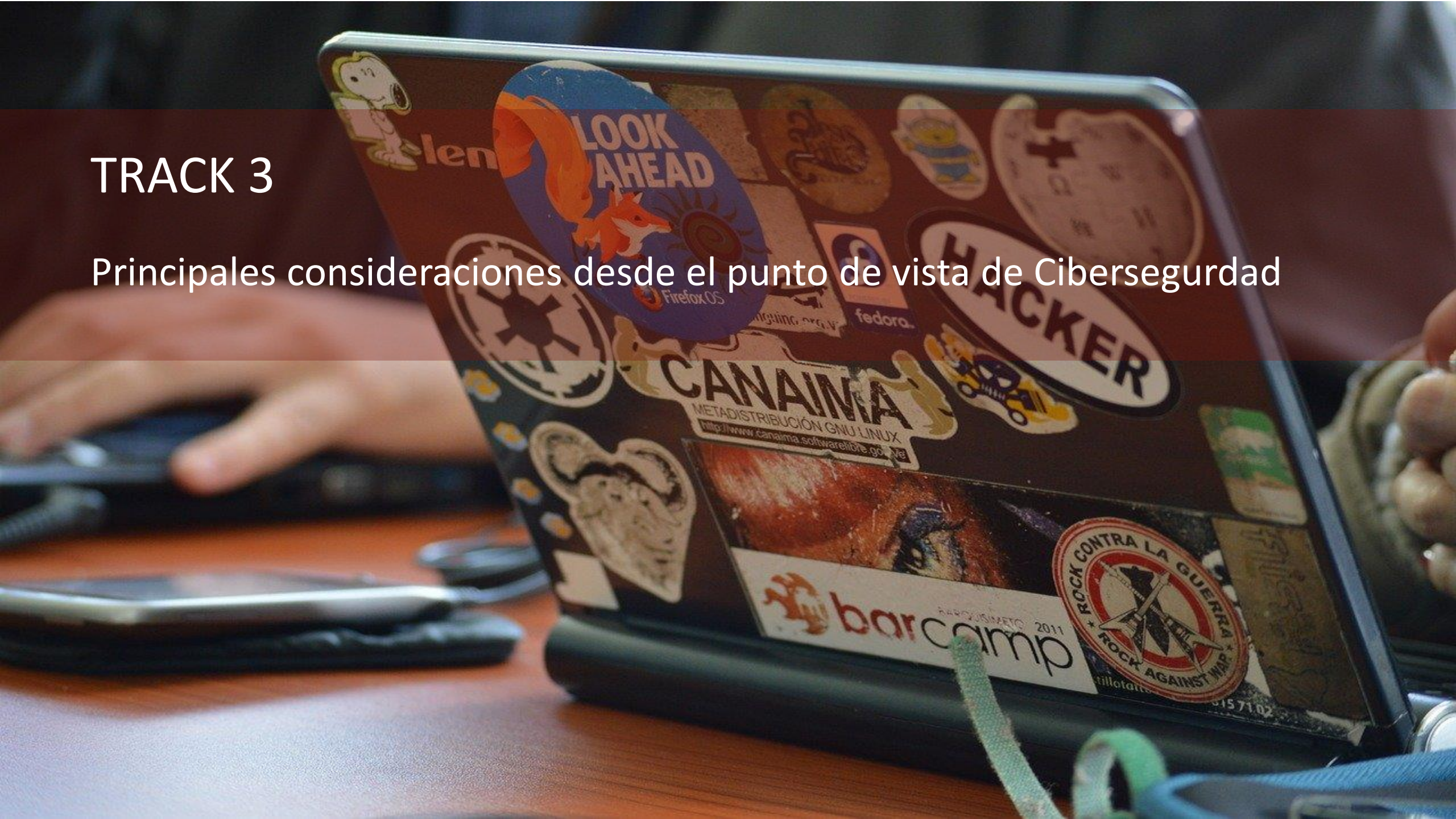
# TRACK 3

Principales consideraciones desde el punto de vista de Cibersegurdad



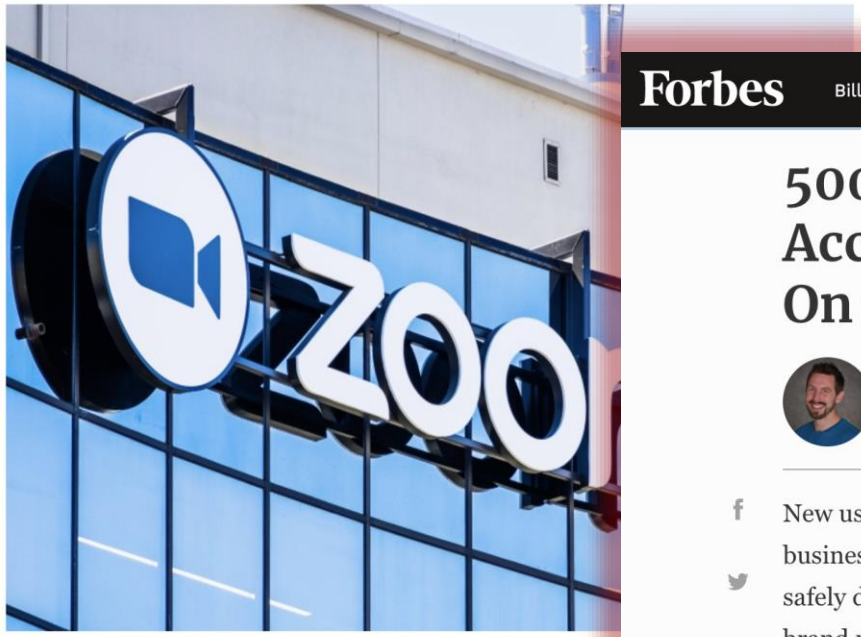
# Objetivos

1. Revisión de contexto internacional
2. Últimos decretos de uruguay vinculados a protección de datos
3. Presentar algunos ejemplos prácticos de implementación de controles
4. Analizar los pasos a seguir para lograr una implementación y aseguramiento de cumplimiento continuo óptimos
5. Aumentar el nivel de concientización respecto del tema
6. Conocer algunas herramientas útiles

# Contexto de Amenazas 2020

threatpost Cloud Security / Malware / Vulnerabilities / Waterfall Security Spotlight / Poc

## Two Zoom Zero-Day Flaws Uncovered




Author:
Lindsey O'Donnell

April 1, 2020 / 12:00 pm

The zero-day Zoom flaws could give local, unp
privileges, and allow them to access victims' mi

UPDATE

Two zero-day flaws have been uncovered in Zoom's macOS

## Zoom vulnerability would have allowed hackers to eavesdrop on calls

*Check Point Research says it figured out which random numbers were valid Zoom calls*

Forbes Billionaires Innovation Leadership Money Business Small Business Lifestyle

## 500,000 Hacked Zoom Accounts Given Away For Free On The Dark Web



**Lee Mathews** Senior Contributor
Cybersecurity
*Observing, pondering, and writing about tech. Generally in that order.*

New users have flocked to the Zoom video conferencing platform as businesses, schools, and other organizations look for ways to meet safely during the Coronavirus pandemic. Unfortunately many of those brand new accounts appear to have been secured with old passwords.


# Contexto de Amenazas 2020

The New York Times

## *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*

By Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber

Sept. 7, 2017

1030

Equifax, one of the three major consumer credit reporting agencies, said on Thursday that hackers had gained access to company data that potentially compromised sensitive information for 143 million American consumers, including Social Security numbers and driver's license numbers.

The attack on the company represents one of the largest risks to personally sensitive information in recent years, and is the third major cybersecurity threat for the agency since 2015.

Equifax has agreed to a settlement over its 2017 data breach that saw as many as 147 million people's personal information, including names, birth dates, addresses, and social security numbers, exposed by the company. As part of the settlement, the company will pay at least $575 million, but this could rise to as much as $700 million depending on the amount of compensation people claim. The company has agreed to provide free credit monitoring services to anyone affected for up to 10 years, as well as cash payments of up to $20,000 per person to refund any costs incurred as a result of the breach.

"Equifax failed to take basic steps that may have prevented the breach that affected approximately 147 million consumers," said FTC Chairman Joe Simons, "This settlement requires that the company take steps to improve its data security going forward, and will ensure that consumers harmed by this breach can receive help protecting themselves from

# Contexto de Amenazas 2020

## SCOTIABANK SOURCE CODE AND LOGIN CREDENTIALS WERE HACKED. USERS SHOULD CONTACT THE BANK TO SECURE THEIR MONEY

Share this...

A severe incident has been confirmed by **IT system audit** specialists. Scotiabank has mistakenly leaked some of its internal source code as well as confidential login credentials for its back-end systems.

The bank's security teams have spent the last twelve hours deleting repositories on **GitHub** that stored sensitive information, which were available to any user for its access. The exposed information includes software blueprints, access keys to exchange rate systems, bank mobile app codes, and database login credentials.

# Contexto de Amenazas 2020

REUTERS

Business Markets World Politics TV

BUSINESS NEWS JUNE 11, 2018 / 4:48 PM / A YEAR AGO

## Bank of Chile trading down after hackers rob millions in cyberattack

2 MIN READ

SANTIAGO (Reuters) - Shares in the Bank of Chile (CHI.SN) were down on Mon
after it confirmed hackers had siphoned off $10 million of its funds, mainly to Hon
Kong, though the country's second-largest commercial bank said no client accoun
been impacted.

SECCIONES CNN CHILE EN VIVO

PAÍS FRAUDE 18.07.2018 / 13:38

## ¿Cómo le robaron $475 millones al Banco de Chile sin que nadie se diera cuenta?

Un informático sustrajo el dinero desde el computador de su oficina. Esta forma de operar se viene repitiendo desde al menos 10 años, dicen auditores.


DESTACAMOS

Todavía estamos a tiempo de salvar la Tierra: Súmate a Desafío Plástico

# Contexto de Amenazas 2020

/policiales/hackeo-federal-advierten-datos-dificiles-eliminar-vidas-riesgo-_0_3y48I8cCB.html

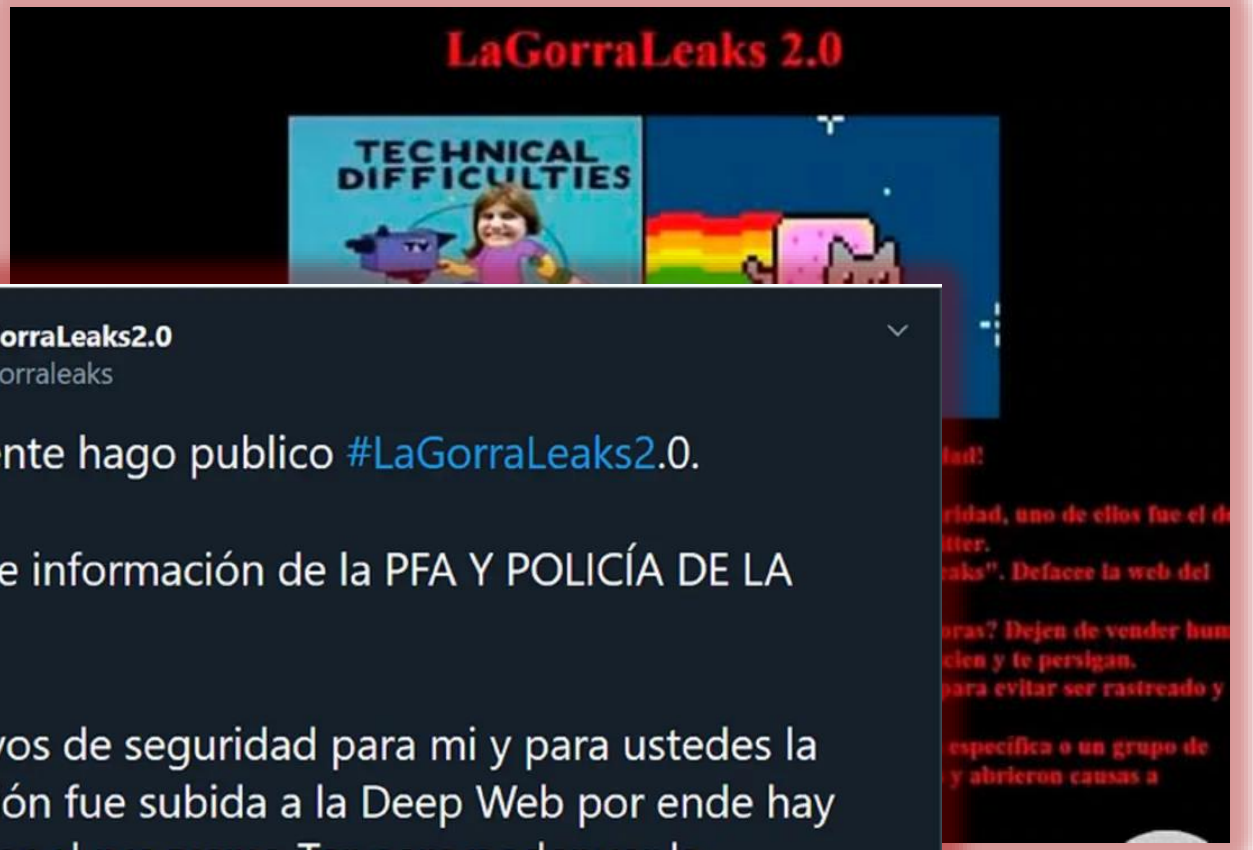
SECCIONES | Clarín POLICIALES

Ciberataque

Hackeo a la Federal: advierten que los datos son muy difícil de eliminar y que "hay vidas riesgo"

Según especialistas, es el mismo hacker que filtró datos de Patricia Bullrich en 2017.


3 7 6




[S] #LaGorraLeaks2.0
@lagorraleaks

Oficialmente hago publico #LaGorraLeaks2.0.

700 GB de información de la PFA Y POLICÍA DE LA CIUDAD.

Por motivos de seguridad para mi y para ustedes la información fue subida a la Deep Web por ende hay que utilizar el programa Tor para poder ver la información.

10:22 a. m. · 12 ago. 2019 · Twitter Web App

# Contexto vinculado a datos personales


Leyes de protección de datos fiscalizadas y controladas fuertemente a nivel internacional

Sin fiscalización ni penalizaciones a nivel local y regional.

La Resolución N° 32/020 de la unidad tiene por objetivo regular los criterios para la designación de la figura del delegado de Protección de Datos Personales, así como aspectos sobre su inscripción y comunicación.

# Contexto vinculado a datos personales

El artículo 40 de la Ley N° 19.670, de 15 de octubre de 2018, establece que las entidades públicas estatales y no estatales, las entidades privadas que traten datos sensibles como negocio principal y las que traten grandes volúmenes de datos **deben designar un delegado de Protección de Datos Personales.**

La Resolución N° 32/020, de 19 de mayo de 2020, **establece los criterios para la designación** de estos delegados, incluyendo los casos de delegados que son personas jurídicas, así como el procedimiento para la comunicación de las designaciones, que deben realizarse a través del sistema de registro de la URCDP*.

El delegado tiene la función de asesorar a sus entidades en el cumplimiento de la Ley N° 18.331 de Protección de Datos Personales y ser el nexo con la URCDP, entre otras tareas.

**La obligación de establecer esta figura** fue reglamentada por el Decreto N° 64/020, de 17 de febrero de 2020, que indica el plazo para realizar dicha designación y los mecanismos de comunicación a la URCDP.

# Decreto 64/020 - 17 de febrero de 2020

IMPO | Centro de Información Oficial — Normativa y Avisos Legales del Uruguay

Volver

**Decreto N° 64/020**

**REGLAMENTACION DE LOS ARTS. 37 A 40 DE LA LEY 19.670 Y ART. 12 DE LA LEY 18.331, REFERENTE A PROTECCION DE DATOS PERSONALES**

Documento Actualizado

**Promulgación: 17/02/2020**

**Publicación: 21/02/2020**

https://www.impo.com.uy/bases/decretos/64-2020

# Decreto 64/020 - 17 de febrero de 2020

## Artículo 3

Medidas de Seguridad. El responsable y el encargado de tratamiento, en su caso deberán adoptar las medidas técnicas y organizativas necesarias para conservar la integridad, confidencialidad y disponibilidad de la información, de forma de garantizar la seguridad de los datos personales. A estos efectos valorarán la adopción de estándares nacionales e internacionales en materia de seguridad de la información, tales como el Marco de Ciberseguridad elaborado por la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento.

Constatada la existencia de incidentes de seguridad que ocasionen, entre otras, la divulgación, destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos, los responsables y encargados de tratamiento deberán iniciar los procedimientos previstos necesarios para minimizar el impacto de dichos incidentes dentro de las primeras 24 horas de constatados.

# Decreto 64/020 - 17 de febrero de 2020

## Artículo 7

Contenido de la evaluación de impacto en la protección de datos personales - La evaluación prevista en el artículo precedente deberá contener, como mínimo:

a) Una descripción sistemática del tratamiento a realizar y su finalidad.

b) Una evaluación del tratamiento con relación al cumplimiento de la normativa de protección de datos personales.

c) Una evaluación de los riesgos para los derechos de los titulares de los datos.

d) Un detalle de las medidas de seguridad y de los mecanismos para demostrar el cumplimento de la normativa de protección de datos personales.

En relación a los tratamientos ya iniciados y que se encuentren incluidos en los supuestos del artículo 6°, el responsable y el encargado de tratamiento en su caso, deberán realizar esta evaluación en un plazo de 1 año a contar de la publicación de este decreto en el Diario Oficial.

Si del resultado de la correspondiente evaluación surge un riesgo potencial y significativo para los derechos de los titulares de los datos, el responsable y el encargado del tratamiento en su caso, deberán ponerlo en conocimiento de la Unidad Reguladora y de Control de Datos Personales, con información pormenorizada de las medidas que adoptaron o adoptarán, y en este último caso el respectivo plazo.

A los efectos de la realización de la evaluación de impacto, según el tipo o volumen de datos y de su tratamiento, la Unidad antes citada fijará criterios que contribuyan al cumplimiento de la obligación prevista en el presente artículo.

# Guía de Evaluación de Impacto en Protección de Datos – 28/1/2020

## Guía de Evaluación de Impacto en la Protección de Datos

28/01/2020

Compartir

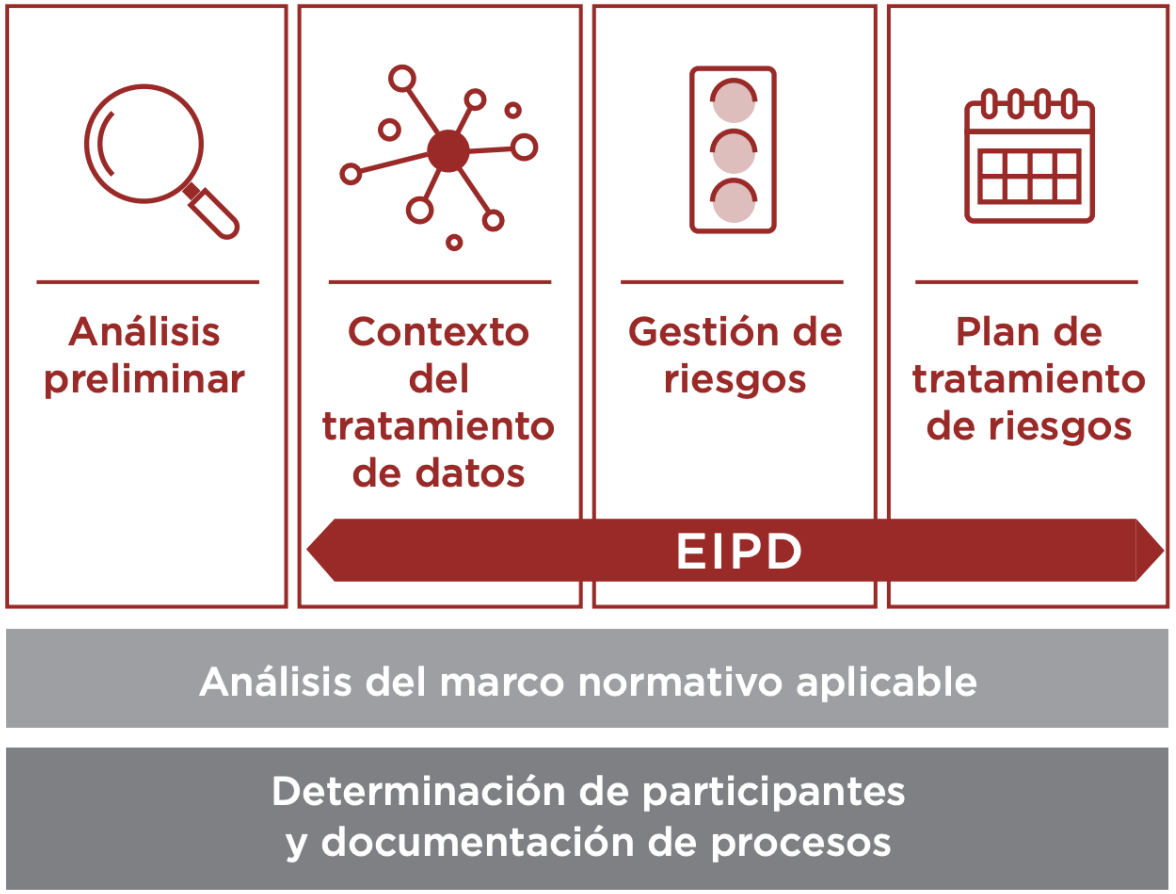
Este documento fue elaborado en forma conjunta entre la Agencia de Acceso a la Información Pública de Argentina (AAIP) y la Unidad Reguladora y de Control de Datos Personales (URCDP) de Uruguay y busca constituirse en una referencia obligada para todas aquellas entidades de la región que realicen tratamiento de datos personales.

### Enlaces de descarga

Guía de Evaluación de Impacto en la Protección de Datos (.pdf 1526 KB)

https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-evaluacion-impacto-proteccion-datos

# Guía de Evaluación de Impacto en Protección de Datos – 28/1/2020





https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-evaluacion-impacto-proteccion-datos

# Decreto 64/020 - 17 de febrero de 2020

## Artículo 8

Privacidad por diseño. El responsable y el encargado de tratamiento, en su caso, deberán incorporar en el diseño de las bases de datos, las operaciones de tratamiento, las aplicaciones y los sistemas informáticos, medidas dirigidas a dar cumplimiento a la normativa de protección de datos personales. A esos efectos, previo al tratamiento y durante todo su desarrollo, aplicarán medidas técnicas y organizativas apropiadas, tales como:

a) Técnicas de disociación, seudonimización y minimización de datos.

b) Mecanismos para asegurar el ejercicio de los derechos de los titulares de los datos personales.

c) Documentación de los consentimientos o de otros fundamentos que legitimen el tratamiento.

d) Tiempo de conservación de los datos, considerando sus tipos y su tratamiento.

e) Adopción de planes de contingencia que incluyan medidas de seguridad de la información.

f) Análisis funcionales y modelos de arquitectura de los datos.

g) Otras medidas establecidas por la Unidad Reguladora y de Control de Datos Personales.

# Decreto 64/020 - 17 de febrero de 2020

## CAPÍTULO IV - DELEGADO DE PROTECCIÓN DE DATOS PERSONALES

### Artículo 10

Alcance. De acuerdo con lo dispuesto en el artículo 40 de la Ley N° 19670 de 15 de octubre de 2018, deberán designar un delegado de protección de datos personales:

a) Entidades públicas, estatales o no estatales y las privadas total o parcialmente de propiedad estatal.

b) Entidades privadas que traten datos sensibles como negocio principal. De conformidad con lo establecido por el artículo 4° literal E) de la Ley N° 18.331 de 11 de agosto de 2008, son datos sensibles aquellos que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

c) Entidades privadas que realicen tratamiento de grandes volúmenes de datos.

Se considera tratamiento de grandes volúmenes de datos cualquier actividad en la que se realice un tratamiento de datos personales de más de 35.000 personas.

La Unidad Reguladora y de Control de Datos Personales, de oficio o ante gestión realizada ante la misma, podrá expedirse sobre la pertinencia de que una entidad privada cuente con un delegado de protección de datos.

# Decreto 64/020 - 17 de febrero de 2020

## Artículo 11

Funciones de los delegados de protección de datos. Las funciones principales de los delegados de protección de datos serán:

a) Asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales.

b) Supervisar el cumplimiento de la normativa sobre dicha protección en la entidad o entidades para las que preste servicios.

c) Proponer todas las medidas que entienda pertinentes para adecuarse a la normativa y a los estándares internacionales en materia de protección de datos personales y verificar su realización.

d) Actuar como nexo entre su entidad y la Unidad Reguladora y de Control de Datos Personales.

## Artículo 12

Calidad y condiciones del delegado. El delegado de protección de datos podrá desempeñar sus funciones a través de cualquier modalidad contractual, sea que implique dependencia o no. Deberá contar con conocimientos en Derecho, especializados en materia de protección de datos personales, los que deberán acreditarse.

En el caso de que el delegado sea persona jurídica, deberá comunicarse a la Unidad Reguladora y de Control de Datos Personales cómo está integrado su órgano de administración, así como los datos de sus integrantes y de la persona o personas físicas que se designen para realizar la tarea.

# RESOLUCIÓN N° 32 2020 - 179 de mayo de 2020

**El Consejo Ejecutivo de la Unidad de la Unidad Reguladora y de Control de Datos Personales**

**RESUELVE**:

**1°.** A los efectos de la designación de delegados de protección de datos, los responsables, y encargados en su caso, deberán tener en cuenta especialmente su calidad de profesional del área jurídica o poseer conocimientos en Derecho, con énfasis en derechos humanos, y conocimientos sobre regulación en materia de protección de datos personales. Ello podrá acreditarse mediante cursos o actividades brindadas por la URCDP u otras entidades nacionales e internacionales, valorándose especialmente la realización de cursos vinculados a responsabilidad proactiva y tratamiento de categorías especiales de datos. Se tendrá en cuenta, asimismo, la experiencia previa en el ámbito de la protección de datos.

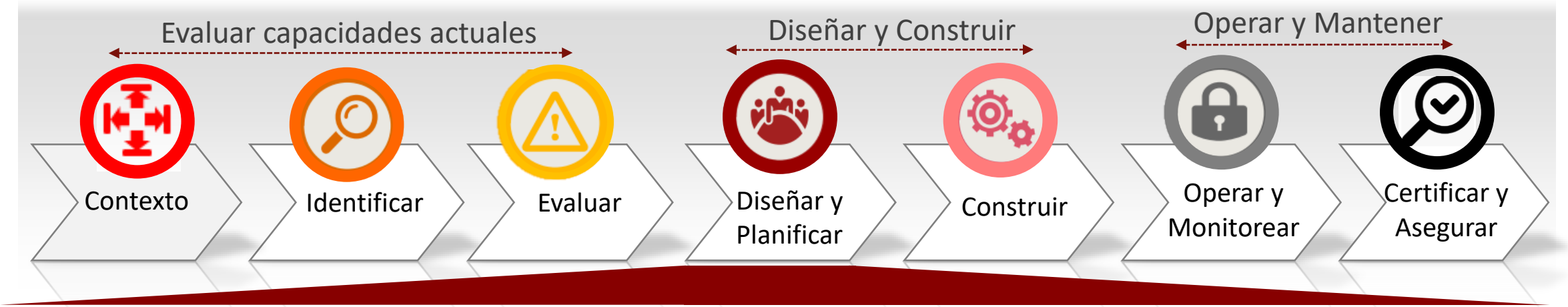
**2°.** Para el tratamiento de datos sensibles, especialmente protegidos u otros que se definan oportunamente, el delegado deberá poseer conocimientos o experiencia en el área de negocio correspondiente, y en aspectos vinculados a la seguridad de la información y gestión de herramientas informáticas.

**3°.** En caso de delegados personas jurídicas, deberá comunicarse a la Unidad Reguladora y de Control de Datos Personales cómo está integrado su órgano de administración, así como los datos de sus integrantes y de la persona o personas físicas que se nominen para realizar la tarea, acreditándose las condiciones de estas personas físicas.

**4°.** La inscripción de Delegados de Protección de Datos se realizará a través del Sistema puesto a disposición por la Unidad, acreditando el cumplimiento de las condiciones citadas.

**5°.** Las comunicaciones de designación de delegados que cumplan con las condiciones señaladas, serán considerarán por la Unidad ante cada gestión, sin perjuicio de las revisiones periódicas y solicitudes de actualizaciones a los delegados designados que se determinen.

https://www.gub.uy/unidad-reguladora-control-datos-personales/institucional/normativa/resolucion-32020




**1. Estrategia y Gobierno**

- Definir alcance, Estructura de Gobierno, roles y responsabilidades. Tener en cuenta emprendimientos de Transformación Digital
- Asegura y respalda el Programa de Privacidad

**2. Gestión de Políticas**

- Políticas, procedimientos, lineamientos y sus respectivos cambios deben estar documentados

**3. Transferencia de Datos fuera de fronteras**

- Definir estrategia teniendo en cuenta que datos, son enviados a dónde para qué y ajustar mecanismos de evaluación

**4. Gestión del Ciclo de Vida de los Datos**

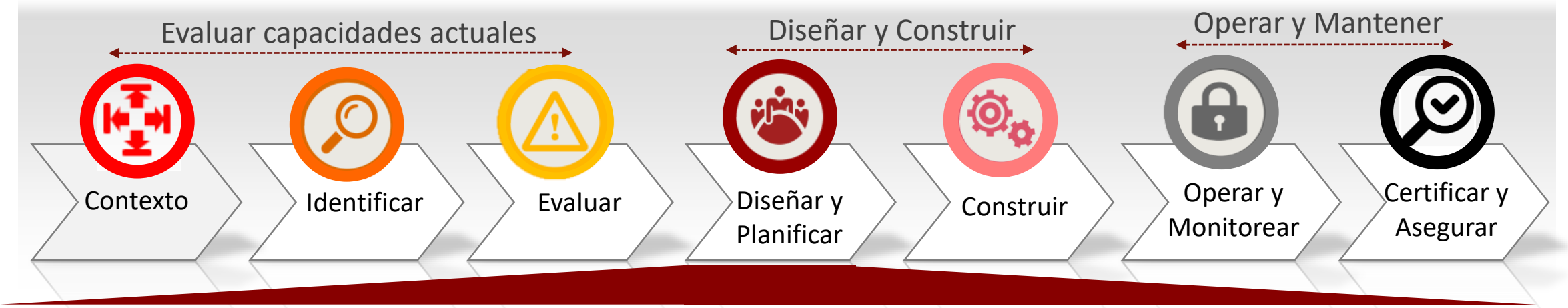
- Mapeo y clasificación de datos
- Mecanismos para identificar nuevos procesamientos y usos de datos personales y eliminación segura
- Gobierno y uso de datos ético
- Prevención Perdida de Datos
- Diseño controles correspondientes

**5. Procesamiento de derechos de los individuos**

- Garantizar correcto procesamiento de derechos y solicitudes de los individuos

**6. "Privacy by Design " (PbD)**

- DPIA
- Incorporar controles de privacidad y evaluación del impacto a través del ciclo de vida de los datos para nuevas iniciativas




**7. Seguridad de la Información**

Diseñar / revisar controles alineados a los existentes:

- Estrategia de Seguridad
- Análisis de Riesgos de IT /Gestión de Riesgos de IT
- Gestión de Identidades y Control de Acceso
- Seguridad de Bases de Datos
- Seguridad Cloud
- CyberRisk & Governance
- Procesos de respaldo
- Network Security
- Gestión de Vulnerabilidades
- Recuperación de Desastres/Continuidad del Negocio
- Estrategias de Encripción, etc.

**8. Gestión de Incidentes**

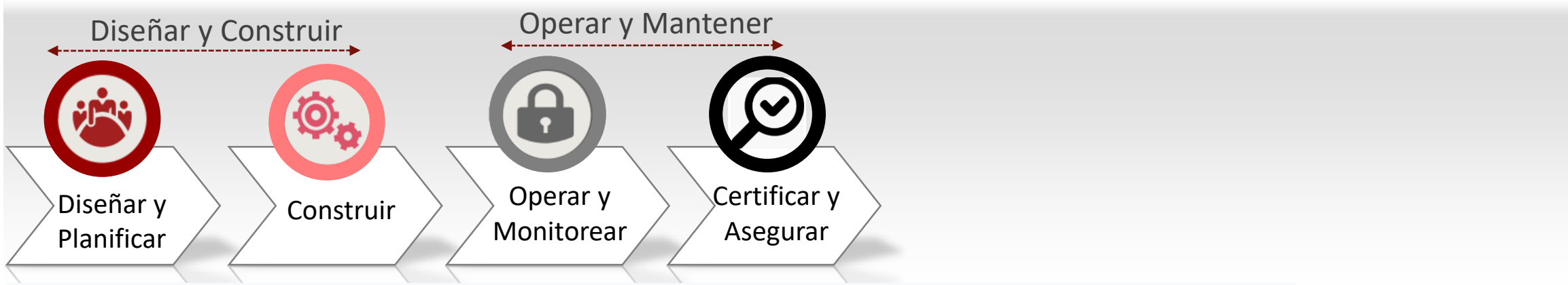
- Gestión de incidentes (preparación y respuesta)
- Mecanismos para identificar nuevos procesamientos y usos de datos personales y eventuales brechas
- Diseñar controles correspondientes

**9. Responsabilidad de Procesadores de datos**

- Definir requerimientos de privacidad p/ 3eros; identificar y mitigar eventuales riesgos
- Inventariar 3eros
- Validar mecanismos de acceso/transferencia de datos y ver cómo se refleja en los contratos

**10. Capacitación y Concientización**

- Inventariar quienes requieren este entrenamiento y definir los Planes




- Procedimientos de seguridad de la información (Seguridad IT)
- Notificación de violación de datos (Seguridad IT)
- Gestión y respuesta a incidentes (Seguridad IT)
- Respuesta ante acciones civiles y estatales (Seguridad IT)
- Estrategias de Encripción (Seguridad IT)
- Procedimientos de back up/ Recuperación de Desastres y Continuidad del Negocio (Seguridad IT)
- Procedimientos de control de acceso (IT)
- Gestión del ciclo de vida de los datos –Gobierno de datos (IT)
- Gestión de Registro ( evidencia de consentimiento y logs de actividad) (IT)
- Mantenimiento del inventario de actividades de sistemas y procesamiento (IT)
- Procedimientos de acceso y borrado de datos de parte de sus propietarios (IT)
- Participación en el Data Protection Impact Assesment (DPIA)

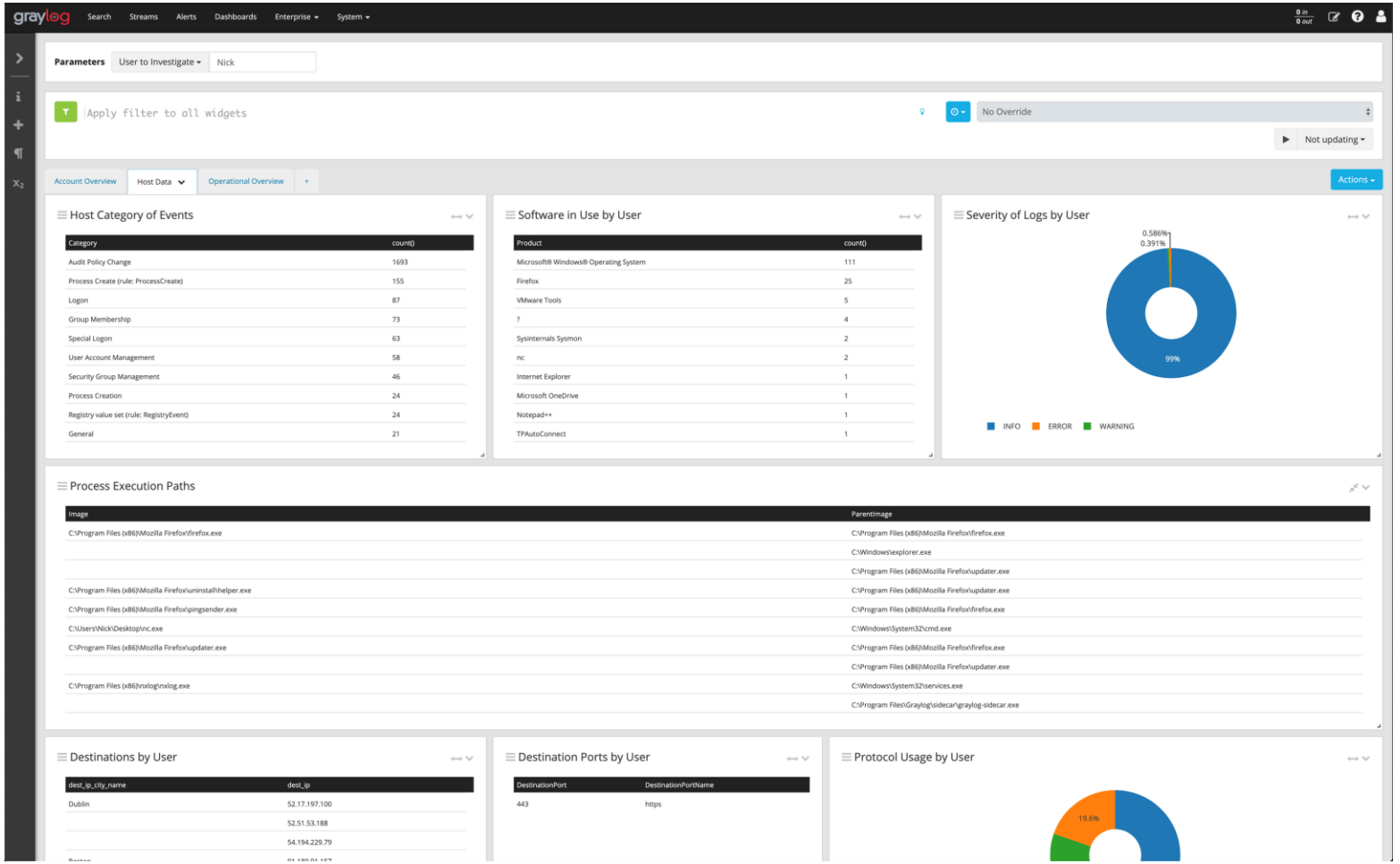
# Gestión de Incidentes


https://thehive-project.org/

# Gestión de Vulnerabilidades

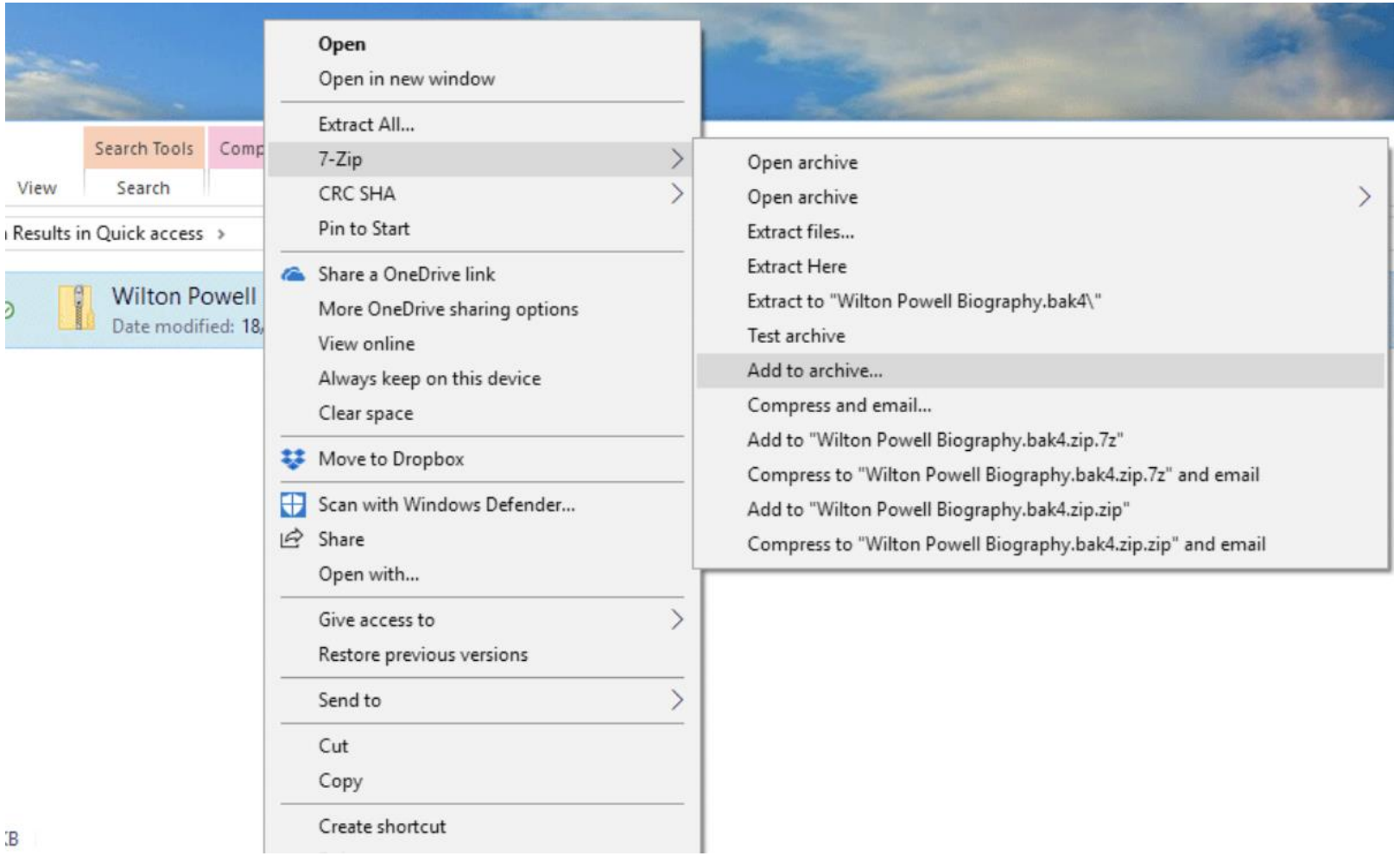

https://www.openvas.org/

# Gestión de Logs




https://www.graylog.org/

# Cifrado de archivos



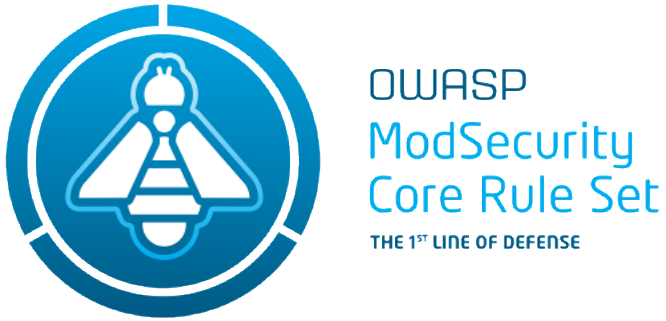
# Gestión de Passwords


## COMPARE SECRET SERVER EDITIONS

| Feature | Free |
| --- | --- |
| | 10 Users Limit |
| | 250 Secrets Limit |

https://thycotic.com/solutions/free-it-tools/secret-server-free/

# WAF


https://modsecurity.org/

https://owasp.org/www-project-modsecurity-core-rule-set/

# Conclusiones

- Controles de Acceso
- Análisis de Vulnerabilidades y Hacking Ético
- Certificaciones y Buenas Prácticas
- Planes de Respuesta y Gestión de Incidentes
- Responsabilidad en Licitaciones y Llamados

- Registro de Bases de Datos
- Plan de Educación de Delegados de Datos
- Plan de formación continuo de profesionales de Ciberseguridad
- Implementación de controles de Ciberseguridad de primer nivel conociendo tendencias del mercado como Gartner
- Existen alternativas abiertas a evaluar para cubrir el GAP de Seguridad.

# Muchas gracias!

*Graciela Ricci*

*Manuel de Campos*

*Mateo Martínez*