga de diligencia)

URIBE · YÁÑEZ

13 CONTRATOS

CONTRATOS O RELACIONES EN LAS QUE HAY ENTREGA DE INFORMACIÓN

- Servicios TICs.
- Servicios de nube .
- Desarrollo de software.
- Bases de datos.
- Maquilas.
- Concursos.
- Empleados.
- Administradores.
- Miembros de junta.
- M&A.

CLÁUSULAS O CONTRATOS QUE DEBEN FIRMARSE

- Cláusula de confidencialidad.
- NDA.
- Cláusula penal en caso de incumplimiento.
- Obligación de tener estándares de seguridad.
- obligación de borrado seguro

URIBE · YÁÑEZ

14 LABORAL

FALTA GRAVE

Artículo 58 Código Sustantivo de Trabajo

En virtud de lo establecido en el Código Sustantivo de Trabajo, respecto del manejo de información, es obligación del trabajador (salvo autorización expresa y los casos establecidos en la ley) mantener la confidencialidad de la información a la que tenga en acceso en el desempeño de su puesto de trabajo.

URIBE · YÁÑEZ

FALTA GRAVE

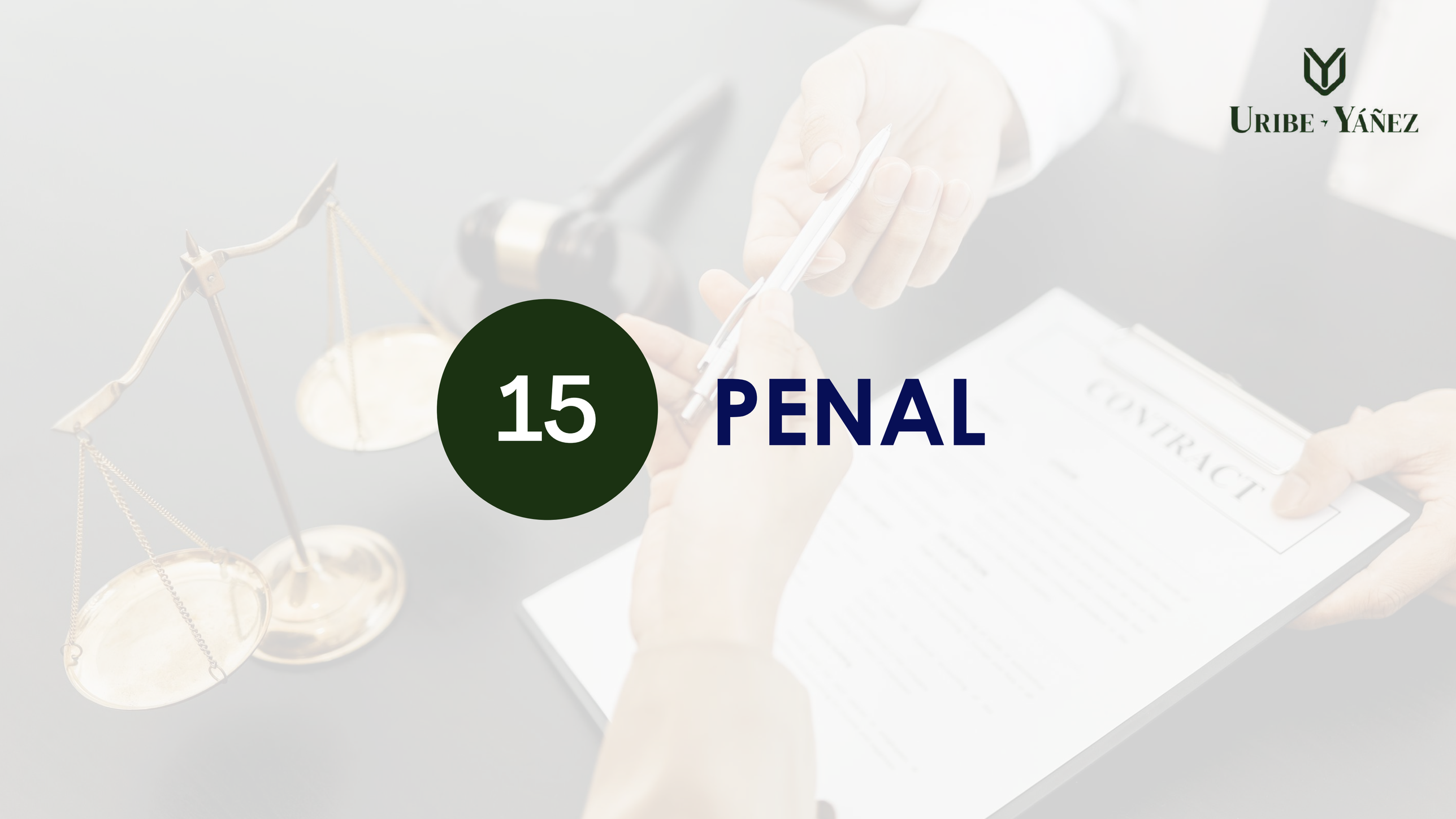
Artículo 62 Código Sustantivo de Trabajo

Asimismo, será falta grave y justa causa de terminación unilateral del contrato de trabajo revelar información de carácter reservado o confidencial a terceros que pueda causar perjuicios al empleador.

Es prudente estipularse:

- En el Reglamento Interno de Trabajo.
- Como obligación del trabajador, en el contrato de trabajo.

URIBE · YÁÑEZ



15 PENAL

VIOLACIÓN DE RESERVA INDUSTRIAL O COMERCIAL

ARTÍCULO 308 CÓDIGO PENAL.

El que emplee, revele o divulgue descubrimiento, invención científica, proceso o aplicación industrial o comercial, llegados a su conocimiento por razón de su cargo, oficio o profesión y que deban permanecer en reserva...

URIBE · YÁÑEZ

UTILIZACIÓN INDEBIDA DE INFORMACIÓN PRIVILEGIADA

ARTÍCULO 258 CÓDIGO PENAL.

El que como empleado, asesor, directivo o miembro de una junta u órgano de administración de cualquier entidad privada con el fin de obtener provecho para sí o para un tercero, haga uso indebido de información que haya conocido por razón o con ocasión de su cargo o función y que no sea objeto de conocimiento público...

LEY 1273 DE 2009

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

URIBE · YÁÑEZ

ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO

ARTÍCULO 269A CÓDIGO PENAL:

El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo...

GESTIÓN DE INCIDENTES DE SEGURIDAD EN EL TRATAMIENTO DE DATOS PERSONALES

Cartilla Superintendencia de Industria y Comercio (2020)

URIBE · YÁÑEZ

URIBE Y YÁÑEZ

16

PRINCIPIO Y DEBER DE SEGURIDAD

DEBERES DE LOS RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO DE DATOS

Gráfico tomado de Superintendencia de Industria y Comercio, basado en la Ley 1581, art. 17, lit. d), y art. 18, lit. b)

Gráfico tomado de Superintendencia de Industria y Comercio, basado en la Ley 1581, art. 17 , lit. n), y art. 18, lit. k)

PASOS PARA LA GESTIÓN DE PREVENTIVA DE INCIDENTES

Gráfico tomado de Superintendencia de Industria y Comercio.

URIBE Y YÁÑEZ

17

MARCO NORMATIVO PARA EL REPORTE DE INCIDENTES DE SEGURIDAD

LEY 1581 DE 2012 Y DEBERES DE LOS RESPONSABLES Y LOS ENCARGADOS DEL TRATAMIENTO DE LOS DATOS

1. Artículo 17: "Deberes de los Responsables del Tratamiento"

"n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridady existan riesgos en la administración de la información de los Titulares." (Ley 1581-2012)

2. Artículo 18: "Deberes de los Encargados del Tratamiento"

"k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares; (…)" (Ley 1581-2012)

INSCRIPCIÓN DE INCIDENTES DE SEGURIDAD AL REGISTRO NACIONAL DE BASES DE DATOS (RNBD)

¿Qué es el RNBD?

Directorio público de las bases de datos sujetas a tratamiento que operan en el país. Es administrado por la SIC y es de libre consulta.

¿Quiénes deben registrarse ante la RNBD?

"Los Responsables del tratamiento, sociedades y entidades sin *ánimo de lucro que tengan activos totales superiores a 100.000 Unidades de Valor Tributario (UVT)(Art. 868, Estatuto Tributario) y personas jurídicas de naturaleza pública". (Circular Única de la* SIC).

REGISTRO NACIONAL DE BASES DE DATOS

RNBD

CIRCULAR ÚNICA DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO: CAPÍTULO II, TÍTULO V

¿QUIÉNES DEBEN REPORTAR UN INCIDENTE ANTE LA RNBD?

DEBEN REPORTAR LOS INCIDENTES

A más tardar dentro los 15 días hábiles siguientes al momento en que se detecten.

Todos los reportes se deben hacer a través del enlace previsto en la página web de la SIC.

Todos los reportes se deben hacer a través del enlace previsto en la página web de la SIC.

Los detalles de la información que se debe suministrar se encuentran en el "**Manual de Ayuda del Registro Nacional de Bases de Datos**".

Gráfico tomado de Superintendencia de Industria y Comercio

CIRCULAR ÚNICA DE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO: CAPÍTULO II, TÍTULO V

URIBE Y YÁÑEZ

18

ENCARGADOS DEL TRATAMIENTO E INCIDENTES

CLÁUSULAS EN EL CONTRATO DE TRANSMISIÓN

Recuerde que:

Si su organización es la Responsable del Tratamiento y contrata a un tercero como Encargado del Tratamiento, Usted debe exigir el cumplimiento de su Política de Tratamiento de datos al tercero contratado.

Si llega a haber una falta, es su empresa la que responde por negligencia ante la autoridad y el titular de los datos.

URIBE Y YÁÑEZ

19

CONSERVACIÓN DE REGISTROS DOCUMENTALES

REGISTROS DOCUMENTALES

Para prever futuros incidentes de seguridad, es fundamental establecer un registro interno de cada falencia presentada, con la finalidad de:

1.“Demostrar el cumplimiento del régimen de protección de Datos Personales en caso de una investigación” (SIC, 2020).

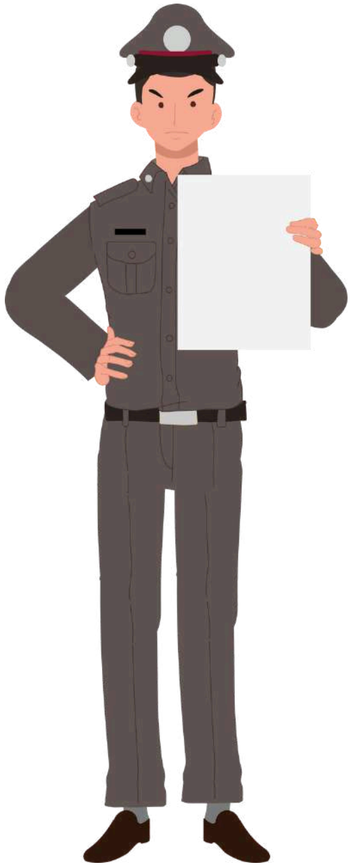
2. Crea alertas para anticiparse a incidentes del mismo tipo.

Los registros deben contener:

a) Suficientes detalles para que la autoridad determine si se dio una respuesta competente.
b) Un sistema de seguridad para su protección de vulneraciones.
c) Debe tener un plazo de conservación.
d) Originalidad e integridad de la prueba técnica.

CONSECUENCIAS DE VULNERAR LA NORMATIVA

- Investigaciones/Multas.
- Demandas/condenas.
- **Estrés, pérdida de sueño**.



URIBE Y YÁÑEZ

20

PROTOCOLO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD

URIBE · YÁÑEZ

¿QUÉ ES UN PROTOCOLO DE RESPUESTA EN EL MANEJO DE INCIDENTES DE SEGURIDAD?

1. Definición

El protocolo es el "marco general que incorpora
roles, responsabilidades y acciones que deben ser desplegadas al interior de las organizaciones
para gestionar un incidente de seguridad" (SIC,
2020).

2. Proceso de manejo del Protocolo

Para su incorporación en una organización, debe ser:

a)Documentado
b)Implementado
C) Comunicado al equipo humano de la organización
D) Monitoreado

FACTORES PARA DEFINIR LOS PROTOCOLOS

Cada organización debe tomar medidas de seguridad según:

a. Los niveles de riesgo del tratamiento para los derechos y libertades de los Titulares.
b. La naturaleza de los datos.
c. Las posibles afectaciones si se vulneran los datos del Titular.
d. Magnitud de titulares de los datos e información.

URIBE · YÁÑEZ

¿QUÉ DEBE INCLUIR EL PROTOCOLO DE TRATAMIENTO?

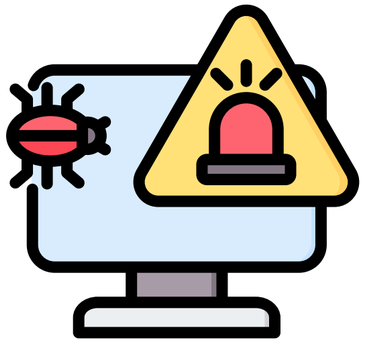
El equipo de respuesta debe evaluar si el protocolo necesita cambios.	**Evaluación de efectividad del protocolo**
Dividir las tareas o gestiones a cada una de las áreas encargadas.	**Asignación de operaciones**
Registro interno de los incidentes para efectos legales.	**Documentación del incidente**
La revisión de cómo ocurrió el incidente y su debido manejo deben ser analizados.	**Evaluación y análisis de la gestión**

TIPOS DE INCIDENTES DE SEGURIDAD Y SUS CAUSAS

1.Tipos

Se clasifican dependiendo el grado de pérdida de las siguientes carácterica de información:

a) Confidencialidad
b) Integridad
c) Disponibilidad



2. Causas

- Inexistencia de políticas preventivas de
- Negligencia humana
- Casos fortuitos
- Actos maliciosos o criminales
- Fallas en los sistemas de la entidad
- Deficiencias en las operaciones
- Alteración, pérdida o destrucción de archivos físicos

PASOS PARA RESPONDER A UN INCIDENTE DE SEGURIDAD

Gráfico tomado de Superintendencia de Industria y Comercio

INTELIGENCIA ARTIFICIAL EN EL TRATAMIENTO DE DATOS PERSONALES

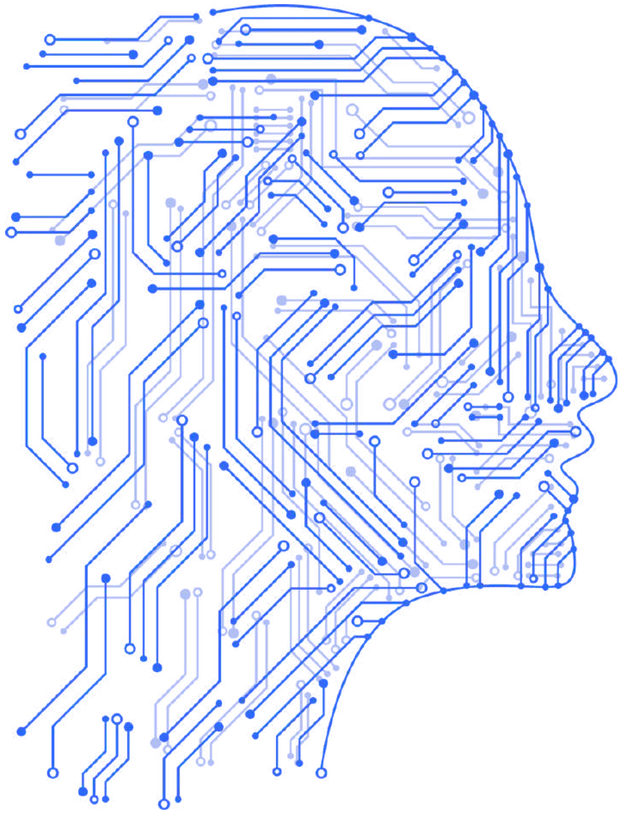
¿QUIÉNES ESTÁN INVOLUCRADOS?

Dada la complejidad del manejo de un proyecto de Inteligencia Artificial, existen varios sujetos involucrados en el tratamiento de los datos, a saber: El Responsable, posibles encargados, titulares, desarrolladores de tecnología, el software y los algoritmos, usuarios, proveedores del sistema y autoridades de protección de datos.

IMPACTO DE LA REGULACIÓN

El tratamiento de datos personales en la era de la inteligencia artificial ha sido objeto de estudios y discusiones en el ámbito jurídico. Es por esto que creó la "Declaración relativa a la ética y protección de datos en la inteligencia artificial" donde se establece la importancia del desarrollo de la IA respetando los derechos humanos, y en este caso el Habeas Data.

Tomado de https://privacyconference2018.org/



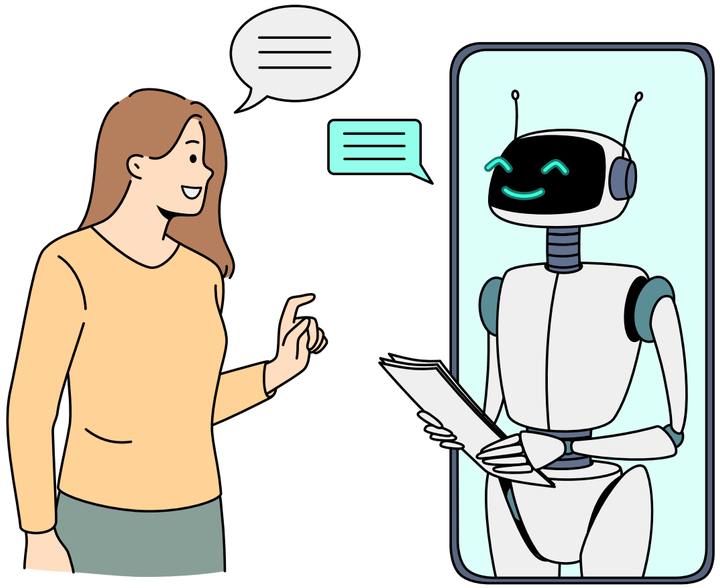
IMPACTO DE LA REGULACIÓN

Asimismo, se ha establecido que cuando los productos de la IA usan datos personales para alcanzar sus fines, los fabricantes de estos deben respetar la regulación especial de datos personales, la cual consta de las regulaciones del país donde se ejerza el uso y por los documentos internacionales expedidos sobre el tema.

Cartilla SIC RECOMENDACIONES GENERALES PARA EL TRATAMIENTO DE DATOS EN LA IA.

¿QUÉ HACER ENTONCES?

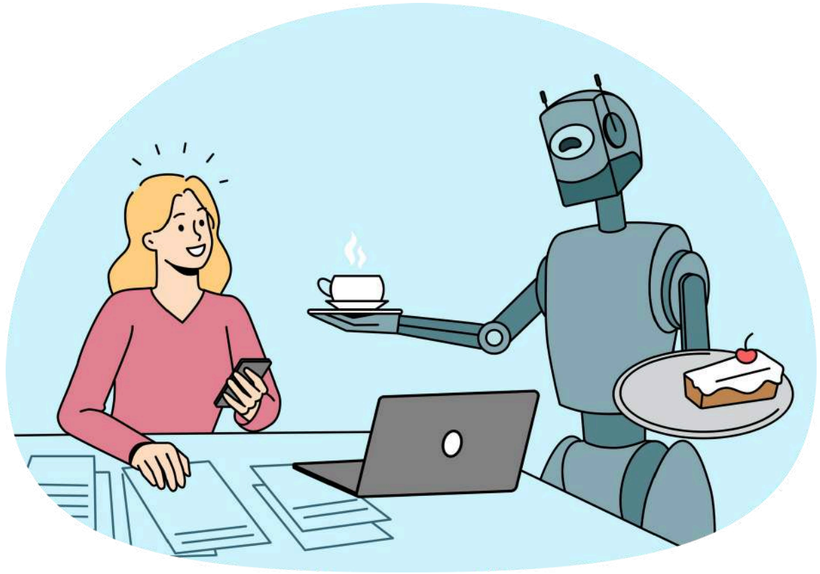
- Revisa las Políticas de Privacidad antes de dar tu autorización.
- Establece contraseñas difíciles y cámbialas con frecuencia.
- Mantén actualizados tus dispositivos y aplicaciones, ya que estos suelen mejorar la seguridad en cada actualización.
- Desconecta dispositivos o servicios de IA cuando no los estés utilizando para reducir la exposición de tus datos.



Cartilla SIC RECOMENDACIONES GENERALES PARA EL TRATAMIENTO DE DATOS EN LA IA.

¿QUÉ HACER ENTONCES?

- Educación Continua.
- Evita autorizar el tratamiento de tus datos si no es necesario.
- Evita brindar información personal o confidencial a herramientas como “ChatGPT” ya que puede utilizarla para su funcionamiento.



Cartilla SIC RECOMENDACIONES GENERALES PARA EL TRATAMIENTO DE DATOS EN LA IA.

URIBE · YÁÑEZ

Asesores Legales

Bogotá - Colombia
info@uribeyanez.com; gerencia@uribeyanez.com
Cra. 19B No. 83-02 oficina 304, Edificio Time Square

WWW.URIBEYANEZ.COM