Tipología y Ciclo de Vida de los Datos: PRA2 - Limpieza y validación de los datos

Autores: Joel Bustos - Iván Ruiz

Junio 2020

Table of Contents

[Introducción 1](#_Toc41322277)

[Presentación. Práctica 2. 2](#_Toc41322278)

[1. Descripción del dataset. ¿Por qué es importante y qué pregunta/problema pretende resolver? 2](#_Toc41322279)

[2. Integración y selección de los datos de interés a analizar. 4](#_Toc41322280)

[• 2.1 Resumen de tratamientos previos 11](#_Toc41322281)

[• 2.2 Carga del nuevo archivo tras el preprocesado 13](#_Toc41322282)

[3. Limpieza de los datos. 17](#_Toc41322283)

[• 3.1 ¿Los datos contienen ceros o elementos vacíos? ¿Cómo gestionarías cada uno de estos casos? 17](#_Toc41322284)

[• 3.2 Identificación y tratamiento de valores extremos 17](#_Toc41322285)

[4. Análisis de los datos 36](#_Toc41322286)

[• 4.1 Selección de los grupos de datos que se quieren analizar/compararar (planificación de los análisis a aplicar) [Pendiente. Word de Joel] 36](#_Toc41322287)

[• 4.2 Análisis particulares, y comprobaciones de normalidad y distribución de la varianza en las variables bajo estudio 36](#_Toc41322288)

[5. Representación de los resultados a partir de tablas y gráficas 44](#_Toc41322289)

[6. Resolución del problema. A partir de los resultados obtenidos, ¿cuáles son las conclusiones? ¿Los resultados permiten responder al problema? 44](#_Toc41322290)

[Contribuciones 44](#_Toc41322291)

[Bibliografía 44](#_Toc41322292)

# Introducción

## Presentación. Práctica 2.

A lo largo de esta segunda práctica, vamos a tratar de profundizar en el análisis que los autores este trabajo planteamos en la primera parte de la asignatura. Así, hacemos referencia al repositorio que creamos y a la documentación generada durante el primer trabajo:

<https://github.com/iruiper/Cyberattacks-History>

En concreto, a pesar de las dificultades que plantea el set de datos sobre el que trabajaremos (y tal como expondremos a través de las distintas secciones), sí que nos gustaría tratar de cerrar las inquietudes y motivación que nos llevó en primera instancia a trabajar sobre la problemática de los ataques de ciberseguridad. En este sentido, nos gustaría iniciar esta segunda exposición rescatando la motivación que planteábamos en el proyecto de obtención de los datos:

*Los equipos de seguridad han necesitado incorporar, cada vez más, perfiles técnicos en el área de la ciberseguridad. Estos equipos técnicos, normalmente con un conocimiento muy específico, en ocasiones no disponen de demasiadas herramientas que les permitan ser proactivos y anticiparse a las nuevas tendencias y técnicas de ciberataque. De esta forma, acaban adaptando un comportamiento reactivo, realizando tareas de mantenimiento y de respuesta ante incidentes.*

*Nos planteábamos, como contexto para la presente práctica, recopilar datos históricos de ciberataques con el objetivo de crear un modelo predictivo que sirviese de soporte al equipo de seguridad de una empresa. Idealmente, estudiando lo que está ocurriendo en relación a delitos cibernéticos, los equipos internos de las distintas entidades, podrían tratar de prepararse mejor contra aquellos riesgos a los que los modelos estadísticos les pudieran sugerir que se encuentran más expuestos.*

Con ese punto de partida, como decimos, a continuación vamos a tratar de plantear un problema concreto que creemos que podría analizarse a través de los datos que hemos conseguido rascar del sitio web <https://www.hackmageddon.com/>.

Para abordar este segundo proyecto, veremos que los datos brutos extraídos durante la primera práctica conllevan retos y problemas iniciales, tales como la falta de agregación, limpieza y homogenización, o incluso la falta de variables relevantes para el análisis. Dado que, como decimos, hay carencias de calidad de datos de base, a pesar de que la propuesta de práctica se centra en tareas de limpieza y acondicionado mediante R, utilizaremos una combinación de Python y R por los motivos que iremos exponiendo en los distintos puntos del tratamiento de los datos.

# 1. Descripción del dataset. ¿Por qué es importante y qué pregunta/problema pretende resolver?

Tal y como explicábamos en la introducción anterior, disponemos de un set de datos con información histórica y clasificada sobre ataques cibernéticos con gran impacto que han producido desde el año 2017 hasta la actualidad. Con esta información, cabe preguntarse hasta qué punto podemos anticiparnos a los problemas que sobrevendrán a una entidad, o si estos datos pueden ayudar en asuntos financieros y presupuestarios para responder a preguntas tales como:

* ¿Hasta qué punto mi compañía se encuentra más expuesta a ciberataques por el sector en el que se encuentra?
* ¿Debería dotar presupuesto y medios adicionales en algún periodo particular del año?
* ¿Debería analizar la documentación cualitativa y los detalles técnicos de algún tipo de ataque particular que afecte a mi compañía?
* ¿Hasta qué punto el encontrarme en un mundo globalizado me expone a ataques internacionales?
* ¿Existen atacantes bien conocidos, con pautas concretas, a los que me encuentre particularmente expuesto?

Todas las preguntas anteriores están relacionadas con buena parte de la información que sí tenemos ya recabada a partir del set de datos en bruto que obtuvimos en durante la realización de la primera práctica:

* Disponemos de datos sobre las entidades o sectores afectados por los ciberataques que aparecen documentados en el dataset.
* Disponemos de la fecha en la que se han producido los distintos ataques.
* Sabemos si los ataques son de amplia cobertura, dado que sabemos si el ataque se produjo sobre un país concreto, o sobre la agrupación de varios de ellos.
* Sabemos qué ataques se encuentran bien documentados en cuanto a su origen (atacante identificado), versus ataques de difícil trazabilidad (atacante desconocido).
* Conocemos la tipología de ataque a que corresponden los distintos incidentes reportados.

En concreto, para que los resultados y los contrastes que llevemos a cabo sean lo más concretos y realistas posibles, vamos a centrarnos en el caso de que **formemos parte del equipo de seguridad de un organismo público**, por lo que nuestros análisis cuantitativos y cualitativos tratarán poner de relieve las diferencias entre nuestro sector y los demás. Esta distición también puede tener como derivada interesante, averiguar el nivel de gasto e inversión acometido por entidades de otros sectores en materia de ciberseguridad, y a partir de nuestra evaluación del riesgo específico, estudiar si puede ser necesaria la aplicación de nuevas partidas presupuestarias para la defensa contra estas amenazas.

Como hemos visto en los materiales didácticos de Subirats, Pérez y Calvo [1], existen muy diferentes retos a la hora de integrar y asegurar la calidad de los datos que necesitamos para dar repuesta a las inquietudes de cualquier analítica de datos. También, según se desprende de dicho material, y de los ejemplos basados en sets de datos estructurados, gran parte de los problemas vienen por los datos numéricos que se utilizan en los estudios. Sin embargo, la principal dificultad que ofrece el set de datos que hemos elegido es precisamente que lo que tenemos no son estadísticas numéricas o datos agregados, sino detalle de incidentes individuales. En consecuencia, gran parte del reto al que nos enfrentamos, y gran parte de los problemas de limpieza que vamos a desarrollar a lo largo de la práctica irán dirigidos a “crear” datos numéricos y estadísticos que permitan resolver las cuestiones sobre las que queremos obtener respuestas.

# 2. Integración y selección de los datos de interés a analizar.

El primer reto que deberemos resolver es precisamente la integración e incluso la creación de las variables numéricas que podrán ayudarnos a resolver las preguntas que nos hemos marcado como objetivo en la sección anterior. Si recordamos, como resultado de nuestra primera práctica, fuimos capaces de recopilar el detalle de incidentes reportados y analizados en el sitio web <https://www.hackmageddon.com/>.

No pretendemos repetir toda la exposición sobre el proceso de extracción, pero es importante explicar y entender que los datos recabados sufren gran heterogeneidad por los distintos motivos

* Los incidentes más actuales (año 2019 en adelante) se reportan mediante informes quincenales, con estructura específica.
* Los incidentes del año 2018 se encuentran agregados en forma tabular.
* Los incidentes del año 2017 se encuentran agregados en forma tabular, pero con formato distinto al año 2018.

En consecuencia, el primer problema con el que nos encontramos (antes incluso de poder generar variables numéricas que cuantifiquen el tipo de ataques), es que tenemos varior archivos csv para distintos periodos temporales, y que el formato de los campos en cada uno de ellos no tiene por qué ser necesariamente igual. A continuación vamos a recordar la estructura de campos del set de datos generado, y vamos a comprobarlo sobre una concatenación sin procesos de tratamiento o limpieza adicionales (llamaremos a este frame *attacks\_Raw*).

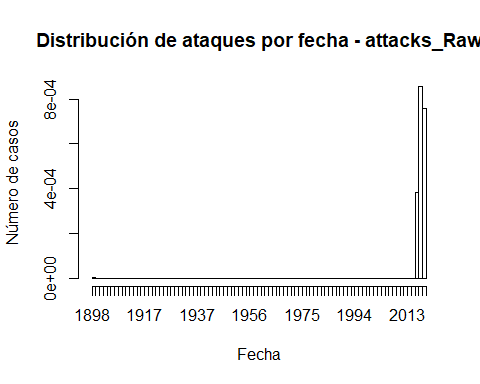
# Almacenamos el set de datos bruto en el frame "attacks\_Raw" para un análisis preliminar de algunos de los campos que utilizaremos  
attacks\_Raw <- read.csv2(file='DatosAtaques\_2017\_2020\_RAW.csv',stringsAsFactors = TRUE)  
  
# Mostramos la estructura del archivo recién cargado  
str(attacks\_Raw)

## 'data.frame': 4468 obs. of 11 variables:  
## $ ID : int 1 2 3 4 5 6 7 8 9 10 ...  
## $ Date : Factor w/ 1054 levels "01/01/2017","01/01/2018",..: 1 1 1 1 71 104 104 104 104 138 ...  
## $ Author : Factor w/ 564 levels ""," LulzSecITA",..: 17 7 166 7 38 7 289 7 7 186 ...  
## $ Target : Factor w/ 3518 levels ""," City of Del Rio",..: 2547 2954 1070 2743 1385 1417 1231 969 2080 2528 ...  
## $ Description : Factor w/ 4453 levels ""," Malaysia's Computer Emergency Response Team (MyCERT) reveal the details of a campaign carried out by APT40, ta"| \_\_truncated\_\_,..: 3591 3443 1072 4046 92 1412 1522 1040 3895 1885 ...  
## $ Attack : Factor w/ 327 levels "\"view as\" vulnerability",..: 3 280 220 177 91 177 97 177 9 263 ...  
## $ Target.Class: Factor w/ 25 levels "C Manufacturing",..: 13 2 13 16 13 13 7 16 15 23 ...  
## $ Attack.Class: Factor w/ 13 levels " CC",">1","CC",..: 4 6 3 3 10 4 3 3 3 4 ...  
## $ Country : Factor w/ 158 levels "",">1","AE","AF",..: 47 129 139 139 47 59 16 139 139 2 ...  
## $ Link : Factor w/ 1144 levels "","http://abcnews.go.com/Politics/fbi-probing-attempted-hack-trump-organization-officials/story?id=47652150",..: 268 174 68 714 1042 44 1032 724 815 69 ...  
## $ Tags : Factor w/ 927 levels "","#OpIsrael, #OpUSA, Anonymous",..: 352 831 213 754 381 556 456 261 582 245 ...

Observamos, ya sobre esta carga inicial, que tenemos varios problemas que resolver:

* Existen campos con mucha información cualitativa, pero que no resultan relevantes para el estudio de los problemas concretos que hemos marcado como objetivo. En consecuencia, podemos comenzar con procesos de **reducción de la dimensionalidad**, a través del descarte de aquellos atributos que no vamos a necesitar:
  + ID. Identificador único dentro de cada informe.
  + Target. Nombre concreto de la entidad atacada, pero nuestro estudio trata de agregar tipologías o sectores.
  + Description. Información de detalle de cada incidente, pero nuestro estudio debe agregar necesariamente tipos de ataques, por lo que el detalle individual no servirá a efectos estadísticos.
  + Attack. De manera análoga a “Description”, es un campo con información detallada sobre el tipo de ataque, pero utilizaremos tipologías agregadas para el análisis.
  + Link. Ofrece un enlace la URL en la que se puede estudiar el detalle que ofrece una noticia sobre el incidente reportado, pero no será de utilidad en el proyectos de explotación de datos que estamos planteando.
  + Tags. Contiene hashtags que resumen categorías, pero de nuevo ofrece información demasiado granular para el objetivo que nos hemos marcado.
* El campo fecha (**Date**) tiene un nivel de granularidad excesivo, ya que no resultará muy dificil encontrar varios ataques reportados en el mismo día. El nivel de granularidad que vamos a marcar para cada observación del set de datos será el número de ataques reportados en un mes concreto, por lo que será necesario separar este campo en dos: “Anyo” y “Mes”.
* Otro problema adicional de la fecha es que podría haberse registrado mal en origen. Podemos hacer un par de breves análisis sobre este campo, que nos confirmarán la necesidad de analizar y limpiar dicho campo:

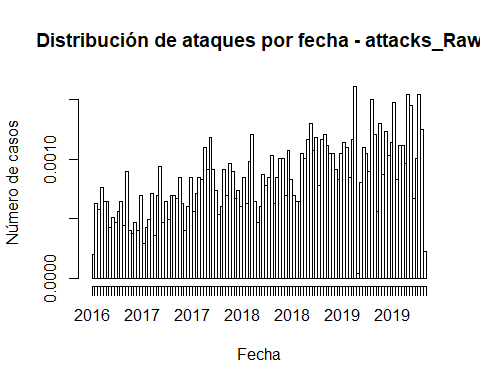
# Extracción y conversión del campo que registra la fecha del incidente  
fechas <- as.Date(attacks\_Raw$Date, format="%d/%m/%Y")  
  
# Análisis gráfico de la distribución de incidentes por fecha  
hist(fechas, breaks=100, main="Distribución de ataques por fecha - attacks\_Raw", xlab = "Fecha", ylab="Número de casos")



# Se observa que necesariamente hay valores erróneos (el típico registro de valor nulo y/o conversión a 01/01/1900). Veámoslo en modo tabla.  
table(format(fechas,"%Y"))

##   
## 1900 2017 2018 2019 2020   
## 4 951 1338 1693 482

# Analicemos de nuevo la distribución de casos por fecha si eliminamos los casos de 1900  
hist(fechas[format(fechas,"%Y")!="1900"], breaks=100, main="Distribución de ataques por fecha - attacks\_Raw", xlab = "Fecha", ylab="Número de casos")



* En relación al tipo de ataque (**Attack.Class**), lo que vamos a tratar de analizar es si hay alguna tipología de ataque concreto que afecte en mayor medida a nuestra entidad, o poder estudiar qué tipo de relación puede existir en cuestión de tendencias, correlación entre distintos tipos de ataques, etc. Para ello, nuestra propuesta consiste en la **creación de variables numéricas** que recojan el número de ataques por cada tipo, así como el número total de ataques por mes y año. Sin embargo, tenemos que analizar primero la calidad de datos de esta variable:

# Analizaremos la calidad de los datos de la variable Tipo de Ataque  
  
tipoAtaque <- attacks\_Raw$Attack.Class  
table(tipoAtaque)

## tipoAtaque  
## CC >1 CC CE   
## 1 1 1469 232   
## CW CW? Cyber Crime Cyber Espionage   
## 50 1 1094 172   
## Cyber Warfare H Hacktivism N/A   
## 33 58 38 5   
## Not Found   
## 1314

* Sobre la tabla anterior, observamos que necesitaremos tendremos que llevar a cabo algunas tareas:
* Homogenizar los valores. Vemos que encontramos tanto valores “Cyber Crime” como “CC”, o “Cyber Warfare” como “CW”. Deberemos acordar un criterio, que será el de las iniciales, y crearemos una estructura tipo *crosstab* [2] con la distribución de ataques por tipo, teniendo en cuenta que tendremos una observación por cada año, mes y tipo de entidad (comentaremos a continuación las particularidades que contempla el tipo de entidad).
* Vemos que hay valores atípicos como “>1” o “N/A”, que agruparemos en “Otros”.
* Observamos la existencia de **valores ausentes**. En los procesos de obtención de datos, es posible que se produzcan errores por distintos motivos, o que incluso en el propio informe de la web no se haya registrado ese dato. Sea por el motivo que sea, hay que tomar una decisión sobre qué hacer con dichos valores, como se nos indica en [1]. Una de las posibilidades pasaría por completar los datos manualmente, como indica Osborne [3], o volver a corregir las tareas del proceso de obtención (podría servir para mejora la calidad de los procesos de obtención de datos, corrigiendo o contemplando nuevas particularidadesd desde la fase de *scraping*).
* La manera de distinguir estos casos va a ser incluir estos ataques en la sección de “Otros”, pero utilizaremos también una variable dicotómica “ProblemasQC”, y que podremos incluso utilizar en nuestros análisis estadísticos para tratar de averiguar si las características de otras observaciones podrían ayudar a tomar una decisión sobre el tipo de ataque a que podría corresponder el valor que no pudo obtenerse.
* En relación al tipo de entidad (**Target.Class**), analizaremos con la misma metodología la necesidad de tener en cuenta algún tipo de consideración particular.

# Analizaremos la calidad de los datos de la variable Entidad Atacada  
  
tipoEntidad <- attacks\_Raw$Target.Class  
table(tipoEntidad)

## tipoEntidad  
## C Manufacturing   
## 82   
## D Electricity gas steam and air conditioning supply   
## 46   
## E Water supply, sewerage waste management, and remediation activities   
## 7   
## G Wholesale and retail trade   
## 86   
## H Transportation and storage   
## 38   
## I Accommodation and food service activities   
## 71   
## J Information and communication   
## 201   
## K Financial and insurance activities   
## 193   
## L Real estate activities   
## 4   
## M Professional scientific and technical activities   
## 68   
## N Administrative and support service activities   
## 33   
## Not Found   
## 1314   
## O Public administration and defence, compulsory social security   
## 263   
## O Public administration, defence, compulsory social security   
## 167   
## P Education   
## 201   
## Q Human health and social work activities   
## 281   
## R Arts entertainment and recreation   
## 119   
## S Other service activities   
## 57   
## U Activities of extraterritorial organizations and bodies   
## 25   
## V Fintech   
## 88   
## X Individual   
## 672   
## Y Multiple Industries   
## 352   
## Y Multiple targets   
## 78   
## Y Multiple Targets   
## 9   
## Z Unknown   
## 13

* Sobre la tabla anterior, observamos que necesitaremos tendremos que llevar a cabo algunas tareas:
* Existe un identificador único (Primera letra), que nos indica algún valor que no tiene exactamente el mismo texto. De hecho, el caso de la entidad que queremos analizar (organismos públicos) está afectada por este error de **calidad de los datos**: “O Public administration and defence, compulsory social security” y “O Public administration, defence, compulsory social security”. Será necesario, por tanto, tener en cuenta como identificador único la letra de la categoría, y utilizar un descriptivo único.
* Como decíamos anteriormente, vamos a considerar un caso como el número de ataques sufridos por un tipo de organismo por mes, por lo que necesitaremos que la estructura *crosstab* que utilicemos considere como claves de reparto del número de ataques estos tres atributos: **Anyo**, **Mes** y **TipoEntidad**.
* Volvemos a tener el problema de **valores perdidos**, que contienen el valor “Not Found”. De nuevo, utilizaremos la dicotómica “ProblemasQC” para conservar el número de casos, y tendremos que crear una entidad *dummy* que denominaremos “\_ Errores” (sustituimos la letra mayúscula de valor único por el caracter guión bajo).
* Al igual que comentábamos el caso de necesidad de homogenización en la entidad “O”, apreciamos que también es necesario hacer lo mismo en “Y”.
* En relación al autor (**Author**), dado el alto número de posibles valores (564 niveles, como veíamos anteriormente), lo que nos parece más interesante aquí es distinguir, en cada observación, distinguir cuántos de los ataques son de delincuentes u organizaciones bien identificadas, y cuántos corresponden a autores anónimos o desconocidos. Esta distinción podría ayudarnos a identificar si estamos más expuestos a ataques de redes conocidas, y por lo tanto dedicar recursos a analizar sus sistemas y tipos de ataques, o si necesitamos mecanismos de defensa mucho más heterogénos porque el número de atacantes diversos sea alto. Veamos cómo podríamos crear dos variables cuantitativas que recojan el **número de ataques de atacantes conocidos**, y **número de ataques de atacantes desconocidos**.

# Analizaremos la calidad de los datos de la variable Author  
head(sort(table(attacks\_Raw$Author), decreasing = T), n = 20)

##   
## ? Anonymous   
## 3612 25   
## Russia? APT28 AKA Fancy Bear   
## 15 14   
## China? TA505   
## 12 12   
## OurMine The Dark Overlord   
## 11 11   
## Turla   
## 10 9   
## Lazarus Group Magecart   
## 9 9   
## APT28 FIN7   
## 8 8   
## APT10 Gnosticplayers   
## 7 7   
## AnonPlus Hidden Cobra   
## 6 6   
## LulzSec ITA and AntiSec ITA MuddyWater   
## 6 6

* Sobre la tabla anterior, observamos que necesitaremos tener en cuenta las siguientes consideraciones:
* En la estructura *crosstab*, la variable “**CasosAutorDesconocido**” contendrá los casos para los casos “?” y " " de la tabla anterior.
* El resto de casos sí que tienen un valor asignado de autor conocido, por lo que el resto de autores sumarán en la variable “**CasosAutorConocido**”.
* Por último, en relación al país afectado (**Country**), observamos que el número de casos documentados es muy alto (158 niveles), por lo que hemos decidido que para el estudio que queremos hacer, será suficiente segmentar el número de casos de ámbito local, versus número de casos con impacto internacional. Para ello, vamos a crear una variable dicotómica “**ImpactoGlobal**” que nos diga si para el tipo de entidad, mes y año, se ha producido algún caso con impacto internacional (valor binario). Veamos a partir de los posibles valores de la variable país, cómo considerar ese valor verdadero o falso:

# Analizaremos la calidad de los datos de la variable Country  
head(sort(table(attacks\_Raw$Country), decreasing = T), n = 20)

##   
## US >1 UK CA IT AU IN RU KR N/A DE JP FR BR   
## 1594 1460 160 90 82 63 63 58 51 50 48 47 44 38 35   
## CN UA IL HK NL   
## 34 29 26 22 21

* A partir de la tabla anterior, consideraremos que ha habido casos de impacto internacional en cada registro que construyamos, si encontramos casos con país “>1” en la combinación Entidad/Año/Mes que compone cada observación.

# 2.1 Resumen de tratamientos previos

Como indicábamos en la sección introductoria, en el proyecto de limpieza de datos que hemos planteado, puede que uno de los principales retos con nuestro set de datos, sea precisamente todo lo relativo a **integración**, **selección**, **reducción** y **conversión** de datos, porque partimos de una situación en la que ni siquiera tenemos una información totalmente tabulada y con las variables cuantitativas que necesitaríamos para el estudio.

En consecuencia, y dado que resulta necesario dar un paso atrás, y combinar las fuentes “*raw*” que creamos en la primera práctica, hemos considerado más eficiente y eficaz llevar a cabo los preprocesamientos anteriores mediante Python y la fuente de datos “DatosAtaques\_2017\_2020\_RAW.csv” que consolida todos los archivos recreados mediante *scraping* en la primera práctica.

Tal y como subimos al GitHub, complementa al código dinámico de R que incluye el presente informe, el código “**XXX.py**” **[por desarrollar]**, que viene a tratar de resolver todos los problemas que hemos expuesto y analizado anteriormente. Como resultado, hemos generado el fichero que nos acompañará en el resto del estudio, y que denominamos “**EstadisticasAtaques2017\_2020\_Input.csv**” **pendiente de crear**

Como hemos comentado anteriormente, las variables que componen cada observación del dataset que utilizaremos para limpiar y analizar son las siguientes *modificar con lo que finalmente componga el set de datos que genera Joel con Python*:

* **Anyo**. Año en el que se se documenta el número de ataques que recoge la observación.
* **Mes**. Mes en el que se se documenta el número de ataques que recoge la observación.
* **Entidad**. Tipo de entidad para la que se documenta el número de ataques, fabricada a partir de la variable original “Target.Class”.
* **ImpactoGlobal**. Variable dicotómica, verdadero o falso, indica si en ese tipo de entidad, en el mes y año correspondiente, se han producido ataques de impacto internacional. Atributo creado a partir de la variable original “Country”.
* **CasosAutorConocido**. Número de ataques con autor conocido e identificable que se han producido para ese tipo de entidad, en el mes y año correspondiente. Variable creada a partir de la variable original “Author”.
* **CasosAutorDesconocido**. Número de ataques con autor desonocido e identificable que se han producido para ese tipo de entidad, en el mes y año correspondiente. Variable creada a partir de la variable original “Author”.
* **AtaquesCC**. Número de ataques de tipo “Cyber Crime” que se han producido que se han producido para ese tipo de entidad, en el mes y año correspondiente. Variable creada a partir de conteo de casos, a través de la variable original “Attack.Class”.
* **AtaquesCE**. Número de ataques de tipo “Cyber Espionage” que se han producido que se han producido para ese tipo de entidad, en el mes y año correspondiente. Variable creada a partir de conteo de casos, a través de la variable original “Attack.Class”.
* **AtaquesCW**. Número de ataques de tipo “Cyber Warfare” que se han producido que se han producido para ese tipo de entidad, en el mes y año correspondiente. Variable creada a partir de conteo de casos, a través de la variable original “Attack.Class”.
* **AtaquesH**. Número de ataques de tipo “Hacktivism” que se han producido que se han producido para ese tipo de entidad, en el mes y año correspondiente. Variable creada a partir de conteo de casos, a través de la variable original “Attack.Class”.
* **AtaquesOtros**. Número de ataques de tipo “Otros” (valores “N/A”, “>1” o “Not Found”) que se han producido que se han producido para ese tipo de entidad, en el mes y año correspondiente. Variable creada a partir de conteo de casos, a través de la variable original “Attack.Class”.
* **AtaquesTotal**. Número de ataques de tipo “Cyber Crime” que se han producido que se han producido para ese tipo de entidad, en el mes y año correspondiente. Variable creada a partir de conteo de casos, a través de la variable original “Attack.Class”.
* **ProblemasQC**. Identificador que señala si la observación concreta ha tenido problemas de calidad identificados en la etapa de generación de la información. Nos indica que los valores cuantificados pueden ser imprecisos, estar clasificados en categorías genéricas, o en entidades no identificadas.

# 2.2 Carga del nuevo archivo tras el preprocesado

Como hemos referido anteriormente, las extracciones en bruto de que disponíamos, no ofrecían un formato ni estructura adecuados para los objetivos del estudio, por lo que ha sido necesario dar un paso atrás y llevar a cabo tareas preliminares de limpieza y acondicionamiento desde el propio origen de los datos. Como hemos explicado, para ello ha resultado más eficiente y eficaz realizar algunas de estas tareas como mejora/modificación de los *scripts* desarrollados en la primera práctica. Y a tal efecto incluimos el código “**XXX.py**” **[por desarrollar]** en GitHub.

A continuación cargaremos el nuevo fichero de *input*, y explicaremos brevemente cómo vamos a avanzar en las siguientes secciones con dichos datos.

# Almacenamos el nuevo set de datos en el frame "attacks\_Input" para una validación adicional, y para explicar algunos de los tratamientos que llevaremos a cabo a lo largo del análisis  
attacks\_Input <- read.csv2(file='processed\_data.csv',stringsAsFactors = TRUE)  
attacks\_Input$Year <- as.factor(attacks\_Input$Year)  
attacks\_Input$Mes <- as.factor(attacks\_Input$Mes)  
  
# Creamos una nueva variable con el número total de ataques por observación  
attacks\_Input$NumeroAtaques <- attacks\_Input$Code\_attack\_class\_.1+attacks\_Input$Code\_attack\_class\_CC+attacks\_Input$Code\_attack\_class\_CE+attacks\_Input$Code\_attack\_class\_CW+attacks\_Input$Code\_attack\_class\_H+attacks\_Input$Code\_attack\_class\_UK  
  
# Mostramos la estructura del archivo recién cargado  
str(attacks\_Input)

## 'data.frame': 1748 obs. of 16 variables:  
## $ Year : Factor w/ 4 levels "2017","2018",..: 1 1 1 1 1 1 1 1 1 1 ...  
## $ Mes : Factor w/ 12 levels "1","2","3","4",..: 1 1 1 1 1 1 1 1 1 1 ...  
## $ Continent : Factor w/ 7 levels "África","América",..: 2 2 2 2 2 2 2 2 2 2 ...  
## $ Country\_name : Factor w/ 112 levels "Afganistán","Alemania",..: 15 15 18 33 33 33 33 33 33 33 ...  
## $ Code\_target\_class : Factor w/ 21 levels "C","D","E","G",..: 7 21 13 1 6 7 10 11 12 13 ...  
## $ Desc\_target\_class : Factor w/ 21 levels "Accommodation and food service activities",..: 11 19 5 12 1 11 15 3 16 5 ...  
## $ ProblemasQC : logi FALSE FALSE FALSE FALSE FALSE FALSE ...  
## $ Author\_processed\_Conocido : int 1 0 0 0 0 1 0 0 1 0 ...  
## $ Author\_processed\_Desconocido: int 0 1 1 3 3 5 1 1 4 10 ...  
## $ Code\_attack\_class\_.1 : int 0 0 0 0 0 0 0 0 0 0 ...  
## $ Code\_attack\_class\_CC : int 1 1 1 3 3 6 1 1 5 10 ...  
## $ Code\_attack\_class\_CE : int 0 0 0 0 0 0 0 0 0 0 ...  
## $ Code\_attack\_class\_CW : int 0 0 0 0 0 0 0 0 0 0 ...  
## $ Code\_attack\_class\_H : int 0 0 0 0 0 0 0 0 0 0 ...  
## $ Code\_attack\_class\_UK : int 0 0 0 0 0 0 0 0 0 0 ...  
## $ NumeroAtaques : int 1 1 1 3 3 6 1 1 5 10 ...

Podemos hacer una comprobación sobra una de las variables más relevantes para nuestros análisis numéricos: el número de ataques totales que estamos analizando, y segmentados en las distintas categorías de ataques que nos indica el atributo original “Attack.Class”.

# Análisis de integridad en la carga: comprobación de la completitud del dataset y la consistencia entre variables numéricas.  
  
colSums(attacks\_Input[7:15])

## ProblemasQC Author\_processed\_Conocido   
## 228 785   
## Author\_processed\_Desconocido Code\_attack\_class\_.1   
## 3899 2   
## Code\_attack\_class\_CC Code\_attack\_class\_CE   
## 2786 468   
## Code\_attack\_class\_CW Code\_attack\_class\_H   
## 104 1206   
## Code\_attack\_class\_UK   
## 118

cat("Suma del número de ataques por categoría: ",sum(colSums(attacks\_Input[8:15])[3:8]),"\n")

## Suma del número de ataques por categoría: 4684

cat("Suma del número de ataques de acuerdo a si se conoce el atacante: ",sum(colSums(attacks\_Input[8:15])[1:2]),"\n")

## Suma del número de ataques de acuerdo a si se conoce el atacante: 4684

cat("Valor acumulado en la variable NumeroAtaques: ",sum(attacks\_Input$NumeroAtaques))

## Valor acumulado en la variable NumeroAtaques: 4684

Con lo anterior, ya podemos considerar que tenemos un primer set de datos completo, y limpio de errores de procesamiento, aunque deberemos acabar de analizar si existen otros problemas de valores extremos a lo largo de la siguiente sección. No obstante, gracias al trabajo de preprocesamiento, hemos conseguido resolver algunos problemas importantes:

* Hemos llevado a cabo tareas de acondicionamiento para poder disponer de cuantificaciones basadas en Año/Mes/País/Entidad.
* Como veíamos al principio del análisis, teníamos muchísimas observaciones que constituían valores perdidos, por fallos en el proceso de extracción. Gracias a los **mecanismos de control de errores y de control de calidad** que hemos desarrollado en la primera práctica y que hemos complementado en la presente, conseguimos de alguna manera la mejor solución al caso de datos perdidos: recuperarlos manualmente. En esta ocasión el proceso no es del todo manual, sino que consiste en volver a ejecutar el *scraper* en los informes que había fallado, y de este modo completamos los datos que aparecían como “Not Found”.
* Mostramos a continuación un ejemplo del archivo de *log* generado en el proceso de rascado de datos, que ha permitido identificar aquellos casos en los que no se estaban leyendo todos los incidentes disponibles en el informe (resaltado sobre la captura algún ejemplo).
* Como resultado, no solo corregimos los valores ausentes, sino que hemos conseguido aumentar el número de casos a considerar en el análisis, desde los 4.468 de que disponíamos en el archivo inicial “DatosAtaques\_2017\_2020\_RAW.csv”, hasta los 4.684 que hemos conseguido recuperar tras el rascado adicional de los informes con error.
* Con el preprocesamiento hemos conseguido también reducir el número de errores en la identificación del tipo de ataque (inicialmente teníamos 1.314 casos “Not found”, y ahora tenemos únicamente 118 ataques documentados como “Unknown”.)
* Para el caso de las entidades, sigue habiendo ciertos problemas que no se han podido resolver en el preprocesamiento, pero al menos hemos podido identificarlos claramente, y podremos utilizarlos en nuestros análisis, siempre que tengamos la cautela de que son casos para los que se desconoce el tipo de entidad (inicialmente teníamos 1.314 casos “Not found”, y ahora tenemos 295 casos, pero que siguen correspondiendo a un número de ataques, 1.397, muy similar al que se apreciaba inicialmente como observamos en la consulta siguiente.)

# Analizaremos la calidad de los datos de la variable Entidad Atacada tras las tareas de preprocesamiento  
  
tipoEntidad <- attacks\_Input$Desc\_target\_class  
table(tipoEntidad)

## tipoEntidad  
## Accommodation and food service activities   
## 46   
## Activities of extraterritorial organizations and bodies   
## 25   
## Administrative and support service activities   
## 29   
## Arts entertainment and recreation   
## 81   
## Education   
## 71   
## Electricity gas steam and air conditioning supply   
## 43   
## Financial and insurance activities   
## 138   
## Fintech   
## 78   
## Human health and social work activities   
## 77   
## Individual   
## 169   
## Information and communication   
## 118   
## Manufacturing   
## 59   
## Multiple Industries   
## 104   
## Other service activities   
## 52   
## Professional scientific and technical activities   
## 51   
## Public administration and defence, compulsory social security   
## 227   
## Real estate activities   
## 6   
## Transportation and storage   
## 34   
## Unknown   
## 276   
## Water supply, sewerage waste management, and remediation activities   
## 6   
## Wholesale and retail trade   
## 58

colSums(attacks\_Input[attacks\_Input$Desc\_target\_class=="Unknown",8:16])

## Author\_processed\_Conocido Author\_processed\_Desconocido   
## 216 1181   
## Code\_attack\_class\_.1 Code\_attack\_class\_CC   
## 1 97   
## Code\_attack\_class\_CE Code\_attack\_class\_CW   
## 59 18   
## Code\_attack\_class\_H Code\_attack\_class\_UK   
## 1104 118   
## NumeroAtaques   
## 1397

# 3. Limpieza de los datos.

# 3.1 ¿Los datos contienen ceros o elementos vacíos? ¿Cómo gestionarías cada uno de estos casos?

# 3.2 Identificación y tratamiento de valores extremos

Como hemos visto en secciones anteriores, gran parte de las variables o atributos que utilizamos en nuestro estudio son cualitativas, por lo que los principales retos a resolver en dichos casos ya se han tratado en las tareas de preprocesamiento y de de tratamiento de elementos ausentes. En realidad, cuando hablamos de valores extremos o outliers, las variables que pueden sufrir este problema son las variables cuantitativas. De hecho, según la definición de Subirats, Pérez y Calvo [1], “son observaciones que se desvían tanto del resto, que levantan sospechas sobre si fueron generadas mediante el mismo mecanismo”. En nuestro set de datos, teniendo en cuanta que las variables numéricas han tenido que ser construidas directamente por nosotros, en realidad no existe el problema de que el cálculo sea heterogéneo. Sin embargo, sí que sigue existiendo la posibilidad de que al cuantificar los incidentes individuales, sigamos teniendo una cuantificación de datos que pueda suponer algún problema en el resto del análisis, por lo que procederemos a estudiarlo.

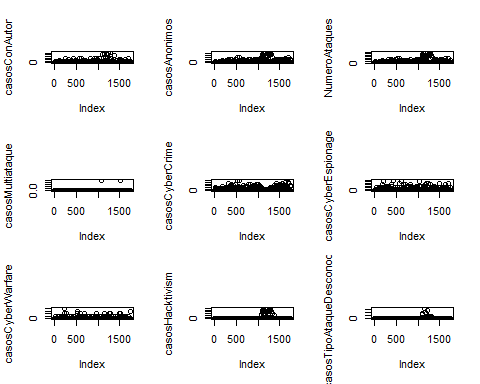
En primer lugar, y vamos a ir anticipando algunos asuntos que será necesario explicar en la sección 4, en realidad las preguntas que nos estamos haciendo en el caso real que estamos planteando, requieren poner el foco en distintas dimensiones del set de datos (por tipo de entidad afectada, por dimensión geográfica, por dimensión temporal, etc.), por lo que algunas de las variables cuantitativas que utilizaremos para dar respuesta a las distintas preguntas puede que requieran procesos de agregación, y que en consecuencia los valores concretos que tomen las variables agregadas requieran de anális o tratamiento particular. De todos modos, en caso de que resulte necesario algún proceso de agregacion específico, lo justificaremos y explicaremos en la sección correspondiente. Para el resto de esta subsección consideraremos el caso de observaciones/casos cuantificados por la combinación de Año/Mes/Entidad/Pais. Para cada una de esas observaciones, disponemos de las siguientes variables numéricas:

* Author\_processed\_Conocido: Número de casos observados con autor reconocido y documentado. En el análisis renombraremos la variable como “casosConAutor”.
* Author\_processed\_Desconocido: Número de casos observados con autor no identificado, y para los cuales resultaría por lo tanto mucho más difícil analizar patrones o reincidencia de algún tipo por autor. En el análisis renombraremos la variable como “casosAnonimos”
* NumeroAtaques: Número total de incidentes de seguridad o ataques que se han documentado para la selección Año/Mes/Entidad/País.
* Code\_attack\_class\_.1: Número de incidentes con más de un tipo de ataque empleado. En el análisis renombraremos la variable como “casosMultiataque”
* Code\_attack\_class\_CC: Número de incidentes de tipo “Cyber Crime”. En el análisis renombraremos la variable como “casosCyberCrime”
* Code\_attack\_class\_CE: Número de incidentes de tipo “Cyber Espionage”. En el análisis renombraremos la variable como “casosCyberEspionage”
* Code\_attack\_class\_CW: Número de incidentes de tipo “Cyber Warfare”. En el análisis renombraremos la variable como “casosCyberWarfare”
* Code\_attack\_class\_H: Número de incidentes de tipo “Hacktivism”. En el análisis renombraremos la variable como “casosHacktivism”
* Code\_attack\_class\_UK: Número de incidentes de tipo “Unknown”. En el análisis renombraremos la variable como “casosTipoAtaqueDesconocido”

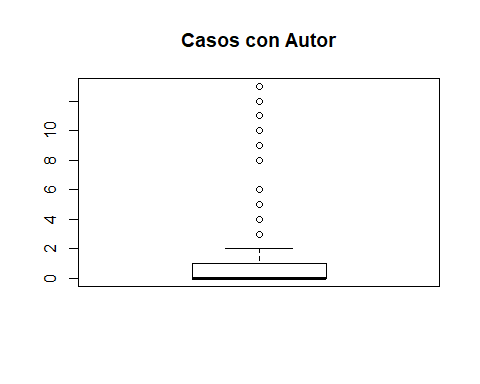
# Creación de las variables anteriores  
  
casosConAutor <- attacks\_Input$Author\_processed\_Conocido  
casosAnonimos <- attacks\_Input$Author\_processed\_Desconocido  
NumeroAtaques <- attacks\_Input$NumeroAtaques  
casosMultiataque <- attacks\_Input$Code\_attack\_class\_.1  
casosCyberCrime <- attacks\_Input$Code\_attack\_class\_CC  
casosCyberEspionage <- attacks\_Input$Code\_attack\_class\_CE  
casosCyberWarfare <- attacks\_Input$Code\_attack\_class\_CW  
casosHacktivism <- attacks\_Input$Code\_attack\_class\_H  
casosTipoAtaqueDesconocido <- attacks\_Input$Code\_attack\_class\_UK

En primer lugar, vamos a ver, mediante gráficos de dispersión, boxplot e histogramas, si encontramos valores extremos para alguna de ellas.

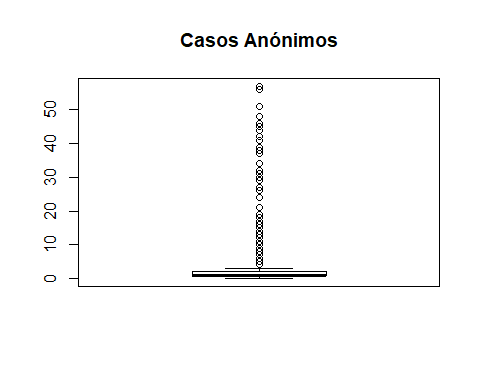
# Representación de los gráficos de dispersión de valores  
  
par(mfrow=c(3,3))   
  
plot(casosConAutor)  
plot(casosAnonimos)  
plot(NumeroAtaques)  
plot(casosMultiataque)  
plot(casosCyberCrime)  
plot(casosCyberEspionage)  
plot(casosCyberWarfare)  
plot(casosHacktivism)  
plot(casosTipoAtaqueDesconocido)



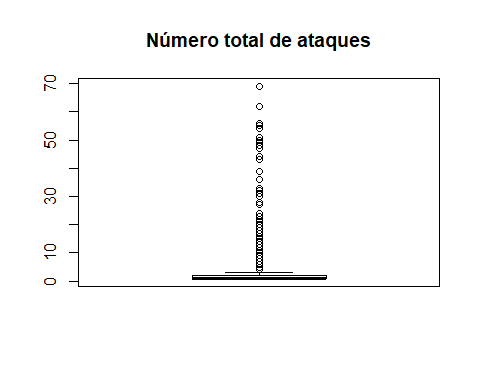
# Representación de los boxplot para las variables numéricas  
  
boxplot(casosConAutor, main="Casos con Autor")



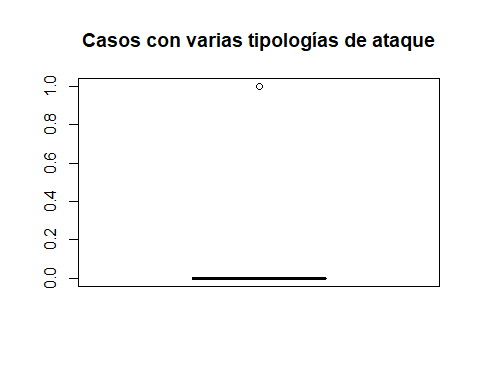
boxplot(casosAnonimos, main="Casos Anónimos")



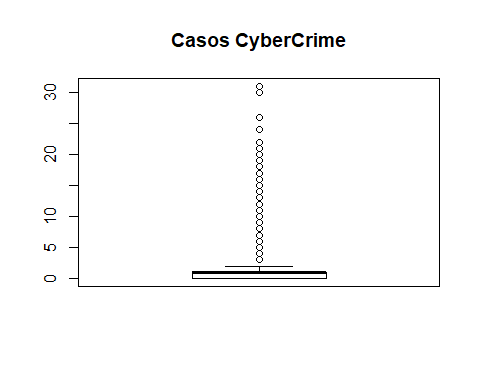
boxplot(NumeroAtaques, main="Número total de ataques")



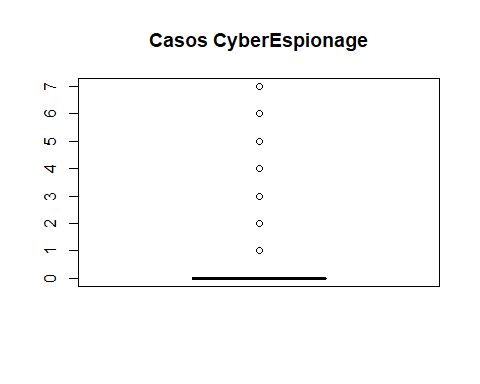
boxplot(casosMultiataque, main="Casos con varias tipologías de ataque")



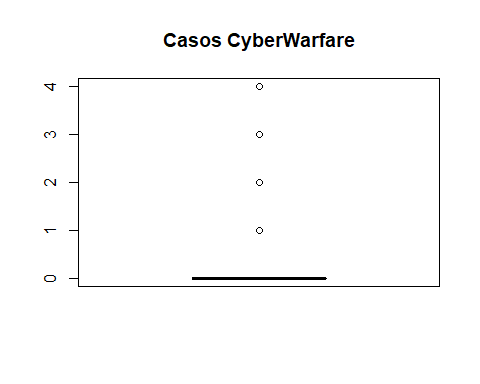
boxplot(casosCyberCrime, main="Casos CyberCrime")



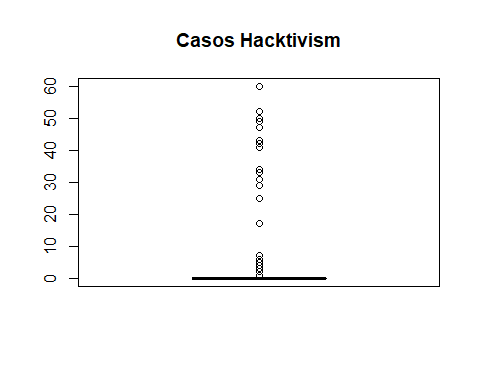
boxplot(casosCyberEspionage, main="Casos CyberEspionage")



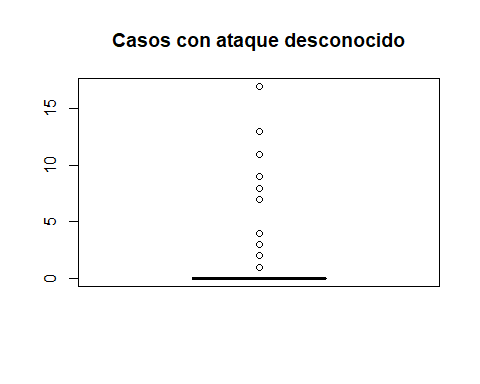
boxplot(casosCyberWarfare, main="Casos CyberWarfare")



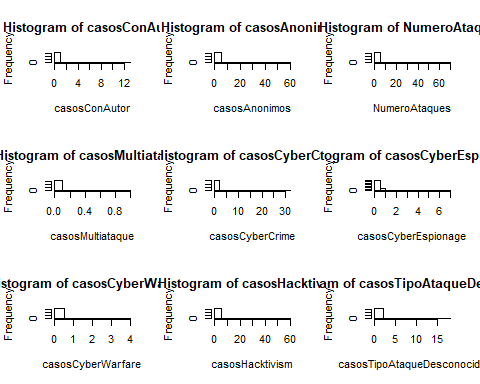
boxplot(casosHacktivism, main="Casos Hacktivism")



boxplot(casosTipoAtaqueDesconocido, main="Casos con ataque desconocido")



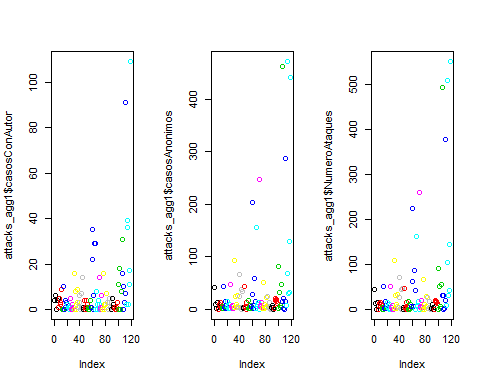
# Representación de los histogramas para las variables numéricas  
  
par(mfrow=c(3,3)) # Establecemos gráficos 3x3  
  
hist(casosConAutor)  
hist(casosAnonimos)  
hist(NumeroAtaques)  
hist(casosMultiataque)  
hist(casosCyberCrime)  
hist(casosCyberEspionage)  
hist(casosCyberWarfare)  
hist(casosHacktivism)  
hist(casosTipoAtaqueDesconocido)



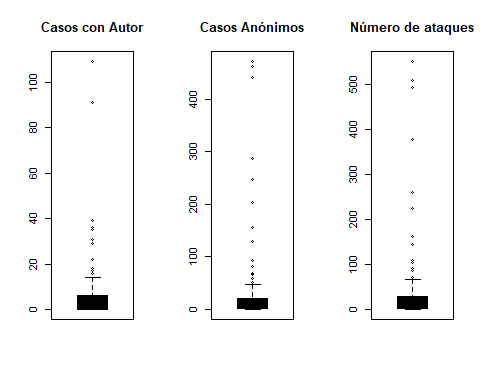
Como anticipábamos antes de llevar a cabo el análisis gráfico, en realidad lo que está ocurriendo es que el grado de granularidad elegido para los casos, basado en hasta cuatro variables cualitativas (Año, Mes, Entidad y País), nos lleva a una distribución de valores de número de ataques por observación muy bajo. Esto justifica plenamente que los análisis que vayamos a hacer por las distintas dimensiones, necesariamente tengan que agregar en un máximo de 3 dimensiones de las anteriores. Un primer intento de reducción de la dimensionalidad se ha llevado a cabo ya en las tareas de preprocesamiento, consiguiendo traducir los códigos de país a los países que corresponde, para a continuación agregar por continente, y así poder hacer el análisis geográfico reduciendo el número de niveles de 158 países, a 7 zonas (5 continentes + desconocido + incidente global).

Aunque, como decimos, estas agregaciones podrán depender del análisis concreto que vayamos a hacer, vamos a analizar, para valorar la utilidad de los mecanismos de agregación, la comparación de los gráficos anteriores, con los que obtendríamos de un nuevo nivel de consideración de casos basado en Entidad y Continente. Para profundizar en la utilidad y mecanismos de agregación, hemos seguido el sistema de trabajo propuesto en [3].

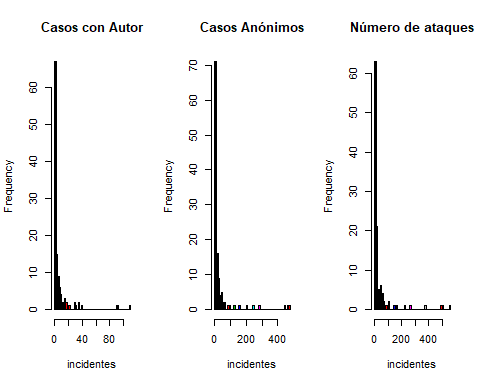
# En primer lugar necesitaremos reconstruir la agregación de datos considerando las cuatro variables cualitativas seleccionadas. El cambio principal con respecto al set de datos inicial es el cambio en la dimensión geográfica de país a continente  
  
library("dplyr") # Librería que utilizaremos para las tareas de agregación [3]  
  
attacks\_agg1 <- attacks\_Input %>% group\_by(Code\_target\_class, Desc\_target\_class, Continent) %>% summarize(NumeroAtaques=sum(NumeroAtaques),casosConAutor=sum(Author\_processed\_Conocido),casosAnonimos=sum(Author\_processed\_Desconocido))  
  
# Representación de los gráficos de dispersión de valores  
  
par(mfrow=c(1,3))   
  
plot(attacks\_agg1$casosConAutor, col=attacks\_agg1$Code\_target\_class)  
plot(attacks\_agg1$casosAnonimos, col=attacks\_agg1$Code\_target\_class)  
plot(attacks\_agg1$NumeroAtaques, col=attacks\_agg1$Code\_target\_class)



# Representación de los boxplot para las variables numéricas  
  
par(mfrow=c(1,3))   
  
boxplot(attacks\_agg1$casosConAutor, col=attacks\_agg1$Code\_target\_class, main="Casos con Autor")  
boxplot(attacks\_agg1$casosAnonimos, col=attacks\_agg1$Code\_target\_class, main="Casos Anónimos")  
boxplot(attacks\_agg1$NumeroAtaques, col=attacks\_agg1$Code\_target\_class, main="Número de ataques")



# Representación de los histogramas para las variables numéricas  
  
par(mfrow=c(1,3))   
  
hist(attacks\_agg1$casosConAutor, col=attacks\_agg1$Code\_target\_class, breaks = 50,main="Casos con Autor", xlab="incidentes")  
hist(attacks\_agg1$casosAnonimos, col=attacks\_agg1$Code\_target\_class, breaks = 50, main="Casos Anónimos", xlab="incidentes")  
hist(attacks\_agg1$NumeroAtaques, col=attacks\_agg1$Code\_target\_class, breaks = 50, main="Número de ataques", xlab="incidentes")



En este caso, para la agregación concreta que queríamos analizar, hemos reducido el número de variables a analizar para no sobrecargar el informe de gráficos, y para los datos de ataques, consideramos únicamente el número total de ataques en lugar de por casuística.

En cualquier caso, seguimos observando valores muy alejados, por lo que hemos querido ver de manera visual si pueden estar correspondiendo a tipologías de entidades concretas. Así se confirma, viendo valores alejados principalmente para 3 colores distintos. Vamos a ver en modo tabla a qué valores corresponden, a través por ejemplo del número total de ataques.

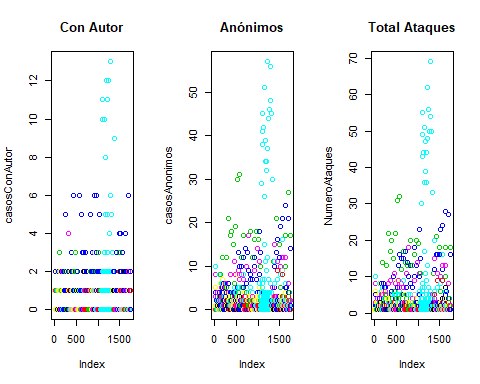
# Análisis de entidades que ocasionan valores extremos  
  
temp <- attacks\_agg1 %>% group\_by(Code\_target\_class, Desc\_target\_class) %>% summarize(sum(NumeroAtaques))  
temp2 <- as.data.frame(temp)  
head(temp2[order(-temp2$`sum(NumeroAtaques)`),])

## Code\_target\_class  
## 21 Z  
## 19 X  
## 20 Y  
## 12 O  
## 14 Q  
## 7 J  
## Desc\_target\_class  
## 21 Unknown  
## 19 Individual  
## 20 Multiple Industries  
## 12 Public administration and defence, compulsory social security  
## 14 Human health and social work activities  
## 7 Information and communication  
## sum(NumeroAtaques)  
## 21 1397  
## 19 704  
## 20 468  
## 12 443  
## 14 300  
## 7 204

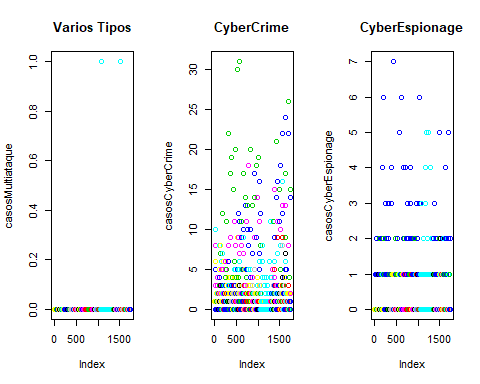
Se aprecia que, efectivamente, los casos que hemos clasificado como desconocidos por errores de lectura o captura de datos, así como los valores de individuos particulares o múltiples sectores, en realidad están introduciendo un ruido que hace incomparables los valores entre unos y otros sectores. Seguramente la mejor decisión que deberemos tomar para estos valores es excluirlos de los análisis sectoriales, o incluso tratar de reasignar los valores desconocidos a alguno de los otros tipos de entidades. Comentaremos más sobre este aspecto en la sección 4 de análisis.

Por el momento, como último análisis visual, vamos a presentar los gráficos por casos iniciales, con la agrupación con máxima granularidad que venimos trabajando (Año, Mes, Entidad y País), con y sin la consideración de los valores que hemos identificado como causantes de las anomalías.

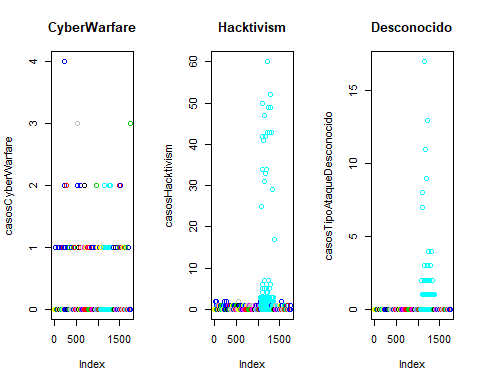
# Representación de los gráficos de dispersión de valores  
  
par(mfrow=c(1,3))   
  
plot(casosConAutor, col=attacks\_Input$Code\_target\_class, main = "Con Autor")  
plot(casosAnonimos, col=attacks\_Input$Code\_target\_class, main = "Anónimos")  
plot(NumeroAtaques, col=attacks\_Input$Code\_target\_class, main = "Total Ataques")



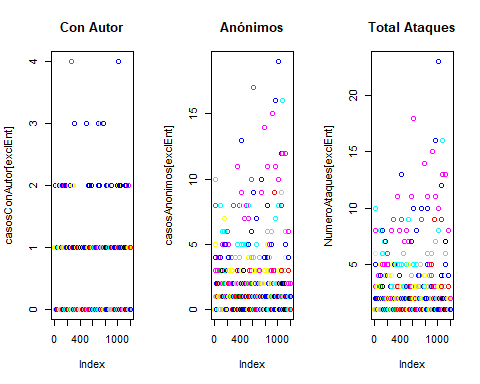
plot(casosMultiataque, col=attacks\_Input$Code\_target\_class, main="Varios Tipos")  
plot(casosCyberCrime, col=attacks\_Input$Code\_target\_class, main="CyberCrime")  
plot(casosCyberEspionage, col=attacks\_Input$Code\_target\_class, main="CyberEspionage")



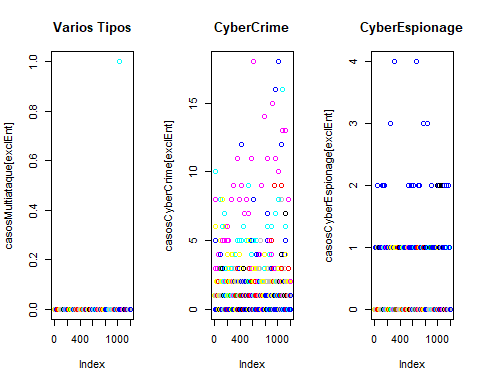
plot(casosCyberWarfare, col=attacks\_Input$Code\_target\_class, main="CyberWarfare")  
plot(casosHacktivism, col=attacks\_Input$Code\_target\_class, main="Hacktivism")  
plot(casosTipoAtaqueDesconocido, col=attacks\_Input$Code\_target\_class, main="Desconocido")



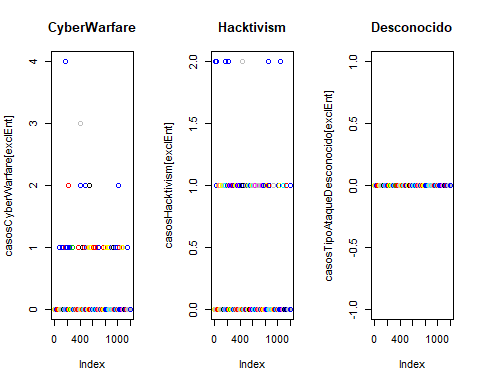
# Representación de los gráficos de dispersión de valores, excluyendo las entidades que generan valores extremos  
  
par(mfrow=c(1,3))   
  
exclEnt <- attacks\_Input$Code\_target\_class!="X" & attacks\_Input$Code\_target\_class!="Y" & attacks\_Input$Code\_target\_class!="Z"  
  
plot(casosConAutor[exclEnt], col=attacks\_Input$Code\_target\_class[exclEnt], main = "Con Autor")  
plot(casosAnonimos[exclEnt], col=attacks\_Input$Code\_target\_class[exclEnt], main = "Anónimos")  
plot(NumeroAtaques[exclEnt], col=attacks\_Input$Code\_target\_class[exclEnt], main = "Total Ataques")



plot(casosMultiataque[exclEnt], col=attacks\_Input$Code\_target\_class[exclEnt], main="Varios Tipos")  
plot(casosCyberCrime[exclEnt], col=attacks\_Input$Code\_target\_class[exclEnt], main="CyberCrime")  
plot(casosCyberEspionage[exclEnt], col=attacks\_Input$Code\_target\_class[exclEnt], main="CyberEspionage")



plot(casosCyberWarfare[exclEnt], col=attacks\_Input$Code\_target\_class[exclEnt], main="CyberWarfare")  
plot(casosHacktivism[exclEnt], col=attacks\_Input$Code\_target\_class[exclEnt], main="Hacktivism")  
plot(casosTipoAtaqueDesconocido[exclEnt], col=attacks\_Input$Code\_target\_class[exclEnt], main="Desconocido")



De todo lo anterior, podemos extraer varias conclusiones muy interesantes sobre la presencia de valores extremos:

* Comprobamos que, efectivamente, las categorías X, Y, Z de tipos de entidad, constituyen casos particulares a considerar separadamente. En concreto, el valor “Unknown” no debería contemplarse de ningún modo en aquellos análisis que consideren un atributo relevante el tipo de entidad, ya que pueden incluir valores agregados de otros tipos de entidades, y en consecuencia generan valores extremos.
* Observamos que la tipología de ataques “Multiataque” tiene un único valor espúreo, siendo siempre 0, por lo que constituye una variable que puede omitirse sin pérdida de generalidad.
* Vemos que una vez excluidas las categorías X, Y, Z, no existen observaciones con tipo de ataque desconocido, por lo que ambas variables vienen a recoger los valores perdidos.
* Con todas las consideraciones anteriores, venimos a observar que el número de casos muestra una distribución de valores con una larga cola a derechas, o lo que es lo mismo, una alta preponderancia de valores bajos. Será necesario corregir este hecho en todos aquellos análisis en los que vayamos a necesitar normalidad de los valores, por lo que será necesaria la normalización.

# 4. Análisis de los datos

# 4.1 Selección de los grupos de datos que se quieren analizar/compararar (planificación de los análisis a aplicar) [Pendiente. Word de Joel]

# 4.2 Análisis particulares, y comprobaciones de normalidad y distribución de la varianza en las variables bajo estudio

A continuación vamos a presentar el trabajo de estudio que requiere responder a alguna de las cuestiones que motivan el proyecto. Por ello, estructuramos la presentación del trabajo más bien de acuerdo a la siguiente estructura:

1. Pregunta que queremos responder.
2. Selección de los datos concretos para resolver la cuestión.
3. Comprobación de normalidad y homogeneidad de la varianza.
4. Aplicación de pruebas estadísticas.

Comencemos con las siguientes cuestiones.

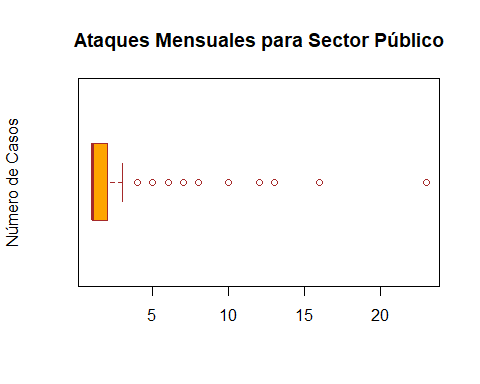
1. *¿Existe algún periodo del año en que debería ampliar el presupuesto y los medios necesarios, al estar más expuesto a recibir ciberataques?*
2. Para responder a esta pregunta, podrían plantearse muy distintas técnicas estadísticas. De hecho, en el momento en que entra en juego la dimensión temporal, podría plantearse un análisis más bien en el terreno del análisis de series temporales. Para este análisis avanzado, hemos encontrado una referencia de Box [5] que podría ser de mucha utilidad, pero que por su complejidad trataremos de simplificar en análisis más sencillos.

En concreto, en lugar de analizar estacionalidad en la serie, lo que vamos a considerar es que la variable “Mes” constituye una variable categórica, que podría segmentar el set de datos en observaciones para cada uno de los meses. Como estamos interesados en lo que ocurre en nuestro sector (recordemos que el caso que analizamos nos pone en el papel de una empresa de sector público, que según hemos visto tiene el identificador “O”), únicamente filtraríamos las observaciones de ataques en nuestro sector, y para no hacer más complejo el análisis, nos interesará el número total de incidentes de seguridad reportados (campo “TotalAtaques”).

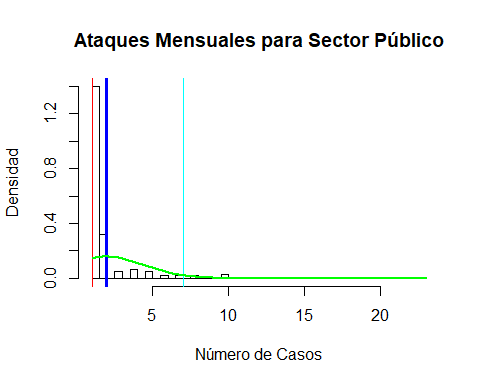
A partir de estos datos seleccionados, es decir, las observaciones individuales para Sector Público “O”, y el número total de ataques, posterioremente fragmentaremos el set de datos en 12 subsets, y querremos ver si existen diferencias estadísticamente significativas entre la media del número de ataques según el mes seleccionado. Para ello, cogeremos como mes de referencia para la comparación aquel en el que la media de ataques sea más alta, y haciendo el contraste de hipótesis sobre la media sobre el resto de grupos, podremos concluir para cuáles de ellos la diferencia entre las medias es estadísticamente igual, o diferencia.

Veamos a continuación cómo seleccionar el subset apropiado para este análisis.

# Set de datos necesario para el análisis de impacto temporal  
  
attacks\_temp <- attacks\_Input[attacks\_Input$Code\_target\_class=="O",c('Year','Mes','NumeroAtaques')]  
  
monthlyAttacks <- attacks\_temp$NumeroAtaques  
  
# Graficamos para la variable seleccionada un diagrama de boxplot, y la distribución de frecuencias de los distintos valores.  
  
boxplot(monthlyAttacks,  
 main="Ataques Mensuales para Sector Público",  
 ylab="Número de Casos",  
 col="orange",  
 border="brown",  
 horizontal=TRUE)

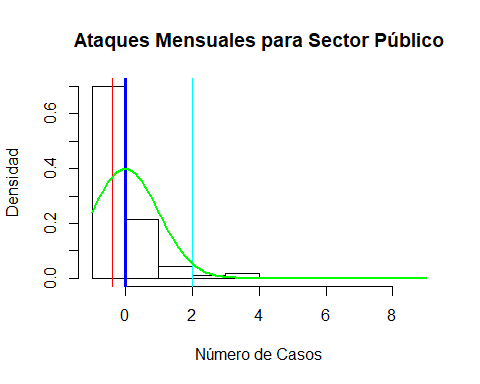


hist(monthlyAttacks, freq=FALSE, breaks=50, main="Ataques Mensuales para Sector Público", xlab="Número de Casos", ylab="Densidad")  
abline(v=mean(monthlyAttacks), col="blue", lwd=3)  
abline(v=median(monthlyAttacks), col="red")  
abline(v=mean(monthlyAttacks)-2\*sd(monthlyAttacks), col="cyan")  
abline(v=mean(monthlyAttacks)+2\*sd(monthlyAttacks), col="cyan")  
curve(dnorm(x, mean=mean(monthlyAttacks), sd=sd(monthlyAttacks)), add=TRUE, col="green", lwd=2)



A partir de los gráficos anterior, sin necesidad de ningún test de normalidad, vemos que la observación tiene una cola pesada a derecha. Vamos a intentar tipificar [6] la variable.

# Tipificación de la variable Número de Ataques  
  
monthlyAttacks\_N <- scale(monthlyAttacks, center = T, scale = T)  
  
hist(monthlyAttacks\_N, freq=FALSE, main="Ataques Mensuales para Sector Público", xlab="Número de Casos", ylab="Densidad")  
abline(v=mean(monthlyAttacks\_N), col="blue", lwd=3)  
abline(v=median(monthlyAttacks\_N), col="red")  
abline(v=mean(monthlyAttacks\_N)-2\*sd(monthlyAttacks\_N), col="cyan")  
abline(v=mean(monthlyAttacks\_N)+2\*sd(monthlyAttacks\_N), col="cyan")  
curve(dnorm(x, mean=mean(monthlyAttacks\_N), sd=sd(monthlyAttacks\_N)), add=TRUE, col="green", lwd=2)



Según apreciamos, seguimos teniendo la dificultad de que el ajuste a la curva normal sea demasiado bueno, puede que por el pequeño tamaño de la muestra sobre la que tenemos que trabajar. Sin embargo, sí que observamos un ajuste más razonable a lo que cabría esperar de una curva normal. Vamos a analizar qué nos dice un test de normalidad sobre dicha variable.

# Test de normalidad para la variable tipificada que hemos creado, para el análisis del número de casos mensuales.  
  
# Carga de librerías para tests de normalidad  
library(normtest)  
library(nortest)  
library(moments)  
  
# Varios tests de normalidad, todos ellos rechazando la hipótesis nula de normalidad  
  
sf.test(monthlyAttacks\_N) # Shapiro-Francia

##   
## Shapiro-Francia normality test  
##   
## data: monthlyAttacks\_N  
## W = 0.41688, p-value < 2.2e-16

jb.norm.test(monthlyAttacks\_N) # Jarque-Bera

##   
## Jarque-Bera test for normality  
##   
## data: monthlyAttacks\_N  
## JB = 7713.7, p-value < 2.2e-16

agostino.test(monthlyAttacks\_N) # Agostino

##   
## D'Agostino skewness test  
##   
## data: monthlyAttacks\_N  
## skew = 4.6251, z = 12.9676, p-value < 2.2e-16  
## alternative hypothesis: data have a skewness

Observamos que la variable que tratamos de analizar no cumple la hipótesis de normalidad bajo ninguno de los tests realizados. Sin embargo, siguiendo a Rovira [7], podremos llevar a cabo nuestro análisis si el contraste que vamos a realizar es sobre la media, en virtud de lo siguiente: *“si una muestra es lo bastante grande (n>30), sea cual sea la distribución de la variable de interés, la distribución de la media muestral será aproximadamente una normal. Además la media será la misma que la de la variable de interés, y la desviación típica de la media muestral será aproximadamenet el error estándar.”*

Es decir, no hemos podido asegurar la normalidad en la variable, pero avanzaremos igualmente con el contraste de hipótesis sobre la media, dado que tenemos un tamaño de muestra considerado grande (superior a 30).

En relación a la homocedasticidad, según se indica en [1], podemos aplicar el test de Fligner-Killeen cuando los datos no cumplen la condición de normalidad.

# test de homocedasticidad para muestras que no cumplen la condición de normalidad: Fligner-Killeen  
  
fligner.test(NumeroAtaques ~ Mes, data = attacks\_temp)

##   
## Fligner-Killeen test of homogeneity of variances  
##   
## data: NumeroAtaques by Mes  
## Fligner-Killeen:med chi-squared = 10.518, df = 11, p-value =  
## 0.4845

En este caso, al menos, sí que hemos podido confirmar que no existe una diferencia significativa de la varianza en el número total de ataques a lo largo de los distintos grupos de meses. En consecuencia, parece razonable admitir que podamos llevar a cabo contrastes de hipótesis sobre la media y aceptar sus conclusiones, a partir del Teorema Central del Límite.

c1) En este caso, seguimos el desarrollo práctico de Amat [8], donde también se afirma que aunque no hayamos encontrado normalidad en la población, el test sobre la media en muestras de más de 30 observaciones *"el t-test sigue siendo suficientemente robusto, aunque un test no paramétrico basado en la mediana (Mann-Withney-Wilcoxon) o un test de bootstraping podrían ser más adecuados*. Como primera aproximación, veremos los resultados a que llegamos con el t-test. Como decíamos al principio, primeramente tomaremos como base de los tests, aquel mes con mayor media de ataques.

# Mes con máximo valor medio de ataques  
  
attacks\_meanByMonth <- attacks\_temp %>% group\_by(Mes) %>% summarize(mean(NumeroAtaques))  
  
attacks\_meanByMonth[order(-attacks\_meanByMonth$`mean(NumeroAtaques)`),]

## # A tibble: 12 x 2  
## Mes `mean(NumeroAtaques)`  
## <fct> <dbl>  
## 1 1 2.59  
## 2 12 2.52  
## 3 6 2.5   
## 4 7 2.2   
## 5 10 2.11  
## 6 2 1.94  
## 7 8 1.88  
## 8 4 1.73  
## 9 5 1.73  
## 10 11 1.58  
## 11 3 1.54  
## 12 9 1.38

De la tabla anterior, observamos que el mes con mayor número medio de ataques sería enero, por lo que vamos a contrastar si la media del número de ataques del resto de meses es estadísticamente igual o diferente (necesariamente menor).

# Contraste de hipótesis sobre igualdad en la media del número de ataques entre enero y el resto de meses, de manera iterativa.  
  
for(i in seq(2,12)){  
 a <- t.test(attacks\_temp[attacks\_temp$Mes==1,3], attacks\_temp[attacks\_temp$Mes==i,3], alternative = "less")  
 cat("p-valor para el contraste entre el mes 1 y el mes",i,":", a$p.value,"\n")  
   
}

## p-valor para el contraste entre el mes 1 y el mes 2 : 0.7193594   
## p-valor para el contraste entre el mes 1 y el mes 3 : 0.8444329   
## p-valor para el contraste entre el mes 1 y el mes 4 : 0.7898819   
## p-valor para el contraste entre el mes 1 y el mes 5 : 0.7785468   
## p-valor para el contraste entre el mes 1 y el mes 6 : 0.5286045   
## p-valor para el contraste entre el mes 1 y el mes 7 : 0.6124608   
## p-valor para el contraste entre el mes 1 y el mes 8 : 0.7374304   
## p-valor para el contraste entre el mes 1 y el mes 9 : 0.877013   
## p-valor para el contraste entre el mes 1 y el mes 10 : 0.6631326   
## p-valor para el contraste entre el mes 1 y el mes 11 : 0.8297838   
## p-valor para el contraste entre el mes 1 y el mes 12 : 0.5206724

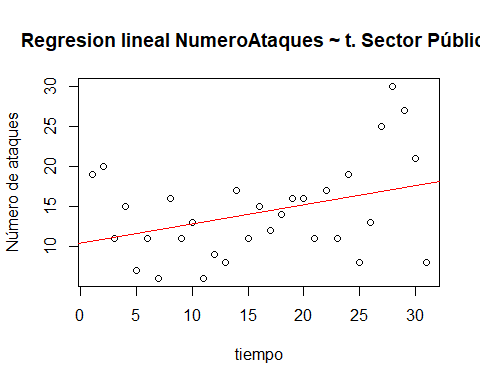
Como se puede apreciar, esto nos indica que no se puede rechazar la hipótesis nula de igualdad en la media en la comparación entre cada par de meses, por lo que de alguna manera lo que concluimos es que el número de ataques se mantiene relativamente estable a lo largo del año. En la sección de conclusiones, desarrollaremos en qué se traduce este hecho para la pregunta que nos planteábamos.

c2) Otro asunto relacionado con la variable temporal que puede resultar interesante analizar, es hasta qué punto la tendencia se mantiene relativamente constante, o si se prevé que el número de ataques aumente o disminuye. De nuevo, puede que la aproximación más ortodoxa pasara por análisis de series temporales, pero vamos a hacer una aproximación lineal que nos permita reflexionar sobre hasta qué punto cabe esperar crecimiento, decrecimiento o mantenimiento. Para ello, vamos a “ordenar” de alguna manera el número de ataques, creando una variable que recoja la secuencialidad de las observaciones a partir de los meses, agregando casos por mes y año, y asignando a esta variable *“t”* un valor secuencial.

# Agregación por Mes y Año, y creación de una variable temporal secuencial "t"  
  
attacks\_sumByMonth <- attacks\_temp %>% group\_by(Year, Mes) %>% summarize(sumAtaques = sum(NumeroAtaques))  
attacks\_sumByMonth <- as.data.frame(attacks\_sumByMonth)  
attacks\_sumByMonth$t <- seq(1,dim(attacks\_sumByMonth)[1])  
  
# Regresión del número de ataques sobre el paso del tiempo (variable secuencial "t")  
  
reg\_attacks\_temp <- lm(sumAtaques ~ t, data = attacks\_sumByMonth)  
  
  
# Mostramos el resumen de la regresión, y la representación gráfica de la recta de regresión sobre el disgrama de dispersión de ambas variables  
  
summary(reg\_attacks\_temp)

##   
## Call:  
## lm(formula = sumAtaques ~ t, data = attacks\_sumByMonth)  
##   
## Residuals:  
## Min 1Q Median 3Q Max   
## -9.8770 -4.4099 -0.1819 3.2750 12.8403   
##   
## Coefficients:  
## Estimate Std. Error t value Pr(>|t|)   
## (Intercept) 10.4645 2.0940 4.997 2.56e-05 \*\*\*  
## t 0.2391 0.1142 2.093 0.0452 \*   
## ---  
## Signif. codes: 0 '\*\*\*' 0.001 '\*\*' 0.01 '\*' 0.05 '.' 0.1 ' ' 1  
##   
## Residual standard error: 5.689 on 29 degrees of freedom  
## Multiple R-squared: 0.1312, Adjusted R-squared: 0.1013   
## F-statistic: 4.381 on 1 and 29 DF, p-value: 0.0452

plot(x=attacks\_sumByMonth$t, y=attacks\_sumByMonth$sumAtaques, main="Regresion lineal NumeroAtaques ~ t. Sector Público", xlab='tiempo', ylab='Número de ataques')  
abline(reg\_attacks\_temp, col=2)



Del análisis anterior, cabe extraer algunas conclusiones interesantes:

* Por un lado, parece que la tendencia en el número de ataques que esperamos recibir, será creciente. De hecho, si consideramos que el factor tiempo tiene una granularidad mensual, el parámetro de 0.23 de la pendiente viene a indicar que en cada mes cabe esperar un crecimiento en el número medio de casos superior al 20%. Es cierto que el número medio de incidentes mensual aún es muy bajo, por lo que el crecimiento en valor absoluto no es muy alto. Sin embargo, esto debe darnos una idea sobre la previsión de inversión futura, y que será necesario cada vez una mayor dedicación y esfuerzo para atajar estos problemas.
* Observamos además que dicha pendiente es estadísticamente significativa, dentro de la regresión que hemos realizado.
* No obstante, el valor del valor del coeficiente de autodeterminación es bastante bajo para lo que se suele exigir en este tipo de análisis, y sin embargo el valor de significatividad global del modelo a través del estadístico F no rechaza la hipótesis nula de buen ajuste global del modelo. Estos datos aparentemente contradictorios pueden venir a expresar que el modelo que hemos utilizado, en el que únicamente consideramos el tiempo, es excesivamente simple, y que gran parte de la varianza en la variable analizada seguramente encuentre justificación en otras variables que no se están incluyendo en el modelo.
* Teniendo en cuenta que lo que queríamos era una primera aproximación a si cabe esperar que el número de ataques en nuestro sector (Sector Público “O”) crecerá, parece razonable afirmarlo. Además, parte del buen ajuste del modelo podría venir explicado también por el hecho de que a través de la prueba anterior, hemos descartado diferencias estadísticamente significativas entre los datos de número de ataques mes a mes.

# 5. Representación de los resultados a partir de tablas y gráficas

# 6. Resolución del problema. A partir de los resultados obtenidos, ¿cuáles son las conclusiones? ¿Los resultados permiten responder al problema?

## Contribuciones

|  |  |
| --- | --- |
| Investigación Previa Redacción de las respuestas Desarrollo código | JBP – IRP JBP – IRP JBP – IRP |

## Bibliografía

[1] Subirats, Laia - Pérez, Diego O. - Calvo, Mireia (2019). “Introducción a la limpieza y análisis de los datos”, Universidad Oberta de Catalunya

[2] Bock, Tim (2019). “What is a Crosstab”, Display R Blog. [en línea] [Última consulta: 15/May/2020] <https://www.displayr.com/what-is-a-crosstab/>

[3] Osborne, Jason W. (2013). “Best practices in data cleaning: A complete guide to everything you need to do before and after collecting your data.” Thousand Oaks, CA. Sage Publications.

[4] Datacarpentry (2018). “Aggregating and analyzing data with dplyr” [en línea] [Última consulta: 20/May/2020] <https://datacarpentry.org/R-genomics/04-dplyr.html>

[5] Peña, D. (2010), “Análisis de Series Temporales”, Alianza Editorial.

[6] Parada, Luis F. (2019). “Tipificación de variables”. RPubs. [en línea] [Última consulta: 24/May/2020] <https://www.rpubs.com/F3rnando/521190>

[7] Rovira, Carles (2009), “Teorema del límite central”, Universidad Oberta de Catalunya.

[8] Amat, Joaquín (2016), “T-test: Comparación de medias poblacionales independientes”, Rpubs. [en línea] [Última consulta: 25/May/2020] <https://rpubs.com/Joaquin_AR/218467>