Evento Híbrido
Virtual / Presencial

SEMANA de la SALUD OCUPACIONAL

Reflexión, madurez y nuevos desafíos

Organiza:

CSOA
CORPORACIÓN DE SALUD OCUPACIONAL Y AMBIENTAL

www.corporacionsoa.co

44° Congreso de Ergonomía, Higiene, Medicina y Seguridad Ocupacional.

Hotel Intercontinental Medellín - Colombia

6, 7 y 8 de noviembre de 2024

"Ciberseguridad para profesionales de la salud: más allá de las barreras físicas"

CO COLOMBIA · ACHO Capítulo Antioquia · ASASI Asociación Colombiana de Seguridad Integral · SCE Sociedad Colombiana de Ergonomía Capítulo Antioquia · Sociedad Colombiana de Medicina del Trabajo Capítulo Antioquia

Organiza:

CSOA CORPORACIÓN DE SALUD OCUPACIONAL Y AMBIENTAL

SEMANA de la SALUD OCUPACIONAL 30

Agenda

1. Panorama de la Ciberseguridad en el Sector Salud

2. Riesgos Cibernéticos Claves en el Sector

3. Estrategias de Protección y Mitigación

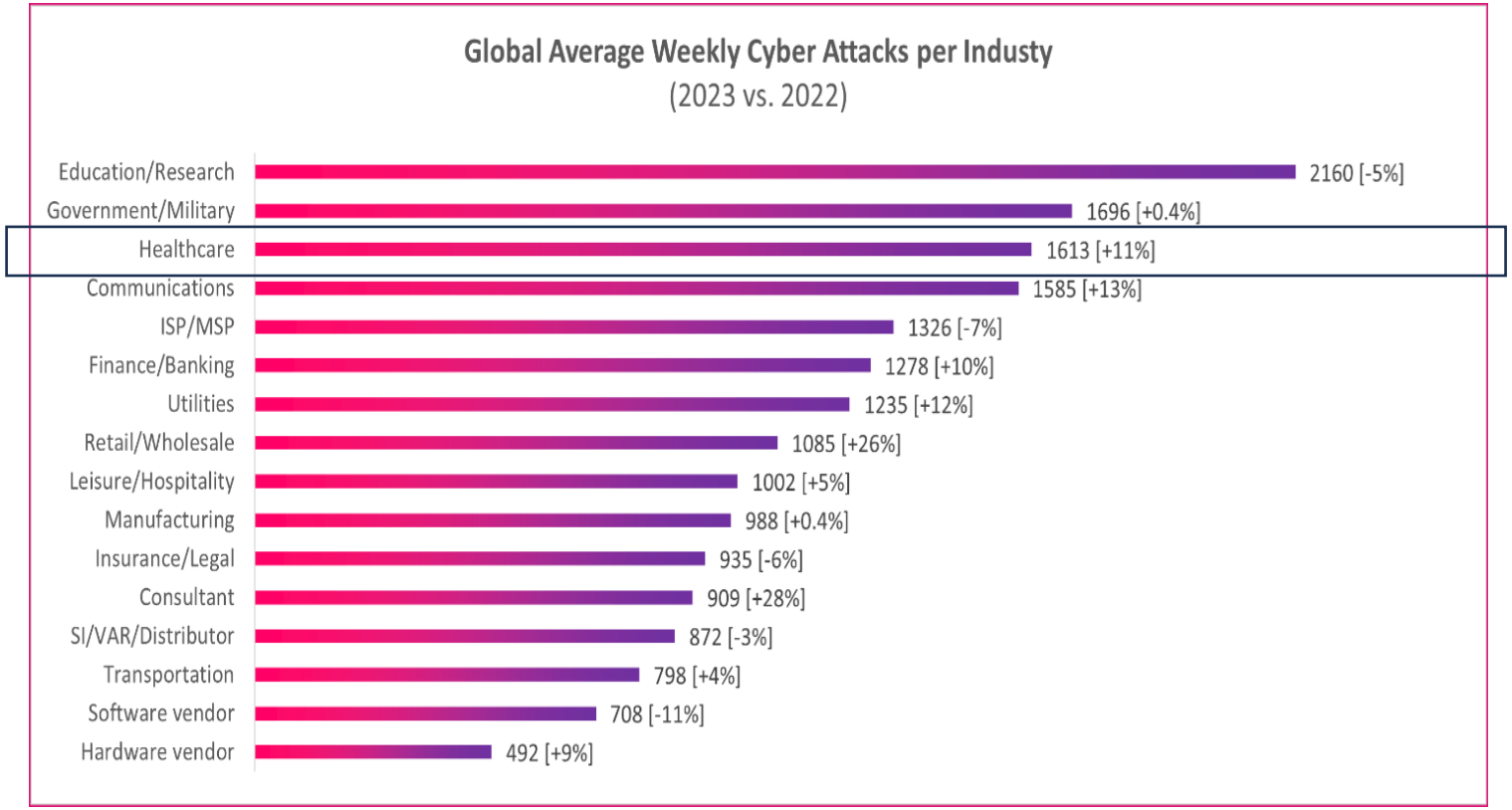
4. Modelos y Marcos de Referencia

1. Panorama de la Ciberseguridad en el Sector Salud

- En los **tres primeros trimestres de 2023**, el sector sanitario global experimentó **1.613 ciberataques por semana**, casi **cuatro veces más que el promedio global,** y un aumento significativo respecto al mismo período del año anterior.
- El **sector sanitario** ha visto un dramático **incremento en los costos por ciberataques en los últimos tres años,** con un **costo promedio de violación de casi 11 millones de dólares**, más del triple del promedio global. **Esto convierte a la sanidad en el sector más costoso en cuanto a ciberataques**.
- Los **ataques de ramsonware** han sido el tipo de ciberataque **más frecuente en las organizaciones sanitarias, representando más del 70%** de los ataques exitosos **en los últimos dos años.**
- La mayoría de los ciberataques (entre el 79% y el 91%), en todos los sectores, comienzan con **tácticas de phishing o ingeniería social**, que permiten a los ciberdelincuentes acceder a cuentas o servidores.

Fuente: *Global-Healthcare-Report-and-Timeline-EN_US* PDF (WWW.KNOWBE4.COM)

Ataques al Sector Salud a nivel Mundial



Una tormenta cibernética continua con crecientes amenazas de ransomware en el sector de salud

(Check Point Research, 25 de octubre de 2023)

Fuente: https://blog.checkpoint.com/security/a-continuing-cyber-stormwith-increasing-ransomware-threats-and-a-surge-in-healthcare-andapac-region/

Ataques al Sector Salud

Entre 2016 y 2021, los ciberataques y la interrupción resultante pueden haber contribuido a la muerte de 42 a 67 pacientes

Los ataques en el sector sanitario mundial superaron la media mundial en más de cuatro veces, con una media de 1613 ataques por semana

Ataques de Ransomware a la Cadena del Sector Salud

Ataques de Ransomware a Hospitales, Servicios Asistenciales, Urgencias

- Empresas de I+D Productos Farmacológicos
- Proveedores de Equipos e Insumos
- Proveedores de Plasma Sanguíneo
- Intermediadores del pagos y reclamaciones
- Farmacias y expendedores de medicamentos
- Proveedores de Seguros y Planes Médicos

Fuente: www.knowbe4.com/hubfs/Global-Healthcare-Report-and-Timeline-EN_US.pdf

Ataques al Sector Salud

- El 4 de enero de 2024 se informó de que se habían presentado demandas colectivas contra ESO Solutions, con sede en Texas, por **un ciberataque al fabricante de software** que **afectó a casi 2,7 millones de personas e incluyó el robo de historias clínicas sensibles**. **El ataque** ocurrió en octubre de 2023 2024 e **impactó a 14 hospitales en los EE. UU**.
- El 25 de enero de 2024, **el sistema informático del Canadian Capital Health Communication Center (CCSC) sufrió un ataque de ramsonware que afectó a todo el sistema de ambulancias de la región, impidiendo a los paramédicos localizar las llamadas al quedar paralizado completamente y** tener que utilizar sus propios teléfonos para orientarse por la ciudad y llegar al lugar de las llamadas.
- El 27 de enero de 2024, el Instituto Nacional do Câncer (INCA), en Brasil, sufrió **un ciberataque que interrumpió el área de radioterapia y la programación de citas**. Las consultas programadas **continuaron con registros manuales, pero se suspendió la reserva de nuevas citas**
- El 2 de febrero de 2024, una **violación de los servicios de pago de asistencia sanitaria franceses Viamedis y Almerys provocó el robo de datos de más de 33 millones de personas**; La información robada **incluía los datos médicos de los clientes y la información personal de su familia.** Se trata del **mayor ciberataque de la historia de Francia**. La compañía **atiende a 20 millones de personas aseguradas a través de 84 organizaciones de atención médica**. El ataque comenzó con **un correo electrónico de phishing**

Ataques al Sector Salud

- **El 31 de enero de 2024**, el Lurie Children's **Hospital de Chicago sufrió un ataque de ransonware** del grupo de ramsonware Rhysida **que dejó fuera de línea toda la red informática de la institución y obligó al personal a recurrir a procesos manuales**. Lurie Children's Hospital brinda atención a más de 239,000 niños anualmente en su hospital del centro de Chicago, **17 centros de servicios ambulatorios y seis centros de atención primaria**. El **7 de marzo de 2024, el grupo de ransomware afirmó haber vendido datos robados del hospital después de ponerlos a la venta en la web oscura por 3,4 millones de dólares**. El listado se actualizó para afirmar: "Se vendieron todos los datos" y se produjo justo cuando **el hospital anunció que estaba avanzando en la restauración de sus sistemas clave, incluida su plataforma de registros médicos electrónicos y su sistema telefónico.**

- El 18 de abril de 2024, **Octapharma, un proveedor de plasma sanguíneo de EE. UU., fue objeto de un ataque de ransomware que cerró 190 centros de plasma en 35 estados de EE. UU**. Los centros **proporcionan el 75% del suministro de plasma sanguíneo que salva vidas para los EE. UU. y Europa**. No está claro si la matriz suiza de la compañía, Octapharma AG, también se vio afectada. **La banda de ransomware BlackSuit publicó datos robados, incluida información de donantes, datos de laboratorio, información confidencial de la empresa y detalles de empleados**.

Ataques al Sector Salud en Colombia

En los últimos cinco años, el sector salud en Colombia ha sido blanco de varios ciberataques importantes, los cuales han afectado gravemente la infraestructura crítica del país.

1. Uno de los incidentes más notables fue el ataque sufrido por **Keralty** en noviembre de 2022, un grupo que gestiona una red de hospitales y centros de salud en América Latina, España y Estados Unidos. Este ataque, atribuido al grupo de ransomware **RansomHouse**, interrumpió sus operaciones y comprometió la seguridad de los datos sensibles de pacientes(Semana)(ACIS). Colsanitas (Grupo Keralty) perdió 0,7 terabytes de información incluyendo estados financieros, balances, presupuestos e información personal de sus usuarios (Portafolio, 2022);
2. Otra entidad afectada fue el **Instituto Nacional de Vigilancia de Medicamentos y Alimentos (Invima)**, que entre 2022 y 2023, sufrió de 3 ciberataques, en los que se estima que fueron capturados 700 GB de datos confidenciales de la entidad y la interrupción de las plataformas tecnológicas que comprometieron temporalmente sus operaciones (ACIS)(La Nota Economica).
3. Además, en 2023, el sistema de salud pública también enfrentó interrupciones masivas debido a ataques que afectaron múltiples entidades, incluidas las **EPS y hospitales**. Estos ataques se centraron en el secuestro de datos a través de ransomware, lo que ha expuesto información confidencial de pacientes, y en algunos casos, los ciberdelincuentes publicaron datos robados(Semana)(Revista Coomtacto).
4. **Salud Total EPS-S** fue objeto de ataque informático externo; En comunicado oficial, Salud Total EPS-S informó que el domingo 1 de mayo de 2022 la plataforma tecnológica de la entidad fue objeto de un ataque informático externo, lo que ha produjo una indisponibilidad en parte de la información relacionada con la operación.(https://revistahospitalaria.org/)
5. **Audifarma** sufrió un ataque a inicios de 2023: La **red de farmacias** fue objeto de un ataque informático externo en su infraestructura tecnológica el domingo 22 de enero de 2023. .(https://revistahospitalaria.org/)

2. Riesgos Cibernéticos Claves en el Sector Salud

Ataques al Sector Salud en Colombia

Concepto del Riesgo Cibernético

2. Riesgos Cibernéticos Claves en el Sector Salud

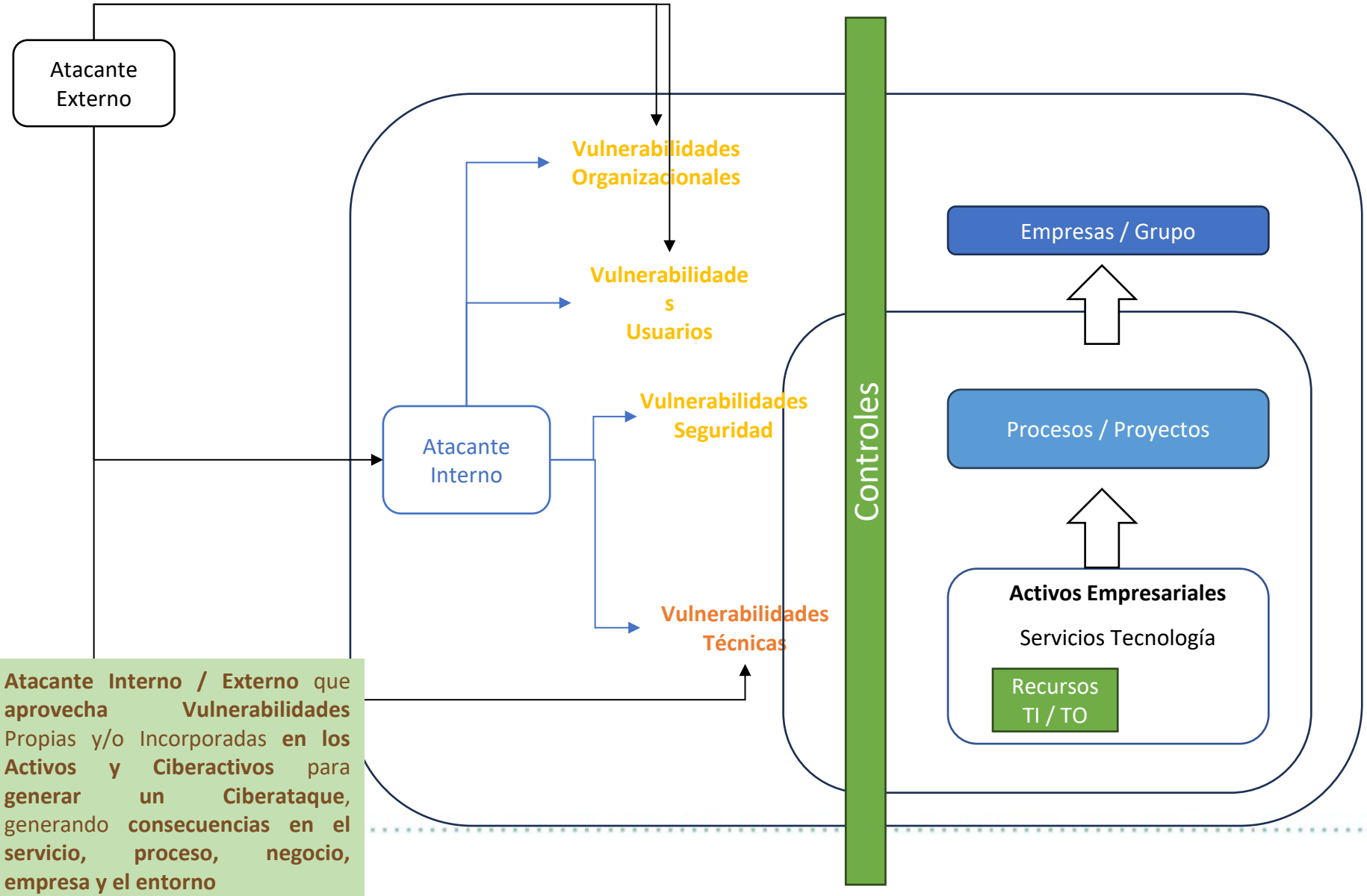
Conceptos Claves del Ciber riesgo

Amenazas
Origen Interno / Externo

Vulnerabilidad

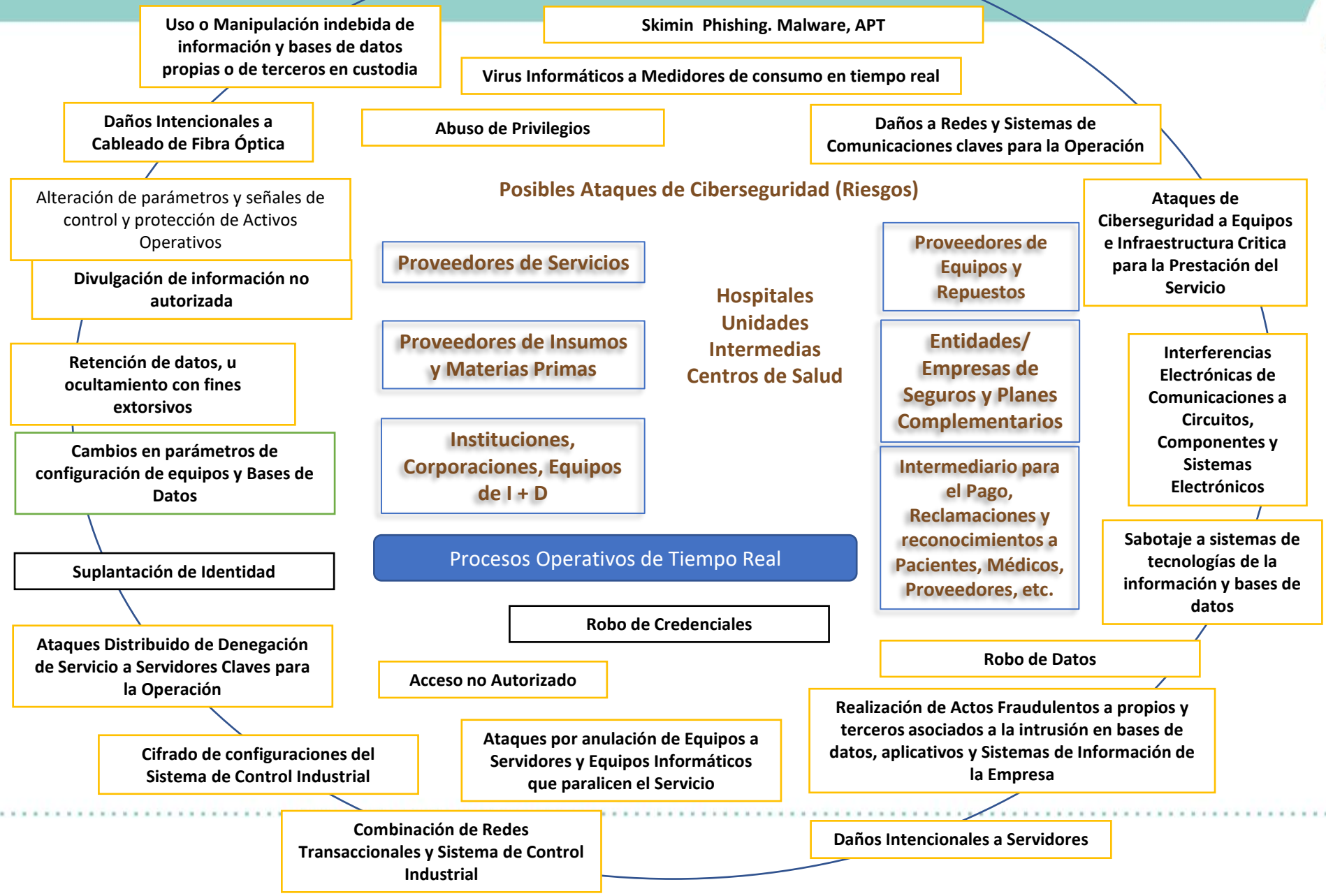
Activos de una empresa

2. Riesgos Cibernéticos Claves en el Sector Salud



Atacante Interno / Externo que **aprovecha Vulnerabilidades** Propias y/o Incorporadas **en los Activos y Ciberactivos** para **generar un Ciberataque**, generando **consecuencias en el servicio, proceso, negocio, empresa y el entorno**

2. Riesgos Cibernéticos Claves en el Sector Salud



2. Riesgos Cibernéticos Claves en el Sector Salud

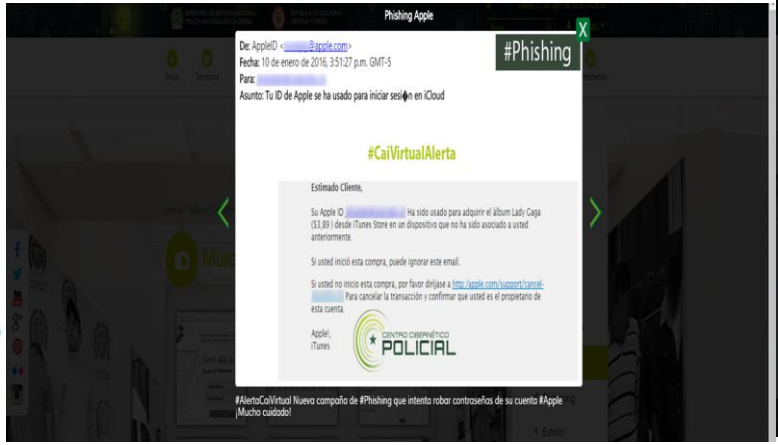
Ataques al Sector Salud en Colombia

Amenazas y Vulnerabilidades Cibernéticas

2. Riesgos Cibernéticos Claves en el Sector Salud

2. Riesgos Cibernéticos Claves en el Sector Salud

Phishing



2. Riesgos Cibernéticos Claves en el Sector Salud

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: Bob Smith <Bob.Smith@company.com>
Subject: Unusual Sign In Activity

Outlook

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account bo******@company.com. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

Review recent activity

Thanks,
The Microsoft Team

Verifica tu cuenta
Detectamos alguna actividad inusual sobre un inicio de sesión **r**eciente en su cuenta de Microsoft xxxx, **es posible que esté iniciando sesión desde una nueva aplicación o dispositivo de ubicación**.

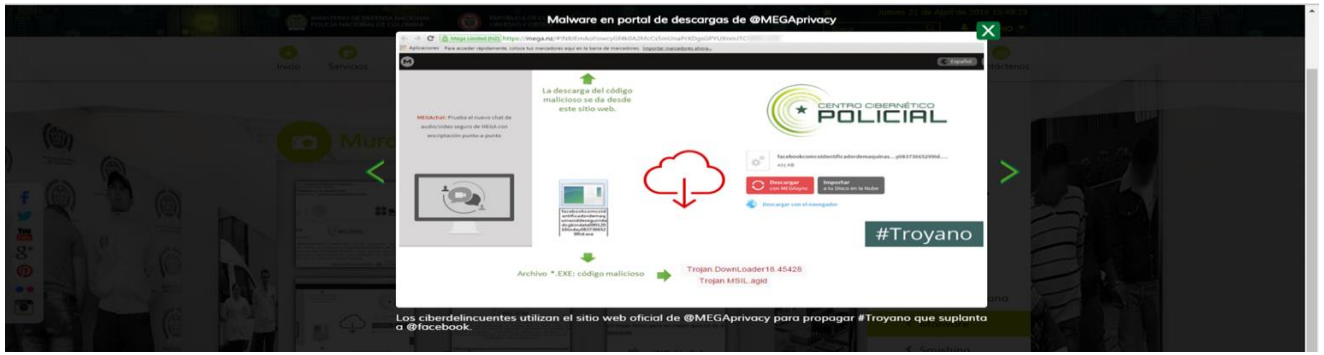
Para ayudar a mantener su cuenta segura. **Hemos bloqueado el acceso a su bandeja de entrada, lista de contactos y calendario para ese inicio de sesión**. Revise su actividad reciente y lo ayudaremos a proteger su cuenta. **Para recuperar el acceso necesitarás confirmar que la actividad reciente fue tuya**.

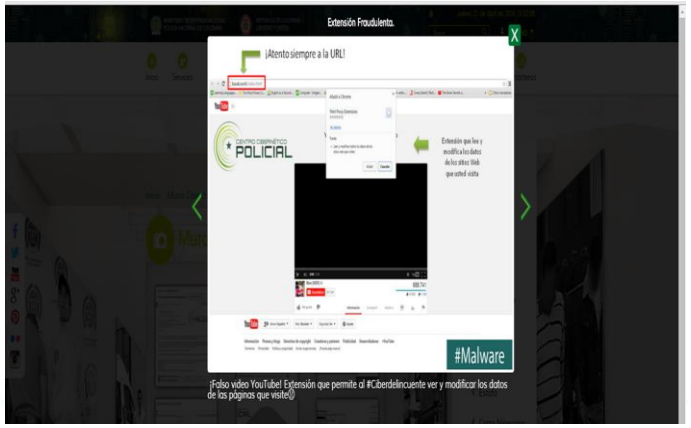
2. Riesgos Cibernéticos Claves en el Sector Salud

2. Riesgos Cibernéticos Claves en el Sector Salud

SEMANA de la SALUD OCUPACIONAL

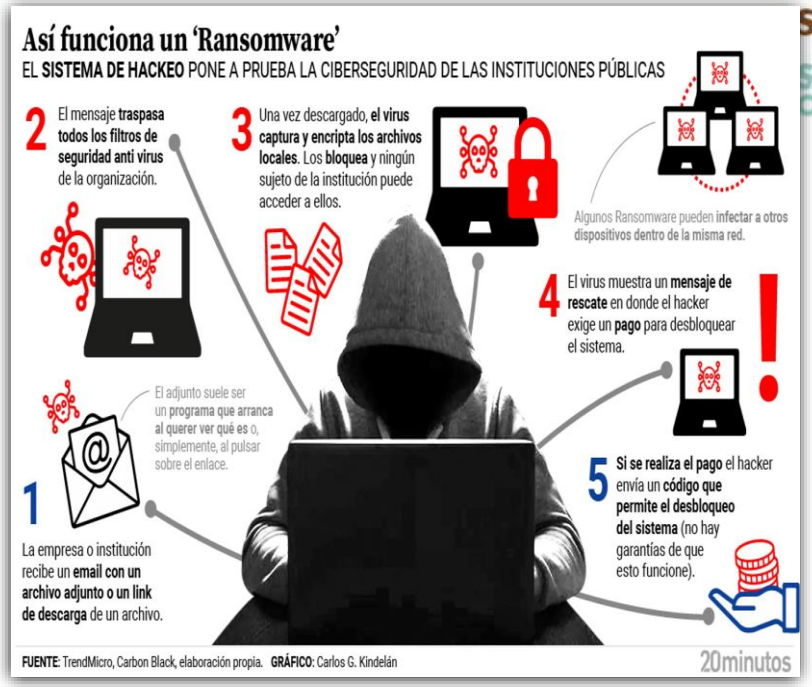
Malware





Ramsonware


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt


Así funciona un 'Ransomware'
EL SISTEMA DE HACKEO PONE A PRUEBA LA CIBERSEGURIDAD DE LAS INSTITUCIONES PÚBLICAS
1 La empresa o institución recibe un email con un archivo adjunto o un link de descarga de un archivo.
El adjunto suele ser un programa que arranca al querer ver qué es o, simplemente, al pulsar sobre el enlace.
2 El mensaje traspasa todos los filtros de seguridad anti virus de la organización.
3 Una vez descargado, el virus captura y encripta los archivos locales. Los bloquea y ningún sujeto de la institución puede acceder a ellos.
Algunos Ransomware pueden infectar a otros dispositivos dentro de la misma red.
4 El virus muestra un mensaje de rescate en donde el hacker exige un pago para desbloquear el sistema.
5 Si se realiza el pago el hacker envía un código que permite el desbloqueo del sistema (no hay garantías de que esto funcione).
FUENTE: TrendMicro, Carbon Black, elaboración propia. GRÁFICO: Carlos G. Kindelán
20minutos


Ransomware Qué Es y Cómo Funciona Definición

2. Riesgos Cibernéticos Claves en el Sector Salud

Vulnerabilidades Técnicas

Vulnerabilidades Usuario

Vulnerabilidades Organizacionales

Vulnerabilidades Seguridad

3. Buenas Prácticas de Seguridad

3. Buenas Prácticas de Seguridad en el Sector Salud

1. Protección de la Información de Salud (PHI) y Privacidad de los Pacientes	Confidencialidad, Manejo Datos Personales Manejo seguro de las Historias Clínicas Electrónicas
2. Contraseñas Seguras y Gestión de Accesos	Contraseñas Fuertes, Autenticación Multifactor Cambios frecuentes de las Contraseñas
3. Capacitación y Conciencia sobre Phishing y Correos Electrónicos Maliciosos	Identificación y Gestión de Correos Sospechosos Campañas de Phishing y Campañas de Concienciación
4. Actualizaciones de Software y Parches de Seguridad	Mantener los Sistemas actualización, Aplicación de Parches de Seguridad y Control Software no Autorizado
5. Protección de Dispositivos Médicos Conectados	Seguridad Dispositivos IOT, Segmentación de Red Monitoreo continuo y alertamiento temprano
6. Copia de Seguridad y Recuperación ante Desastres	Copias periódicas establecidas, Pruebas y simulaciones de Recuperación y Almacenamiento seguro Respaldos

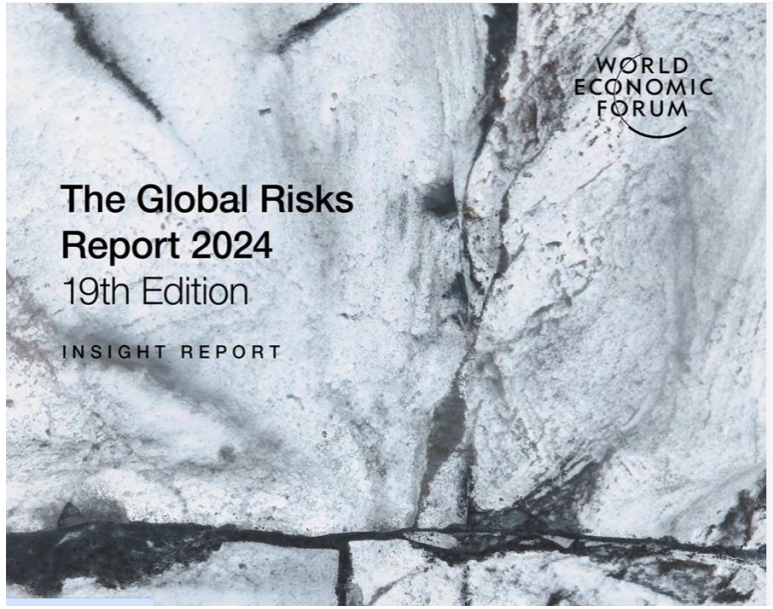
3. Buenas Prácticas de Seguridad en el Sector Salud

7. Control de Acceso Físico	Protección de las Instalaciones y Accesos, Seguridad Perimetral Física y Electrónica y Seguridad de Los Activos y Dispositivos
8. Cultura de Seguridad y Responsabilidad Compartida	Fomento de la Comunicación Abierta, Inclusión de todas Las partes involucradas, La Seguridad un Compromiso de Todos y Campañas permanentes de Formación y Entrenamiento
9. Ejercicios periódicos de Etical Hacking, Pentesting, RED TEAM y BLUE TEAMS	Fomento de la Comunicación Abierta, Inclusión de todas Las partes involucradas, La Seguridad un Compromiso de Todos y Campañas permanentes de Formación y Entrenamiento
10. Conformación de un Equipo de Respuesta a Incidentes	Fomento de la Comunicación Abierta, Inclusión de todas Las partes involucradas, La Seguridad un Compromiso de Todos y Campañas permanentes de Formación y Entrenamiento

4. Modelos y Marcos de Referencia

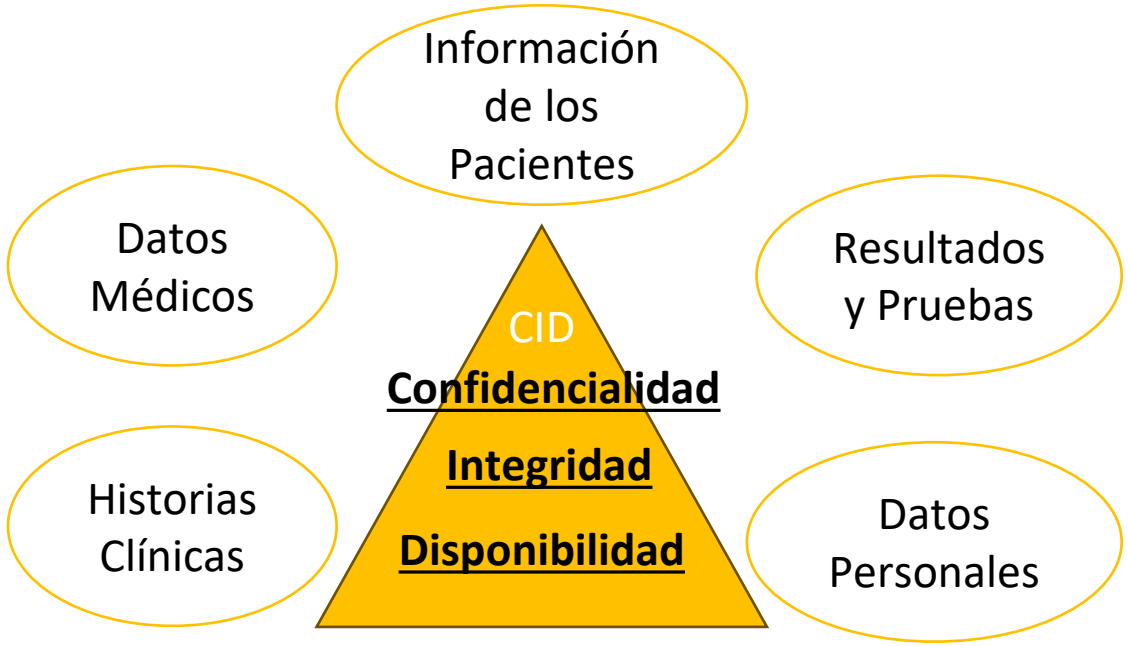
https://revistahospitalaria.org/enportada/ciberseguridad-en-el-sector-salud-un-compromiso-moral-legal-y-de-sostenibilidad/

Ciberseguridad en el sector salud: un compromiso moral, legal y de sostenibilidad



Durante los próximos dos años, se prevé un uso generalizado de la información errónea, la desinformación y de las herramientas para difundirlo.

Ciberseguridad en el sector salud: un compromiso moral, legal y de sostenibilidad



Los ciberdelincuentes pueden utilizar esta información para cometer **fraudes, extorsiones o venderla a terceros**, llevando a consecuencias devastadoras, **poniendo en riesgo la privacidad de los pacientes, la integridad de los datos médicos y, en última instancia, la vida de las personas.**

Ciberseguridad en el sector salud: un compromiso moral, legal y de sostenibilidad

El RGPD establece los requisitos específicos para empresas y organizaciones sobre recogida, almacenamiento y gestión de los datos personales.

Se aplican tanto a las organizaciones europeas que tratan datos personales de ciudadanos en la UE como a las organizaciones que tienen su sede fuera de la UE y cuya actividad se dirige a personas que viven en la UE.

El RGPD se aplica cuando:

- la empresa trata datos personales y tiene su sede en la UE, independientemente de dónde se traten de hecho los datos
- la empresa tiene su sede fuera de la UE pero trata datos personales relativos a ofertas de bienes o servicios a ciudadanos en la UE.

si se encuentra bajo la jurisdicción del GDPR, debe integrar los siguientes 6 principios de privacidad en su empresa.

1. Legalidad, equidad y transparencia en las políticas de privacidad

2. Limitaciones en los fines del procesamiento, solo se recopilan y utiliza la información de la manera en que sus clientes dan su consentimiento

3. La minimización de datos, solo se recopilan los datos que realmente se necesita y nada más

4. Precisión de los datos Asegúrese de que los datos que posee sean precisos y estén actualizados

5. Las limitaciones en el almacenamiento de datos solo conservan los datos durante el tiempo que sea necesario

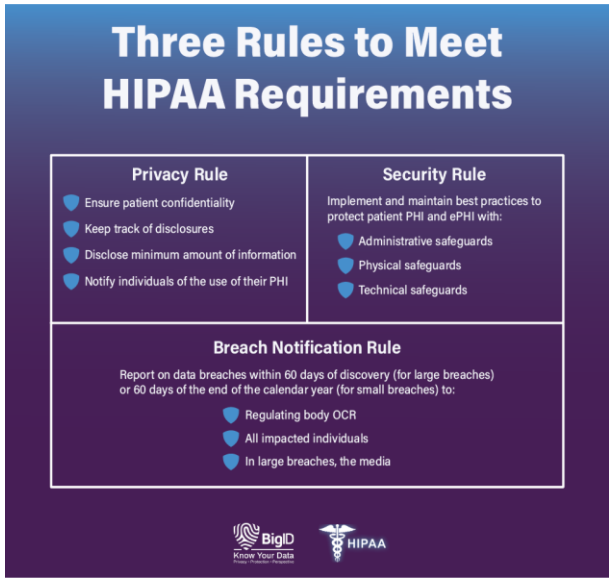
6. Integridad y confidencialidad implementar medidas de seguridad de datos adecuadas y contar con un plan de respuesta a las filtraciones de datos

Fuente: Reglamento general de protección de datos (RGPD) | EUR-Lex (europa.eu)

Ciberseguridad en el sector salud: un compromiso moral, legal y de sostenibilidad

HIPAA
Health Insurance Portability and Accountability Act

HIPAA es un acrónimo de la Ley de Portabilidad y Responsabilidad de los Seguros Médicos, una Ley destinada principalmente a reformar la industria de los seguros de salud en USA que también condujo a la adopción de normas federales para salvaguardar la "Información de Salud Protegida" (PHI) de los pacientes y garantizar la confidencialidad, integridad y disponibilidad de la PHI creada, mantenida, procesada, transmitida o recibida electrónicamente (ePHI).



Regla de Privacidad de HIPAA. Esta Regla estipula qué usos y divulgaciones de PHI por parte de los proveedores de atención médica "cubiertos" son necesarios o permitidos, y cuáles requieren el consentimiento o la autorización del paciente.

La Regla de Seguridad de HIPAA contiene estándares destinados a garantizar la confidencialidad, integridad y disponibilidad de la PHI cuando se crea, mantiene, procesa, transmite o recibe electrónicamente. Los estándares son en su mayoría de naturaleza administrativa o técnica y se implementan "detrás de escena", por ejemplo, copias de seguridad de datos, controles de acceso, planificación y pruebas de contingencia, etc.

¿Qué es HIPAA? (hipaajournal.com)

SEMANA 30 de la SALUD OCUPACIONAL

Ciberseguridad en el sector salud: un compromiso moral, legal y de sostenibilidad

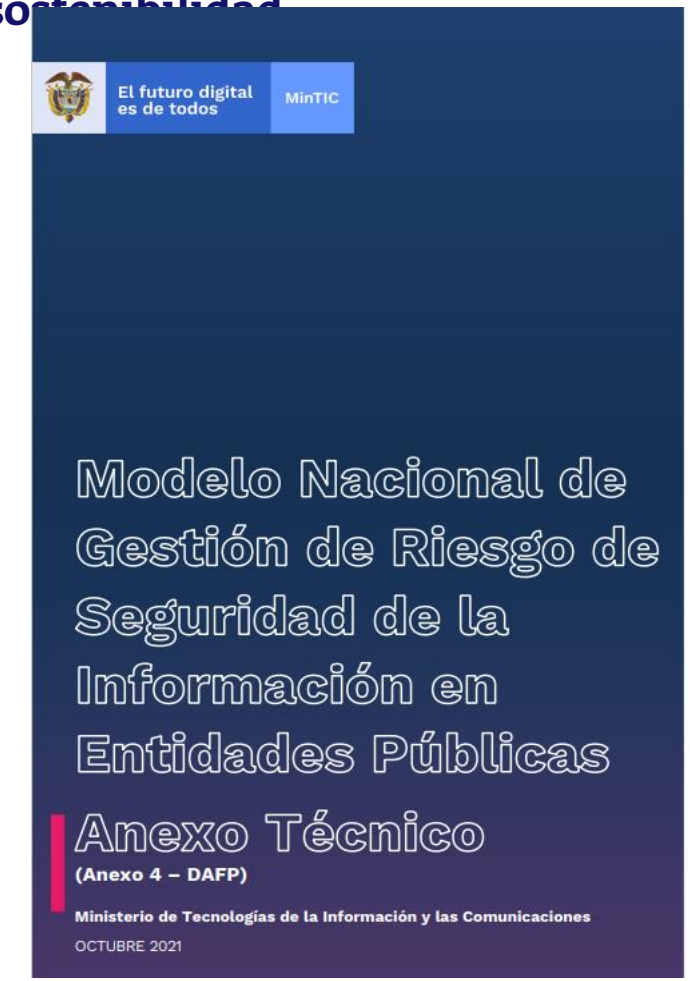
LOS 7 PASOS PARA LA IMPLEMENTACIÓN DE CIBERSEGURIDAD PROPUESTOS SON:

1. Incluir la ciberseguridad como prioridad en la gestión estratégica de la organización.
2. Definir la estructura organizacional en ciberseguridad.
3. Definir los objetivos y las metas de ciberseguridad.
4. Realizar un diagnóstico de situación con análisis de brechas o GAP.
5. Elaborar un plan director de ciberseguridad.
6. Ejecutar el plan director.
7. Evaluar los resultados y el riesgo remanente.

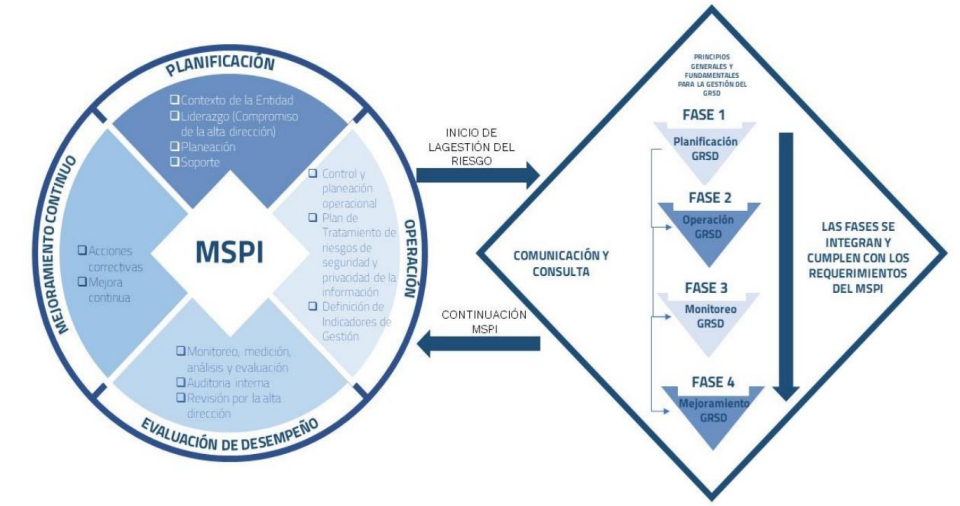
El plan director de ciberseguridad es el instrumento de gestión que se utilizará para cumplir los objetivos y metas de ciberseguridad. No es otra cosa que un programa con duración, alcance y presupuesto determinados, que agrupa todos los proyectos de ciberseguridad que deben realizarse para cumplir un conjunto de metas y objetivos y reducir el GAP existente.

IDB
Inter-American Development Bank

Ciberseguridad en el sector salud: un compromiso moral, legal y de sostenibilidad



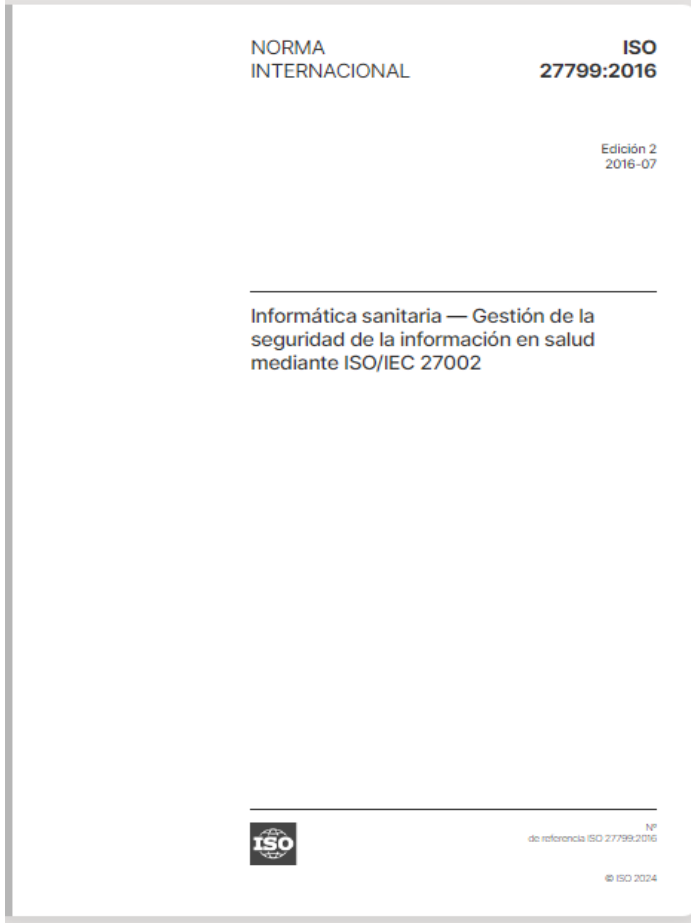
MNGRSI



FUENTE: MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

El objetivo principal de este documento es **orientar a todas las entidades públicas del orden nacional y territorial**, en la **implementación de la Gestión de Riesgos de Seguridad de la información**, que permita **incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información** en las entidades.

Ciberseguridad en el sector salud: un compromiso moral, legal y de sostenibilidad


NORMA INTERNACIONAL

ISO 27799:2016

Edición 2
2016-07

Informática sanitaria — Gestión de la seguridad de la información en salud mediante ISO/IEC 27002

ISO

Nº de référence ISO 27799:2016

© ISO 2024

ISO/IEC 27799

Esta norma fue publicada en 2008 y actualizada en el 2016.

A diferencia del resto de las normas, que son genéricas, la ISO/IEC 27799 ofrece una **guía específica para implementar las cláusulas de control de la ISO/IEC 27002, pero para organizaciones del sector salud o que custodien datos de pacientes.**

Más allá de que los datos personales son importantes y de que se debe resguardar su confidencialidad, integridad y disponibilidad, los datos de los pacientes, en particular, **deben contar con resguardos adicionales ya que su afectación podría comprometer la seguridad física de las personas**, razón por la que en la mayoría de los países son clasificados como información sensible y han de cumplir normativas específicas.

Otro punto importante es **la disponibilidad de esa información puesto que para la eficiencia de la atención médica es crítico contar con dichos datos en cualquier situación** y, en particular, durante desastres o emergencias.

Por esta razón **la guía aplica mayores restricciones a los controles y brinda información más precisa sobre cuál es la mejor manera de usarlos.**

La norma ISO/IEC 27799 incluye 3 anexos.

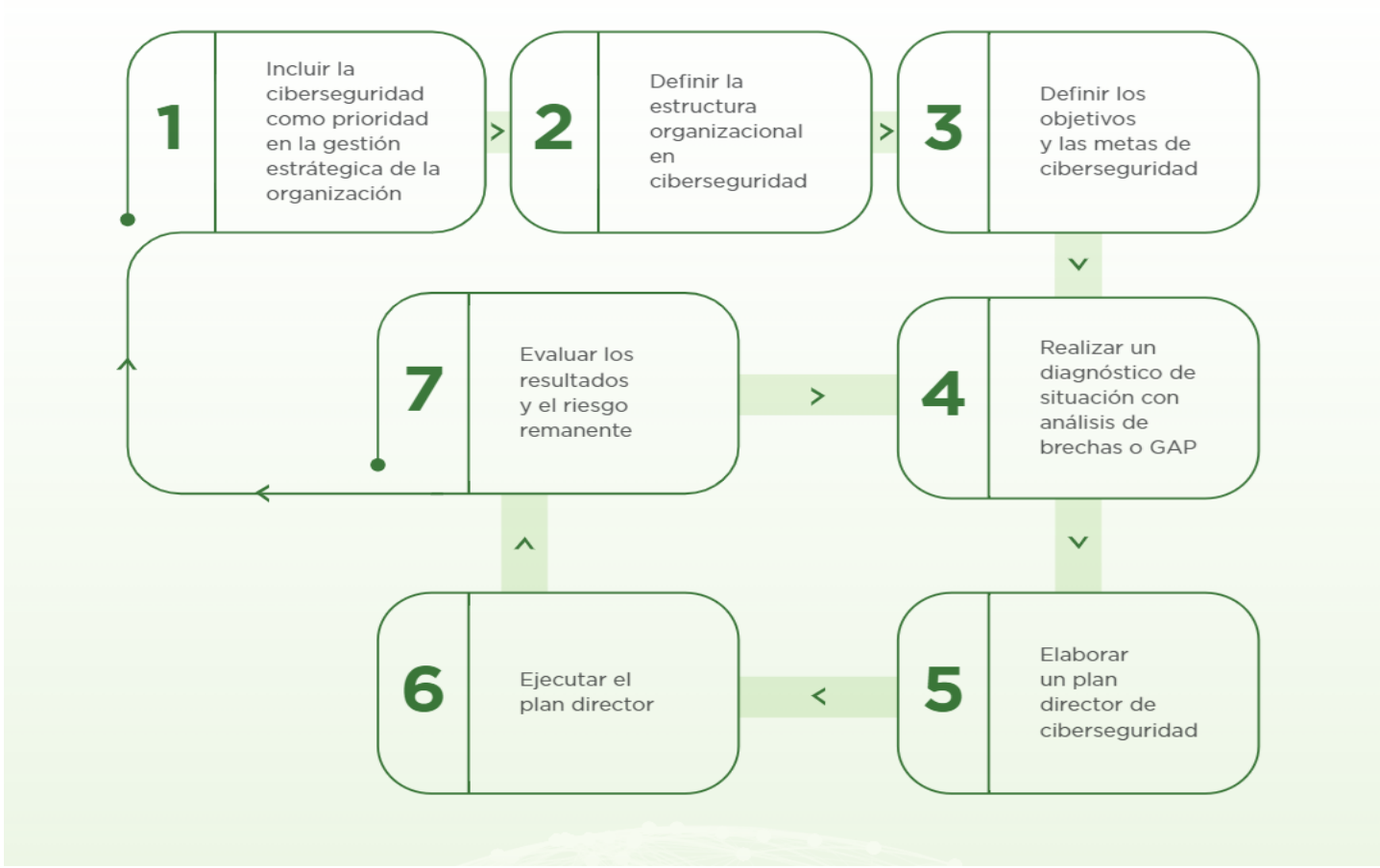
El primero hace referencia a **las amenazas para la protección de la información de salud.**

El segundo anexo **presenta un plan de acción práctico sobre cómo usar el estándar para implementar ISO/IEC 27002 en organizaciones del sector salud.**

El último anexo brinda un **checklis para realizar una autoevaluación de conformidad** que sirve como apoyo a lo descrito en la cláusula de cumplimiento.

Ciberseguridad en el sector salud: un compromiso moral, legal y de sostenib[illegible]

FIGURA 6 • 7 pasos para la implementación de ciberseguridad



Ciberseguridad en el sector salud: un compromiso moral, legal y de sostenibilidad

FRAMEWORKS
ISO/IEC 27001
NIST Cybersecurity Framework v 2.0
COBIT 5
HITRUST CSF V9.4

CONTROLES
ISO/IEC 27002
NIST 800 - 53 Rev. 5
NIST SP 800 - 171
SANS – CIS Control V8.0
OWASP ASVS
ISO/IEC 27799

MARCO REGULATORIO
GDRP (UE)
HIPAA (USA)
MSPI (Colombia)

GUIAS
NIST SP 1800-30
NIST SP 1800-8
Guías de ENISA para el Sector Salud
OWASP – OWASP TOP Ten

TÍTULO DEL TEMA

Ataques al Sector Salud

https://youtu.be/YkCgjrU6cUo?si=fAA4MZqbuHSjVfX9

https://youtu.be/hoGbRqXNoBk?si=oJi3_QG0GjJoJ-2w

Evento Híbrido
Virtual / Presencial

44° Congreso de Ergonomía, Higiene, Medicina y Seguridad Ocupacional.

Hotel Intercontinental Medellín - Colombia

6, 7 y 8 de noviembre de 2024

SEMANA de la SALUD OCUPACIONAL

Reflexión, madurez y nuevos desafíos

..!! La Seguridad un compromiso de todos ¡¡..

Organiza:

CSOA
CORPORACIÓN DE SALUD OCUPACIONAL Y AMBIENTAL

www.corporacionsoa.co