TESIS FINAL DE GRADO

CIBERSEGURIDAD EN EMPRESAS

LEANDRO ENCINAS

Universidad de San Isidro “Dr. Plácido Marín”

ALUMNO: Leandro Encinas

DNI: 39346079

TEMA: Ciberseguridad en empresas

TUTOR: Sergio Bogliolo

CARRERA: Lic. Administración de Negocios

1 - INDICE

2 - INTRODUCCION

Para el desarrollo de mi tesis sobre Ciberseguridad utilizaré métodos de investigación cualitativos y cuantitativos.

La información sobre la que se basa el trabajo es obtenida y recopilada de cursos, videos, entrevistas, encuestas, charlas e informes de especialistas y páginas web de distintas entidades como por ejemplo KPMG (Red global de firmas de servicios profesionales que ofrece servicios de auditoría, de asesoramiento legal, fiscal, financiero y de negocio en 156 países. Es una de las cuatro firmas más importantes del mundo de servicios profesionales).

Dada la complejidad y diversidad del tema elegido para analizar, opté por implementar una amplia gama de herramientas que me permitan obtener una visión integradora del mismo y darle un enfoque desde el punto de vista económico.

Se incluyen en el marco investigativo, entrevista realizada al jefe de Seguridad Informática de Pampa Energía, empresa que presenta un gran plan de Ciberseguridad haciendo énfasis en la protección de la información de sus usuarios y los activos de la organización. La segunda entrevista fue realizada a Leandro Pompeo, consultor independiente y Lead MLOps Engineer en Quadrant Health, especialista en Inteligencia Artificial y Ciberseguridad.

2.1 – OBJETIVO

El objetivo de esta tesis es poder informar y concientizar a las empresas y sus empleados sobre el crecimiento de los ciberdelitos, el riesgo, costos y consecuencias de los mismos. Aportarles los conocimientos necesarios para la correcta toma de decisiones en asuntos relacionados con la Ciberseguridad.

2.2 - HIPOTESIS

La hipótesis de este trabajo de investigación se basa en afirmar el alto riesgo que enfrentan las empresas ante los ciberataques, en los cuales sus bases de datos y principales activos se encuentran totalmente expuestos.

3 – DESARROLLO DE LA INVESTIGACION

3.1 – MARCO TEORICO

Para poder entender de manera óptima nuestro tema a desarrollar en la investigación, primero debemos definir el concepto de Ciberseguridad. Además, debemos analizar la evolución de los Ciberdelitos a lo largo de los años y medir el impacto de los mismos en las organizaciones.

3.2 – DEFINICION DE CIBERSEGURIDAD

La ciberseguridad es la protección de sistemas, datos, software y hardware que están conectados a Internet. Su objetivo es principalmente proteger los datos, muchos de ellos confidenciales, de las empresas evitando el robo de los mismos, los ataques cibernéticos y las usurpaciones de identidad.

Para NIC Argentina (Dirección Nacional del Registro de Dominios de Internet), es también conocida como *"Seguridad de las tecnologías de la información, es la rama de la informática que procura detectar vulnerabilidades que ponen en juego la integridad, disponibilidad y confidencialidad de los sistemas informáticos"*. (NIC, noviembre 2018).

3.3 – HISTORIA Y EVOLUCION DE CIBERDELITOS

3.3.1 – 2000 A 2003: EL USO DEL CORREO ELECTRÓNICO Y LOS VIRUS INFORMÁTICOS.

La evolución del ciberdelito se centra en el comienzo del siglo XX, tras la alarma generada en la población con el llamado "Efecto 2.000".

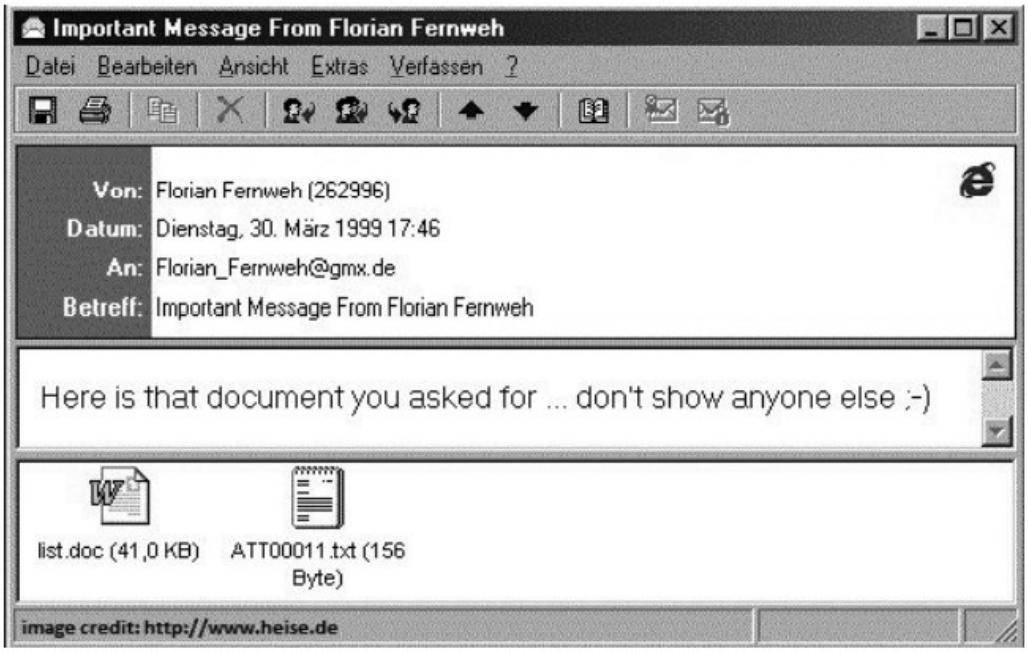
Este efecto marcó un antes y un después en el ciberdelito, asistiéndose a la aparición de toda una serie de ciberataques motivados principalmente por el desafío que suponían para el ciberdelincuente los avances en las nuevas tecnologías. En estos años se populariza el envío de softwares maliciosos a través de mensajes de correo electrónico no deseado. Normalmente, estos emails se acompañan de un vínculo o archivo adjunto. Tal es el caso del virus "I love you", mensaje de correo electrónico no deseado con "I love you" en el asunto y un archivo adjunto que pretendía ser una carta de amor, que provocó el colapso en los equipos informáticos de decenas de millones de usuarios de Windows. Algunas de las víctimas del ataque fueron: el Pentágono, el Parlamento Británico, la Reserva Federal, Ford, AT&T, Iberia, el Grupo Prisa, Vodafone, Dell o Telecinco. Los daños causados se estiman entre 4,9 y 7,7 millones de euros.

EJEMPLO DEL VIRUS “I LOVE YOU”

FUENTE https://www.elandroidelibre.com

El predecesor fue “Melissa”, un macro virus que utilizaba técnicas de ingeniería social y que a través del mensaje “Aquí está el documento que me pediste, no se lo enseñes a nadie”, en apenas unos días, protagonizó uno de los casos de infección masiva más importantes de la historia, causando daños de más de 80 millones de dólares a empresas norteamericanas y compañías tales como Microsoft, Intel o Lucent Technologies, que tuvieron que bloquear sus conexiones a internet.

EJEMPLO DEL MACROVIRUS “MELISSA”



FUENTE: http://www.pandasecurity.com

Estos ataques proporcionaron a los ciberdelincuentes la atención que buscaban, a la vez que los puntos de acceso wifi comenzaban a ganar impulso suponiendo una nueva oportunidad para la ciberdelincuencia al facilitar el robo de información de los usuarios en redes inalámbricas no protegidas y completamente vulnerables.

3.3.2 – 2004 A 2005: LOS ORDENADORES ZOMBIES.

En estos años la aparición del adware (Software gratuito promocionado mediante publicidad en ventanas emergentes) o software compatible con la publicidad, que muestran los pop ups de forma automática o anuncios de descarga en el equipo del usuario para hacer que éste compre productos o servicios, es determinante en la evolución del ciberdelito. Los proveedores de programas publicitarios vieron cómo aumentaban sus ingresos y los ciberdelincuentes aprovecharon la oportunidad para instalar diferentes paquetes de adware en millones de sistemas a cambio de grandes cantidades económicas.

Los rootkits también jugaron un papel importante en esta época. Definido como un software espía, llegaba a los ordenadores de las víctimas aprovechando cualquier deficiencia, modificando el funcionamiento del sistema operativo y su núcleo. Los rootkits son invisibles, lo que los hace difíciles de desinfectar, sin embargo, y a diferencia de los gusanos y virus, no tienen capacidad para duplicarse.

Por otro lado, comienza el nacimiento de los ordenadores zombies. Los ciberdelincuentes podían infectar miles de máquinas al mismo tiempo, controlándolas de forma remota y sin el conocimiento de los usuarios, de tal manera que un ejército de ordenadores zombies siguiera las ordenes de los ciberdelincuentes. En todos los casos, el objetivo principal de la delincuencia en este momento era ganar dinero, bien amenazando a las empresas con que atacarían sus ordenadores y sitios web a través del chantaje, o bien por las ventas generadas gracias al spam (Mensajes no solicitados, no deseados o de remitente desconocido que pueden contener malware o software malicioso).

EJEMPLO DE SPAM

FUENTE: https://www.bing.com

3.3.3 – 2006 A 2008: LAS BANDAS ORGANIZADAS

El dinero favoreció la organización de los ciberdelincuentes en bandas. Algunos poseían incluso una estructura similar a la de la mafia. Para proteger sus crecientes imperios comerciales, los ciberdelincuentes se hicieron más discretos a la hora de utilizar sus métodos, a la vez que mostraban todas sus habilidades tecnológicas. En este contexto, muchos de los ciberdelincuentes simplemente se unieron a organizaciones que ya operaban fuera del medio digital, de tal manera que mientras éstas últimas aportaban su experiencia, los ciberdelincuentes aportaban sus conocimientos de expertos. En este sentido, los primeros

escenarios de la delincuencia organizada se focalizan en el fraude en el comercio electrónico y en la banca electrónica, como instrumentos más rápidos para obtener beneficios.

Finalmente, las bandas organizadas van perdiendo su razón de ser. El crimen organizado y el ciberdelincuente comienzan un proceso donde se desvinculan a nivel operativo, de tal forma que la colaboración entre ambos se centra en la compra de los servicios a los Ciberdelincuentes. De esta forma, se desvincula del hecho delictivo concreto y sólo ofrece el servicio.

El más ejemplo más claro de esto es la venta de kits de phishing en la que un usuario cualquiera, sin conocimientos avanzados de informática puede adquirir en el mercado del malware, un kit que sólo hay que configurarlo y poner en funcionamiento, para empezar a infectar equipos y obtener información de sus usuarios. Incluso en los acuerdos de servicio por el kit, informan que el desarrollador no se hace responsable del mal uso del programa, desligándose de la actividad.

3.3.4 – 2009: REDES SOCIALES Y LA IMPORTANCIA DE LOS DATOS

A finales de la primera década del siglo XX las redes sociales consolidan su papel como agentes de socialización. Los ciberdelincuentes encuentran en estos medios de comunicación social una fuente de datos para cometer actos delictivos de toda índole.

Las redes sociales son herramientas que los usuarios utilizan diariamente de forma masiva para informarse, comunicarse y entretenerse. De acuerdo con un estudio Digital 2021 de HootSuite y We Are Social hay más de 4.033 millones de usuarios de redes sociales en todo el mundo, y va en aumento cada año.

Los usuarios promedio dedican más de 2 horas al día para disfrutar de las redes sociales y cuando acceden a ellas lo hacen a través de un dispositivo móvil en un 99% de los casos. Esta facilidad de acceso puede suponer que muchos usuarios utilicen las redes mientras están en su jornada laboral y que la conexión sea a través de la red de la empresa.

A partir de los accesos a sus perfiles de redes sociales desde el trabajo comenzaron a provocarse brechas de ciberseguridad en las propias empresas a través del robo de datos personales de la plantilla, lo que desencadenó en el robo de información financiera o de credenciales vinculadas a la organización o por los ataques a los equipos que se utilizan.

3.3.5 – EL CIBERDELITO EN LA ACTUALIDAD: INGENIERÍA SOCIAL Y DEEP WEB

Habiendo realizado un repaso de la evolución de los ciberdelitos, el verdadero motivo de su estudio no podría justificarse de otro modo sino es a través del análisis de cifras reales. El ciberdelito ha experimentado un crecimiento exponencial en los últimos años, y así queda en evidencia en el mapa mundial a tiempo real de la empresa rusa Kaspersky, donde se puede observar que diariamente la cifra de ciberataques asciende a más de 300.000 ataques diarios. Según Brett Kelsey, vicepresidente y director de tecnología de Intel Security en Latinoamérica, el ciberdelito significa un 0,8% del PIB mundial, o lo que es lo mismo, 6,100 millones de dólares, cifra que va en aumento año tras año.

La ingeniería social podría definirse como un elemento no técnico de bajo costo, utilizado por los ciberdelincuentes, que manipula a los individuos utilizando la conducción psicológica, para inferir en los sistemas de seguridad, influyendo en sus actitudes, acciones y relaciones. El objetivo del ciberdelincuente es obtener información, realizar fraudes u obtener acceso ilegítimo de los usuarios bien sea por vía telefónica, por contacto directo o por correo, tanto electrónico como tradicional. La ingeniería social se utiliza cada vez con más frecuencia en el ataque a las medianas y pequeñas empresas, así como a las grandes corporaciones.

Normalmente la ingeniería social se aprovecha de la inexperiencia del usuario, conociendo bien a su víctima, haciéndose pasar por alguien de su entorno o agente superior, utilizando la persuasión.

En general, los métodos de la ingeniería social están organizados de la siguiente manera:

1. **Acercamiento**: el ciberdelincuente trata de ganarse la confianza del usuario adoptando un rol cercano al usuario: una empresa cliente, un posible proveedor de servicios, etc.

2. **Alerta**: utiliza un pretexto de seguridad o situación de emergencia para que el usuario colabore.

3. **Distracción**: el ciberdelincuente comunica al usuario que su colaboración ha sido de ayuda y que todo ha vuelto a la normalidad, evitando que este pueda avisar a alguien de su empresa o entorno.

Los medios más utilizados se describen a continuación:

1. Teléfono (vishing): llamadas telefónicas de personas que se hacen pasar por una organización con una buena imagen de marca y alta notoriedad.

2. Correo electrónico (phishing).

3. Correo tradicional.

4. USB (baiting): el atacante carga unidades de USB con malware y espera que el usuario las conecte a su dispositivo.

5. Mensajería instantánea.

6. Páginas web.

7. Redes sociales

Fuente: Reporte Norton 2013

El problema en este tipo de ataques es que no hay una alerta inmediata que advierta de un ataque, y por ello se recomienda seguir las siguientes indicaciones:

1- Antes de ofrecer información tanto personal como empresarial, averiguar la identidad de la persona que solicita la información.

2- En caso de que se acceda a facilitar la información solicitada, verificar qué información se está dando.

3- Preguntarse la importancia de la información que se está pidiendo.

La ingeniería social aplicada a las redes sociales es una de las técnicas más sencillas y efectivas para acercarse a la víctima, ya que, en líneas generales, los usuarios suelen aceptar invitaciones de otros sin verificar el perfil. A esto se le une el hecho de la facilidad con la que se obtiene información a través de estos medios puesto que, hoy por hoy, muy pocos usuarios limitan la privacidad de sus perfiles, accediendo, desde cualquier ubicación.

Según afirma Emanuel Abraham, hacker ético de Security Solution & Education, “la persona que efectúa este método trata de engañar a la víctima, buscando entrar en confianza o haciéndose pasar por alguien más para obtener lo que necesita. Teniendo en cuenta que somos muy vulnerables y nos movemos a través de una serie de impulsos irracionales, el que ejecute esta técnica usará comúnmente el teléfono, internet, el disfraz u otros métodos para engañar fingiendo ser alguien más. En muchos de los casos la persona suplanta a un trabajador de la empresa o a alguien de servicio técnico” (Emanuel Abraham, 2019.)

La Deep Web es la parte de la red que no está incluida en los motores de búsqueda o directorios, dando forma a lo que se ha llamado la “Internet Profunda”. Hoy en día se estima que cerca de un 85% de todo el contenido que hay en internet se encuentra en la Deep Web. Con respecto a la clasificación de los contenidos presentes en esta parte de internet, cabe mencionar la dificultad de dicha tarea, debido a la enorme diversidad de estos.

Actualmente se estima que existen aproximadamente 550 billones de documentos en la Deep web frente a 1 billón de documentos en la red superficial, siendo las redes virtuales privadas (virtual private networks o VPN) tecnologías que corresponden a esta clasificación de red invisible y sus principales representantes. Estas redes corresponden a contenidos a los que se puede acceder únicamente a través de un software específico, siendo uno de los ejemplos más representativos TOR.

Según la propia página web de TOR, “la red TOR es un grupo de servidores operados por voluntarios que permite a la gente mejorar su privacidad y la seguridad en Internet. Usuarios

de TOR emplean esta red mediante la conexión a través de una serie de túneles virtuales, en lugar de hacer una conexión directa, lo que permite a ambas organizaciones e individuos compartir información a través de redes públicas sin comprometer su privacidad. En la misma línea, TOR es una efectiva herramienta de elusión de la censura, permitiendo a sus usuarios llegar a destinos o contenidos que de otra manera estarían bloqueados".

TOR es un proyecto diseñado e implementado por la Marina de los Estados Unidos. Puede definirse como una red de túneles virtuales que permite a los usuarios navegar con privacidad en internet, y a los desarrolladores crear aplicaciones para el intercambio de información sobre redes públicas sin tener que comprometer su identidad. Igualmente, ayuda a reducir o evitar el seguimiento que hacen los sitios web de los hábitos de navegación de las personas y a publicar sitios web y otros servicios sin la necesidad de revelar su localización. Si bien, el objetivo de TOR es proteger a los usuarios de la vigilancia en internet (por ejemplo, del análisis de tráfico). También se ha utilizado para mantener ocultos diferentes servicios de dudosa legalidad.

Así, en la Deep Web se pueden encontrar contenidos ilegales de entidades anónimas que buscan realizar diferentes transacciones bajo privacidad. La venta de bienes y servicios de origen ilícito se puede clasificar en 6 grandes grupos definidos a continuación (Iter Criminis, 2016):

1**. Tráfico de drogas**: supone un 62% de los bienes que se trafican en la Deep web. Dentro de esta categoría se pueden encontrar los productos químicos para su fabricación, productos derivados, así como el conjunto de actos que conlleva el consumo de droga.

2. **Tráfico de información** (16%): engloba desde la venta de listados de direcciones de páginas web a información robada de compañías. También se pueden encontrar cuentas sustraídas a usuarios legítimos de servicios en internet que son vendidas en subasta al que más pague por obtenerlas, siendo sus precios menores a los oficiales.

3. **Venta de aplicaciones maliciosas** (15%): se pueden encontrar principalmente las siguientes aplicaciones o programas maliciosos:

— **Keyloggers**: son programas informáticos que ayudan al ciberdelincuente a rastrear las pulsaciones que son realizadas por el trabajador de una empresa en su teclado, cuya finalidad es conocer qué información mete el usuario su computadora, así como contraseñas.

— **Exploits**: son programas que se usan para aprovechar la inseguridad de un sistema para conseguir fines, como puede ser el acceso no autorizado. Se venden desde exploits por 1 euro ya parcheados anteriormente por las empresas, hasta exploits "0 Day" (exploits no registrados por la empresa y que aún no existe forma de neutralizarlos) de hasta cientos de miles de euros.

— **Botnet**: es una red de ordenadores que son afectados para que mediante un ataque DDOS se quede sin funcionamiento un servidor o página web, mediante el colapso provocado por

miles de peticiones de acceso a un ordenador. Contratar este tipo de ataque puede valer tan sólo 1 euro, aunque depende del tiempo de operación.

— **Ransomwares**: es un tipo de troyano, el cual cifra los archivos de la víctima, y le muestra que, si quiere recuperar su información personal, tendrá que pagar una cantidad de dinero (dinero virtual o bitcoins).

4. **Venta de armas** (2%): en el ranking mundial de venta ilegal, la de armas ocupa el tercer lugar; por delante de la misma encontramos la venta de drogas y tráfico de personas. Sin embargo, en la Deep Web abarca el 2% del mercado ilegal. Algunas de estas armas provienen de países de Europa del este, cuyo rastro se perdió por la disolución de la Unión Soviética o durante la Guerra de los Balcanes, y pertenecen al mercado negro.

5. **Asesinatos/agresiones por encargo** (1%): dentro de esta red existen personas que se ofrecen para realizar delitos anónimos por mandato de otros a cambio de una cantidad de dinero. Este tipo de delitos comprende palizas o incluso matar directamente a alguien.

Además de las seis categorías citadas anteriormente, dentro del mercado ilegal en la Deep Web, se encuentra WikiLeaks, organización internacional de medios de comunicación y sin fines de lucro, la cual sube a su sitio web, bajo el anonimato de sus fuentes, informes y documentos filtrados con información sensible para el interés público, como pueden ser el espionaje, la corrupción o las guerras.

3.3.6 – CONTEXTO ACTUAL

Según la Unidad Fiscal Especializada en Ciberdelincuencia la modalidad conocida como “Ramsonware” aumentó 280% en el primer trimestre de 2021.

En 2020 un informe de Ciberamenazas de PwC resaltó que “el Ramsonware, que ese año se expandió por efecto de la pandemia, la explosión del trabajo remoto y la reorientación de organizaciones criminales hacia la ciberdelincuencia” (PwC, 2020). De hecho, un informe de Checkpoint Research, una consultora de seguridad informática precisó que en la primera mitad de 2021 los ataques de Ramsonware en el mundo crecieron 57% respecto de 2020, en el que ya habían aumentado 75 por ciento. El estudio detectó además que, en cantidad de ataques por organización por semana, India era el país más afectado con 213 casos, seguido por la Argentina, con 104 (pero con un descenso del 54% respecto de 2020) y Chile cercano tercero con 103 casos (Checkpoint Research, 2021).

Existen distintos criterios de calificación e información de un delito que, por lo general, las víctimas prefieren ocultar. En Estados Unidos avanza la decisión de hacer obligatoria la denuncia tras dos ataques de alto perfil. Uno de los ataques fue a Colonial Pipeline, cabe

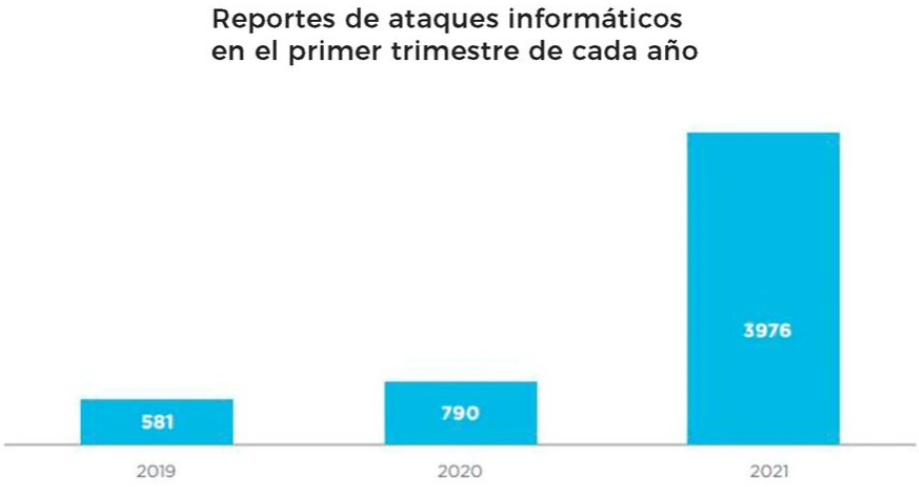
aclarar que esta empresa tiene la red de oleoductos más grande de Estados Unidos. Abastece casi la mitad de los combustibles líquidos consumidos por la costa Este de Estados Unidos. Este ataque paralizó y luego afectó durante una semana la provisión de combustible en parte de la costa Este.

Colonial pagó en mayo de 2021, 75 bitcoins de rescate (unos USD 4,3 millones entonces, de los cuales el FBI pudo recuperar 2,3 millones) al grupo criminal ruso Dark Side (Lado Oscuro). “Tuvimos que pagar, nadie quiere ser extorsionado por criminales”, se defendió ante el Senado de EEUU Joseph Blount, CEO de Colonial, La organización fue criticada porque el hackeo ocurrió a través de una cuenta no protegida por múltiple autenticación (un principio básico de ciberseguridad), a la que se podía acceder con un solo código. “Era un código complejo, no era Colonial123” (Joseph Blount, 2021).

El otro ataque fue al productor de carne más grande del mundo, JBS USA. El ataque afectó a los servidores que soportan sus sistemas de TI en Norteamérica y Australia. Esto llegó a afectar al suministro de carne y también a su precio.

3.3.6.1 – SITUACION EN ARGENTINA

“El ciberdelito ya venía en aumento, es un negocio que mueve entre 2 y 3 billones (millones de millones) de dólares por año, más que el PBI de muchos países. En los últimos años se formaron organizaciones especializadas, fondeadas, con distintos roles, criminales que estaban en otras actividades y se mudaron al ciberdelito, por lo redituable. Uno de los mayores problemas es la dificultad de hallar a los cibercriminales. Pueden estar en cualquier parte del mundo, separados por miles de kilómetros entre sí, anonimizados, además, la amenaza se “democratizó”: los potenciales blancos no se limitan a un banco o gran empresa. Los ataques pueden ser contra compañías de 20.000, 2.000 o 200 empleados, una pyme” (Diego Taich, 2021).



Fuente: Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)

Muchas veces el ataque no pasa a mayores, pero en otros casos se produce una cibercrisis: se para la operación de la organización y hay pedido de rescate, usualmente en bitcoins. “Ante la crisis, hay poca información de lo que pasó y hay que tomar muchísimas decisiones, que muchas veces no están protocolizadas, a diferencia de EEUU y Europa, donde hay más madurez al respecto. Del otro lado tenés tipos preparados, bien fondeados: es una lucha muy desigual entre una empresa que no tiene recursos infinitos y bandas que se dedican a eso y tienen todo el tiempo del mundo” (Diego Taich, 2021).

Un buen plan debe incluir desde la respuesta a los extorsionadores y la denuncia judicial hasta la comunicación pública. En primer lugar, se aconseja no acceder a la extorsión, porque incentiva la actividad y que vuelvan a extorsionar a la persona o empresa afectada. Pero en los últimos meses el mismo FBI reconoció que “en ciertas situaciones no queda otra que poner algo”.

Según Crowd Strike, uno de los principales proveedores mundiales de programas antivirus y soluciones contra el ciberdelito, el sector más atacado en el mundo es la Salud.

En situaciones extremas, se puede dar una “prueba” al extorsionador. Algunos acceden por un rescate mucho menor al inicialmente solicitado, pero la recomendación general es no pagar e involucrar a fuerzas de seguridad, que pueden hacer exhortos y accionar contra cibercriminales situados en otros países.

Costo promedio de una intrusión a la base de datos, según el porcentaje de empleados que trabajan en modo remoto (en millones de dólares)

Fuente: Ponemon Institute, IBM

Según un informe del Ponemon Institute, la probabilidad y costo potencial de una intrusión informática aumenta con la proporción de empleados que trabajan de modo remoto.

Daniel Monastersky, director de una diplomatura en Gestión y Estrategia en Seguridad de la Universidad del CEMA (Centro de Estudios Macroeconómicos de la Argentina) coincide en que “el Ramsonware es una de las preocupaciones más grandes hoy en las organizaciones, pero se puede minimizar mucho tomando ciertos recaudos. Entre ellos figuran el back up (copia de seguridad) permanente y doble factor de autenticación. También ayudan sistemas como “Zero Trust”, un concepto creado por la empresa Forrester que, a diferencia del modelo de “seguridad perimetral”, postula que las organizaciones no deben confiar en ninguna entidad, aunque sea interna, y deben delimitar datos, redes, dispositivos, operaciones, personas.” (Monastersky, 2021).

Un caso concreto de daño extremo ocurrió cuando 30 servidores del Hospital Universitario de Düsseldorf, en Alemania, fueron atacados por un Ramsonware que denegó la atención de un respirador a una paciente que, horas más tarde y por ese motivo falleció.

“Mi consejo, por temas de compliance, es que si un cliente sufre un Ramsonware, haga la denuncia penal de inmediato. Eso dispara, por ejemplo, un ciberseguro. Pero en casi el 100% de los casos no se llega a determinar el autor. Pueden ser chinos, rusos, coreanos, aunque también hay organizaciones que operan con ‘falsa bandera’. Organizaciones puramente locales

todavía no hay. En CABA, las denuncias de delitos informáticos aumentaron más de 500%, porque al haber más gente conectada desde su casa, los vectores de ataque aumentaron: hay más posibilidades de acceder y escalar". (Monastersky, 2021).

Una fuente de la Superintendencia de Tecnología y Delitos Informáticos de la Policía de la Ciudad también afirmó que "el ciberdelito dio un salto exponencial durante la pandemia a partir de que muchas personas no habituadas a operar por canales virtuales generaron muchas vulnerabilidades".

La recomendación siempre es no pagar. No solo por el efecto de incentivación, sino porque tampoco es seguro que el pago asegure la recuperación completa de archivos y sistemas.

Los ataques ocurren a menudo por descuidos y la mayoría no son teledirigidos, sino al voleo. Muchas empresas hacían trabajo presencial y no tenían problemas, pero con el trabajo remoto e ingreso por VPN y computadoras no actualizadas que navegan por sitios no seguros, descargan programas malignos o mails fraudulentos, el malware se termina infiltrando un sistema.

Costo promedio de un ingreso malicioso a una base de datos, por registro afectado (en dólares)

Fuente: Cost of Data Breach Report 2021, Ponemon Institute, IBM

El costo de un Ramsonware aumenta con la cantidad de registros de la base de datos afectada.

La dimensión exacta del Ramsonware en la Argentina es difícil de establecer, pero un informe de la Unidad Fiscal Especializada en Ciberdelincuencia, en septiembre del año actual, brinda algunos datos al respecto. La Unidad, a cargo del fiscal Horacio Azzolin, registró que "entre 2019 y 2020 aumentó 381% la cantidad de reportes de delitos informáticos, de 2.369 a 11.396 (de un promedio diario de 6,5 a 31 reportes). Además, entre abril de 2020 y marzo de este año hubo 14.583 reportes (aumento del 465%) y se iniciaron 289 investigaciones".

El aumento de la ciberactividad y el trabajo remoto fueron terreno propicio, explica la UCEFI, citando que “hacia mayo de este año el número de usuarios de Mercado Libre había aumentado un 40% y que según un informe de Google ya en octubre de 2020 un tercio de los argentinos encuestados había concretado su primera compra online y que la mitad había elegido esa modalidad “para minimizar las salidas” durante la pandemia. Además, según el BCRA, en 2020 las transferencias electrónicas aumentaron 90%, producto de un aumento de 86% en las de homebanking, 167% en las de mobile banking y de 227% en los pagos remotos con tarjeta de débito.” (UCEFI, 2021).

Las modalidades delictivas que más aumentaron fueron los fraudes mediante engaño. Las maniobras de phishing aumentaron de 244 casos en los 12 meses previos a la pandemia, a 1.079 en los 12 posteriores.

3.4 – TIPOS DE CIBERDELITOS

Según Gordon et. al. (2006), “Los delitos reconocidos tienen una gran diversidad de infracciones, lo cual hace más difícil su clasificación o tipología. Uno de los sistemas de clasificación es el definido por el Convenio sobre la Ciberdelincuencia, en el que se distinguen cuatro tipos diferentes de infracciones:

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.

2. Delitos Informáticos.

3. Delitos relacionados con el contenido.

4. Delitos relacionados con el derecho de autor.”

“Esta clasificación no es del todo coherente porque no se fundamenta en un criterio único para distinguir las categorías. De estas categorías, tres hacen referencia al objeto de la protección jurídica: ‘’delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos; delitos relacionados con el contenido; y delitos relacionados con el derecho de autor’’. La cuarta categoría, delitos informáticos, no se identifica con el objetivo de la protección jurídica sino con el método. Esta incongruencia hace que haya un poco de coincidencia entre las categorías” (Gercke, M. 2014).

3.4.1 – CIBERDELITOS CONTRA LAS PERSONAS FISICAS

Se entiende por ciberdelincuencia contra las personas aquella que comete un delito contra los principios básicos del individuo, teniendo un conjunto de características comunes, detalladas a continuación:

- Es una manera rápida de infringir mediante procedimientos fáciles de ejecutar a un costo reducido.
- Puede aportar elevadas cantidades de dinero bajo el anonimato como consecuencia de que la investigación de fraude habitualmente es tardía, existiendo un bajo porcentaje de éxito en su detección. Además, por lo general, no se denuncia de manera frecuente y las sentencias son leves

Los delitos mas comunes contra las personas físicas se describen a continuación:

- Acoso a menores o grooming: un adulto se hace pasar por un menor, ganándose la confianza del otro, coaccionándole para conseguir mediante chats, redes sociales o mensajería instantánea: imágenes o contenidos sexuales.

- Carding: consiste en adquirir algún producto o servicio mediante el uso de tarjetas de crédito pertenecientes a algún titular o producidos por algún programa informático. Por el contrario, está la venta de productos a través del comercio electrónico; el usuario realizará la compra y pago de un producto, pero este no recibirá nada, pues ha sido estafado.

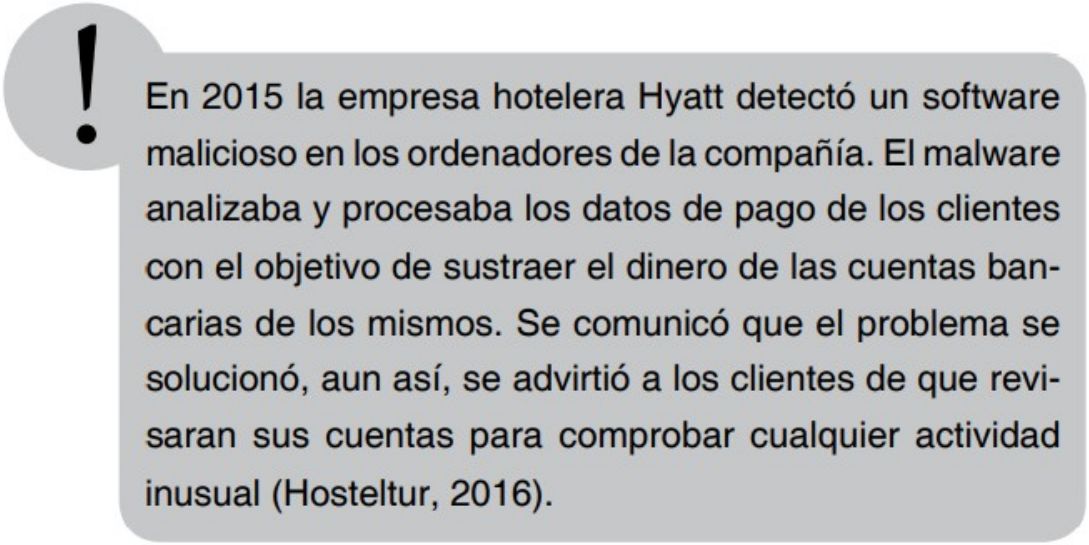
- Phising: se trata de adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información de tarjetas de crédito.

- Pharming: es la explotación de una vulnerabilidad en el software de los servidores DNS o en el equipo de los usuarios.

- Ataques XSS o estafas en la venta de productos: explotan la confianza del individuo que deposita en cierta página web.

3.4.2 – CIBERDELITOS CONTRA LAS PERSONAS EMPRESAS

La ciberdelincuencia contra las empresas se entiende como el conjunto de conductas relacionadas con el acceso, la apropiación o el intercambio de información en las redes, llevados a cabo sin el consentimiento o autorización requeridas, o haciendo un uso ilícito de la misma, que van en contra de una institución u organización.



En su gran mayoría, los ciberdelincuentes que atentan contra la empresa se aprovechan de la escasa formación del factor humano y de los mecanismos insuficientes de autenticación de muchas organizaciones, que van desde la gestión de salarios hasta la gestión de clientes, eligiendo de manera efectiva sus objetivos dentro de las organizaciones. La motivación económica es uno de los principales móviles por lo que uno de los objetivos más valorados es el robo de documentación e información susceptible de ser comercializada. No obstante, no se trata de ataques casuales que van dirigidos a todos los miembros de la organización, sino que es un proceso complejo que puede durar varios meses. El ciberdelincuente analiza el sistema que la empresa utiliza y decide el perfil del empleado a través del cual va a tener acceso a los datos, el puesto que ocupa dentro de la organización, la forma de comunicación, para posteriormente preparar su estrategia.

Aunque sus formas son variadas, los ciberdelitos más comunes y usuales en las empresas son los siguientes:

- En un 68% infección de equipos a través de programas maliciosos

De todos quizás el más conocido por su impacto mediático sea el Ramsonware (Ciberdelito de Ramson o Rescate). Un programa que encripta los datos de los equipos hasta el pago de un rescate en criptomonedas como el Bitcoin. En esta lista negra podemos añadir los programas que espían nuestros datos y comportamientos (Spyware) para venderlos a un tercero o los no menos famosos Virus: troyanos o gusanos que buscan normalmente la destrucción de la información almacenada en nuestros equipos.

- Un 15% de accesos no autorizados

Como fallos, deficiencias u obsolescencia de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota. Estos agujeros de seguridad pueden ser aprovechados por los ciberdelincuentes para acceder a los sistemas sin ningún tipo de limitación.

- Un 11% de fraudes

Estos fraudes cibernéticos o informáticos son realizados a través del uso de un ordenador o de internet. La piratería informática (hacking) es una forma común de fraude, en la que el delincuente usa herramientas tecnológicas sofisticadas para acceder a distancia a un ordenador con información confidencial. Otra forma de fraude se realiza mediante la intercepción de información en una transmisión electrónica, que puede ocasionar el robo de contraseñas, el número de cuentas bancarias o de tarjetas de crédito, u otra información confidencial sobre la identidad de una persona.

3.4.2.1 – CIBERDELITOS CONTRA LAS PYMES

Las PYMES desempeñan un papel fundamental en las economías nacionales. Cuando se les confía datos de sus clientes, estas empresas también tienen la responsabilidad de proteger esta información contra atacantes online. Sin embargo, como se detalla en el estudio comparativo sobre capacidades de seguridad de Cisco (2015), las PYMES muestran signos de que sus defensas contra atacantes son más débiles. A su vez, estos puntos débiles pueden poner en riesgo a los clientes empresariales que tienen. Los atacantes que pueden vulnerar la red de una empresa pequeña o mediana también podrían encontrar una puerta de entrada en una red empresarial.

Según los resultados del estudio comparativo sobre capacidades de seguridad de Cisco (2014), las PYMES utilizan menos procesos para analizar riesgos y menos herramientas de defensa contra amenazas de las que utilizaban el año anterior.

Por ejemplo, el 48% de las PYMES afirmaron en 2015 que usaban seguridad web, el 59% afirmó que lo hacía en 2014. Sólo el 29% ha dicho que usaban parches y configuración en 2015, en comparación con el 39% en 2014.

Además, de los encuestados de PYMES que no tienen un responsable ejecutivo de seguridad, aproximadamente una cuarta parte no cree que sus empresas sean objetivos de gran valor para los ciberdelincuentes. Esta opinión indica un exceso de confianza en la capacidad de su empresa para evitar los sofisticados ataques online actuales o bien que los ataques nunca ocurrirán en su empresa.

3.5 – HERRAMIENTAS Y TECNICAS PARA PROTEGER LA ORGANIZACION

A continuación, teniendo en cuenta la actividad delictiva en el ciberespacio, se definen y caracterizan las herramientas y técnicas utilizadas con más frecuencia en el ciberataque empresarial.

1. **Troyano**

Descripción: Tipo de virus que aparenta ser un software de ayuda o divertido para pasar inadvertido pero que en realidad está provocando daños o el robo de datos.

Síntomas: Aquellos terminales que se encuentren infectados por troyanos mostrarán algunas señales como que aparezcan o desparezcan archivos, que se ejecuten o se cierren programas sin razón aparente o que algunos periféricos dejen de funcionar. Estos son algunos de los muchos síntomas de un sistema infectado.

Riesgos: Su propósito principal es dar acceso remoto al ciberdelincuente a un sistema para que pueda usar otro tipo de software como un keylogger para registrar las teclas pulsadas y obtener información.

Métodos de prevención: Además de tener todos los softwares de tu ordenador actualizado, existen otras formas de protegerse de este tipo de ataques como no conectarse a una red Wifi abierta o diferenciar las cuentas de usuario de las cuentas de administrado, en caso de que se infecte la cuenta de usuario, el atacante no tendrá permisos de administrador y no tendrá un acceso completo.

2. **Troyano bancario**

Descripción: Una variedad del troyano que está orientado al robo de datos bancarios.

Síntomas: En general, al igual que el troyano clásico, la existencia de un troyano bancario en un sistema suele reducir la velocidad de este hasta el punto de que puede provocar errores entre los periféricos o algún software.

Riesgos: Tienen como principal objetivo robar datos privados de las cuentas bancarias de los usuarios. Utilizan diferentes técnicas para obtener los datos de acceso a todo tipo de entidades financieras.

Métodos de prevención: Este tipo de ataques se aprovechan de la ingenuidad de las personas, por lo que sería primordial la concienciación de los trabajadores y evitar descargarse archivos de páginas web poco fiables.

3. Rootkit

Descripción: Están diseñados para proporcionar a los hackers un acceso administrativo a la computadora sin el conocimiento del usuario.

Síntomas: La evidencia de un sistema infectado por un rootkit es más compleja de detectar, por lo que debería ser un programa antivirus el que detectara archivos ocultos, inicios de sesión ocultas al usuario o datos que se están enviando fuera de la terminal.

Riesgos: Da el control total de la terminal al ciberdelincuente desde el momento en el que se enciende el ordenador y dificulta la detección de otros archivos dañinos que haya en el sistema.

Métodos de prevención: Es necesario un programa que no solo analice los archivos del ordenador, sino que también debe controlarse lo que se hace al ejecutar cada programa.

4. Keylogger

Descripción: Un tipo de software usado para registrar todo lo que se escribe en el teclado, de esta forma los ladrones pueden leer cualquier información que se escriba, como contraseñas, tarjetas de crédito, correos electrónicos, etc.

Síntomas: Suelen presentar los comportamientos que comparten la mayoría de los virus informáticos, un uso excesivo del disco duro o de la red, un enlentecimiento del sistema o algún tipo de retraso en el comportamiento y uso del ordenador.

Riesgos: Quien controla este software puede ver que teclas está pulsando su víctima, de manera que junto a otro tipo de malware puede obtener contraseñas o incluso lograr tener acceso a los datos bancarios del infectado.

Métodos de prevención: Se debe utilizar un antivirus actualizado, evitar acceder a redes Wifi abiertas y no manipular información personal en ordenadores públicos.

5. Gusanos

Descripción: Se divide de manera similar a las células del cuerpo humano y se propaga a través de las redes de los terminales. Este tipo de malware es capaz de reproducirse a

través de algún medio de comunicación como, por ejemplo, el correo electrónico. Todo esto con la finalidad de infectar el mayor número de terminales posibles.

Síntomas. Para poder infectar una terminal con un gusano, primero ha de penetrar el sistema. Para ello se suelen enviar archivos por correo y, cuando se tratan de gusanos informáticos suelen tener una doble extensión, pero para poder observar esto, el ordenador debería tener desactivada la función de "ocultar las extensiones del archivo para tipos de archivos conocidos". Una vez infectado, un claro síntoma sería que la disquetera se abra y se cierre continuamente y sin razón aparente.

Riesgos: Se podría decir que el mayor riesgo de un gusano informático es su velocidad de propagación. Infecta un gran número de terminales y, combinado con otras herramientas, puede recabar información o llevar a cabo actividades perjudiciales para la empresa.

Métodos de prevención: Para evitar ser infectado por un gusano es recomendable mantener actualizado el sistema operativo en todo momento al igual que otros softwares que se tengan instalados. También se debe realizar una navegación segura y prudente, tratando de evitar páginas con dudosa reputación y evitar ejecutar archivos sospechosos, esto incluye los archivos adjuntos que recibamos por email.

6. Botnets

Descripción: Es el nombre con el que se denomina a un grupo de PC que estén infectados y sean controlados por un atacante de forma remota. Los ordenadores que forman la botnet son los llamados bots o zombies.

Síntomas: El ordenador vaya más lento de lo normal o que algunas aplicaciones dejen de funcionar son unos de los principales indicadores de que nuestra PC puede haber sido infectada y estar siendo usada como lo que se conoce como un "ordenador zombie".

Riesgos: Alguien puede estar usando la terminal de forma remota y puede conseguir datos personales que se guarden en el ordenador, puede ser utilizado para reenviar spam o infectar a otros terminales o incluso puede cometer otro tipo de delitos desde tu ordenador suplantando tu identidad.

Métodos de prevención: Mantener actualizado el sistema operativo, antivirus y tener unos buenos hábitos de uso son unas de las maneras de evitar ser infectado y convertir tu ordenador en parte de una botnet. También se debe evitar instalar nada que no se haya elegido, pulsar enlaces de emails cuyo remitente se desconoce o desconfiar de los anuncios sospechosos.

7. Backdoor

Descripción: Son accesos desconocidos por el usuario, dejados por el ciberdelincuente para poder acceder al sistema de su víctima en cualquier momento.

Síntomas: No tienen unos síntomas claros, dado que existen backdoors que han sido instalados a propósito para poder llevar a cabo tareas de mantenimiento o administración de forma remota.

Riesgos: Da un acceso que normalmente pasa inadvertido, al sistema que el ciberdelincuente puede usar para obtener información sensible de la empresa o llevar a cabo otras acciones perjudiciales.

Métodos de prevención: Es muy importante eliminar un backdoor por completo para eliminar cualquier posibilidad de fallar al intentar removerlo del sistema. Es recomendable disponer de un programa que realice esta limpieza de forma automática puesto que es muy difícil e improbable lograr eliminar un backdoor por completo de forma manual.

8. Sniffing

Descripción: En términos generales, el sniffing consiste en la detección o retención de toda la información que circula por una red. Una vez que se obtiene la información, se almacena y se interpreta para poder conseguir datos sensibles como contraseñas, información bancaria o cualquier otra información que pueda ser usada en beneficio del ciberdelincuente. Este método es uno de los principales que se realizan cuando se intenta robar información.

Síntomas: El sniffer entra a la PC a través de su instalación y para ello el usuario debe aceptar la instalación. En el caso de que se solicitara la instalación de un archivo sospechoso y se aceptara, existen programas que detectan el sniffer en el sistema o a través de la red.

Riesgos: El atacante obtiene acceso a la información almacenada en el sistema atacado, dejando información personal en manos del ciberdelincuente y podrá usarla de la forma que le plazca.

Métodos de prevención: Es recomendable no hacer uso de una red wifi pública dado que tal vez se trate de una red fraudulenta que esté esperando a que un usuario se conecte para poder capturar la información. También se debe evitar enviar información sensible a través de la red para no dar la oportunidad de un robo de datos.

9. Rogueware

Descripción: El rogueware es una aplicación que intenta parecerse a otra, por apariencia o nombre, para engañar a los usuarios.

Síntomas: Al tratarse de un programa que se hace pasar por otro, simplemente haría falta comprobar si el programa en cuestión está llevando a cabo con su función o que el programa sospechoso está usando más memoria de lo que debería.

Riesgos: Generalmente se utiliza para conseguir dinero, pero mediante esta estafa también se puede obtener información.

Métodos de prevención: Este tipo de programas intentan suplantar la identidad de otros softwares, por ello el principal método de prevención sería evitar descargar programas desde páginas no oficiales.

10. Adware

Descripción. Es un tipo de software gratuito patrocinado mediante publicidad que suele aparecer en ventanas emergentes, o pop-ups. La mayoría de las veces el adware es molesto pero seguro, aunque a veces se suele usar para recopilar información personal sin autorización.
Síntomas: Señales de que estamos infectados por un adware serían que nos saltan pop-ups de publicidad continuamente, que nos instalen barras de herramientas o añadan páginas como favoritos en nuestros navegadores.

Riesgos: Aunque no suele representar una gran amenaza, el adware pone la información personal de los usuarios a disposición de quien distribuya o publique el software, además de resultar muy molesto para la persona afectada.

Métodos de prevención: Se pueden eliminar manualmente, pero dependiendo del adware, puede resultar demasiado complejo. Por ello, existen programas que automatizan la eliminación de este tipo de software.

11. Spear phising

Descripción: Un ataque a una organización específica en la que el phisher simplemente obtiene detalles de un empleado y los utiliza para obtener un acceso más amplio al resto de la red a través de un envío de un email fraudulento u otras medidas.

Síntomas: Un empleado consciente de las amenazas que existen en la red, no tendrá problemas en identificar una acción de spear phishing. Esto gira alrededor de la ingeniería social y generalmente suele llevar a cabo sus ataques a través de correos electrónicos. Estos correos llegan a un empleado en concreto con la intención de que se descarguen el archivo adjunto y les permita entrar en el sistema. Es por esto que resulta de suma relevancia el instruir y concienciar a los empleados sobre los riesgos existentes.

Riesgos: El atacante obtiene acceso a la red a la que esté conectado la terminal infectada, pudiendo acceder a toda la información de esa red.

Métodos de prevención: Para prevenir ser atacados de esta manera, los empleados deben ser conscientes de que pueden recibir emails falsos que les pidan información. Algunos especialistas también recomiendan usar un buen gestor de contraseñas.

3.6 – COSTOS PARA UNA CIBERSEGURIDAD PRECISA Y EFICAZ

Los servicios de ciberseguridad pueden englobar distintos tipos de acciones orientadas a proporcionar un determinado nivel de seguridad o protección en el entorno digital.

En concreto, los expertos en ciberseguridad pueden ofrecer servicios relacionados con la identificación de vulnerabilidades, la protección de los sistemas, la identificación de incidentes o intrusiones, y la contención y recuperación frente a posibles ataques.

En su artículo de 2002, The Economics of Information Security Investment (Aspectos económicos de la inversión en seguridad informática), Lawrence Gordon y Martin Loeb de la Universidad de Maryland estimaron que, en la mayoría de los casos, la inversión óptima en seguridad informática es menor o igual al 36,97% de la pérdida esperada en caso de no haber seguridad.

Los costos varían depende la magnitud de la madurez de una empresa en cuanto a ciberseguridad, por eso depende mucho la evaluación de riesgos, amenazas y vulnerabilidades a las que se enfrenta la organización.

Muchas empresas invierten gran cantidad de dinero en tecnología, pero un empleado que haga click en un solo spam puede desperdiciar toda inversión posible. Por eso la concientización es un costo muy importante a tener en cuenta.

En base al EVITDA de la organización, se analiza cuanto se está dispuesto a invertir, que riesgos aceptar y cuales darle mayor importancia. Al aceptar riesgos nos referimos a darle menos énfasis a la hora de combatirlos ya que pueden tener poca ocurrencia en la compañía.

3.7 – RIESGOS

Dado el creciente número de ciberataques y violaciones de datos, la ciberseguridad es una prioridad para el logro de los objetivos empresariales de todos los sectores y por lo tanto ocupa un lugar privilegiado en la agenda las organizaciones. Los costos asociados con estos ataques han llegado a ser tan significativos que las empresas están centrando su atención en cómo proteger sus activos, en especial los datos sensibles: información personal, datos bancarios o de titulares de tarjetas, información financiera de la empresa, propiedad intelectual y cualquier otra información significativa que no es pública.

Los riesgos involucrados son graves y pusieron en alerta a las organizaciones, pero muchas de ellas no se sienten preparadas. Según la encuesta Harvey Nash / KPMG CIO Survey 2019, el presupuesto asignado por las empresas para temas relacionados con la tecnología ha aumentado. Un 14% de los encuestados indicó que el incremento está destinado a inversiones en ciberseguridad, por considerarlo un tema prioritario. Este informe además resalta que sólo el 26% de los líderes de TI sienten que están “muy bien preparados” para defenderse de un ciberataque.

¿Cómo pueden las organizaciones cerrar la brecha en la preparación para enfrentar los desafíos de la ciberseguridad?

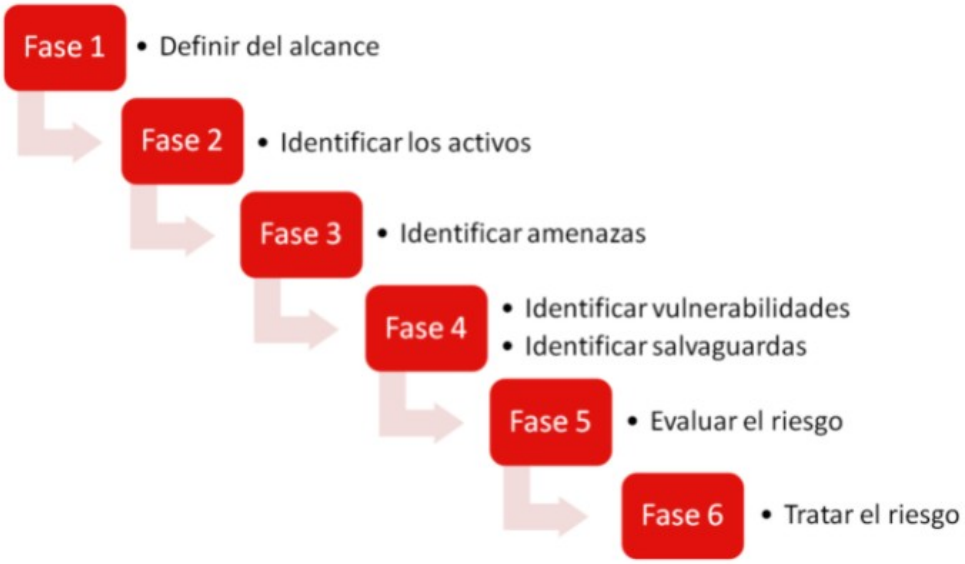
Las actividades que contribuyen a la violación de datos u otras formas de ciberdelincuencia incluyen el error humano, la intencionalidad política o criminal, las tecnologías emergentes o el cambio en los negocios, entre otros. Los Ciberdelincuentes han evolucionado desde criminales aislados o los script kiddies (utilizan programas y scripts desarrollados por otros para atacar sistemas de computadoras y redes) que apuntaban al robo de identidad, oportunidades de autopromoción o robo de servicios, a convertirse hoy en día en delincuentes organizados, activistas o personas con información privilegiada que se centran en la propiedad intelectual, la información financiera o el acceso estratégico a los recursos clave.

El análisis de riesgos es uno de los trabajos más importantes a la hora de definir proyectos e iniciativas para la mejora de la seguridad de la información. Si consideramos que las herramientas tecnológicas y la información que manejamos son de gran valor para nuestra organización debemos empezar a pensar en poner en práctica un Plan Directo de Seguridad.

El Plan Directo de Seguridad (PDS) se puede simplificar como la definición y priorización de un conjunto de proyectos en materia de seguridad de la información, dirigido a reducir los riesgos a los que está expuesta la empresa hasta unos niveles aceptables a partir de un análisis de la situación inicial. Llevar a cabo un buen análisis nos permitirá centrar nuestro foco de atención en los riesgos asociados a los sistemas, procesos y elementos dentro del alcance del PDS. De esta forma mitigaremos la posibilidad de tener algún tipo de incidente de ciberseguridad. Por otra parte, también podemos obtener beneficios si realizamos un análisis

de riesgos de forma aislada en lugar de llevarlo a cabo dentro de un contexto mayor como es el del desarrollo de un PDS.

A continuación veremos de forma sencilla las principales tareas del análisis de riesgos, aportando recomendaciones prácticas sobre cómo llevarlo a cabo, y considerando algunas particularidades a tener en cuenta para que aporte el máximo valor al PDS. Cabe señalar que las fases que componen un análisis de riesgos dependen de la metodología escogida por la organización.



Fuente: Instituto Nacional de Ciberseguridad (INCIBE)

Fase 1. Definir el alcance

El primer paso a la hora de llevar a cabo el análisis de riesgos es establecer el alcance del estudio. Vamos a considerar que este análisis de riesgos forma parte del Plan Directo de Seguridad. Por lo tanto, recomendamos que el análisis de riesgos cubra la totalidad del alcance del PDS, dónde se han seleccionado las áreas estratégicas sobre las que mejorar la seguridad. Por otra parte, también es posible definir un alcance más limitado atendiendo a departamentos, procesos o sistemas. Por ejemplo, análisis de riesgos sobre los procesos del departamento de Administración, análisis de riesgos sobre los procesos de producción y gestión de almacén, etc.

Fase 2. Identificar los activos

Una vez definido el alcance, debemos identificar los activos más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio.

Fase 3. Identificar / seleccionar las amenazas

Habiendo identificado los principales activos, el siguiente paso consiste en identificar las amenazas a las que estos están expuestos. Tal y como imaginamos, el conjunto de amenazas es amplio y diverso por lo que debemos hacer un esfuerzo en mantener un enfoque práctico y aplicado.

Fase 4. Identificar vulnerabilidades

La siguiente fase consiste en estudiar las características de nuestros activos para identificar puntos débiles o vulnerabilidades. Por ejemplo, una posible vulnerabilidad puede ser identificar un conjunto de computadoras o servidores cuyos sistemas antivirus no están actualizados. Estas consideraciones debemos tenerlas en cuenta cuando vayamos a estimar la probabilidad y el impacto en la empresa.

Fase 5. Evaluar el riesgo

Para evaluar el riesgo, una empresa dispone de los siguientes elementos:

- Inventario de activos.
- Conjunto de amenazas a las que está expuesta cada activo.
- Conjunto de vulnerabilidades asociadas a cada activo (si corresponde).
- Conjunto de medidas de seguridad implementadas

Con esta información, nos encontramos en condiciones de calcular el riesgo. Para cada par activo-amenaza, estimaremos la probabilidad de que la amenaza se materialice y el impacto sobre el negocio que esto produciría. El cálculo de riesgo se puede realizar usando tanto criterios cuantitativos como cualitativos. Pero para entenderlo mejor, veremos a modo de ejemplo las tablas para estimar los factores probabilidad e impacto.

Tabla para el cálculo de la probabilidad

Cualitativo	Cuantitativo	Descripción
Bajo	1	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio	2	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto	3	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Tabla para el cálculo del impacto

Cualitativo	Cuantitativo	Descripción
Bajo	1	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio	2	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto	3	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Cálculo del riesgo

A la hora de calcular el riesgo, si hemos optado por hacer el análisis cuantitativo, calcularemos multiplicando los factores probabilidad e impacto: RIESGO = PROBABILIDAD x IMPACTO.

Si por el contrario hemos optado por el análisis cualitativo, haremos uso de una matriz de riesgo como la que se muestra a continuación:

		IMPACTO		
		Bajo	Medio	Alto
PROBABILIDAD	Baja	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy alto

Fase 6. Tratar el riesgo

Una vez calculado el riesgo, debemos tratar aquellos riesgos que superen un límite que nosotros mismos hayamos establecido. Por ejemplo, trataremos aquellos riesgos cuyo valor sea superior a “4” o superior a “Medio” en caso de que hayamos hecho el cálculo en términos cualitativos. A la hora de tratar el riesgo, existen cuatro estrategias principales:

- Transferir el riesgo a un tercero. Por ejemplo, contratando un seguro que cubra los daños a terceros ocasionados por fugas de información.
- Eliminar el riesgo. Por ejemplo, eliminando un proceso o sistema que esté sujeto a un riesgo elevado.
- Asumir el riesgo. Por ejemplo, el costo de instalar un grupo electrógeno puede ser demasiado alto y por tanto, la organización puede optar por asumir.
- Implantar medidas para mitigarlo. Por ejemplo, contratando un acceso a internet de respaldo para poder acceder a los servicios en la nube en caso de que la red principal haya caído.

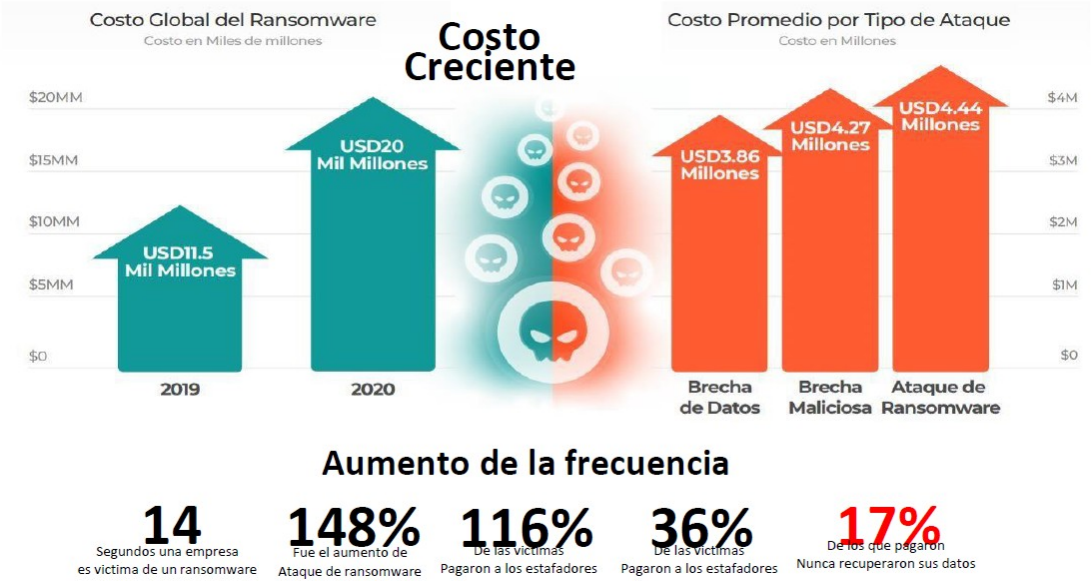
3.8 – CONSECUENCIAS ECONOMICAS DE LOS CIBERDELITOS

Hoy en día cabe considerar a la ciberdelincuencia como una especie del ‘impuesto’ sobre innovaciones, y de la misma, se produce el efecto inmediato de ralentizar el desarrollo de las innovaciones globales y reduce los ingresos de los inventores e inversores. En este sentido, constituye un hecho evidente que, en los países industrializados, cada vez más dicho fenómeno tiene un impacto directo, y afecta gravemente a la ocupación.

No hay que olvidar que, por ejemplo, la ciberdelincuencia ocasiona el mayor daño a las grandes economías, como las de EE. UU., China, Japón y Alemania, que pierden hasta 200.000 millones de dólares al año, según afirman los analistas, y especialistas de esta situación, donde además, se estima que los daños alcanzan la cifra aproximada de 150.000 millones de dólares, al año, solamente por los perjuicios derivados del robo de datos personales.

Las consecuencias económicas en las empresas pueden ser desbastadoras, provocando inclusive la pérdida total de la compañía.

Existen también las consecuencias de reputación, donde una empresa puede ver muy afectada su imagen luego de un ciberataque de pequeña o gran magnitud. Se verá afectado el posicionamiento de la organización y los clientes perderán confianza, abriendo el paso para la competencia.



Fuente: curso de ciberseguridad en Pampa Energía

3.9 – MARCO INVESTIGATIVO

3.9.1 – METODOS DE INVESTIGACION

Se utilizarán métodos de recolección de datos será mediante encuestas y Entrevistas con personal de seguridad informática, con preguntas abiertas y semiestructuradas. Considero que todos estos elementos son claves para poder profundizar en el desarrollo de mi trabajo y extraer datos de calidad.

3.9.2 – ANALISIS DE LAS ENTREVISTAS

En el desarrollo de la primera entrevista se buscará hacer énfasis en el día a día de una empresa relacionado con la ciberseguridad. La entrevista a realizar es una excelente fuente y podremos analizar la seguridad informática dentro de una organización en primera persona.

Con respecto a la segunda entrevista, nos sentaremos ante un gran especialista, el cual nos brindará una gran experiencia que nos permitirá poder introducirnos en el mundo de la Ciberseguridad desde el punto de vista de un consultor.

3.9.2.1 – PERSONAS ENTREVISTADAS

SANTIAGO LOPEZ GALANES

CISO (Chief Information Security Officer) en Pampa Energía.

LEANDRO DAMIAN POMPEO

Lead MLOps Engineer en Quadrant Health

3.9.2.2 – PREGUNTAS PARA LOS ENTREVISTADOS

ENTREVISTA A SANTIAGO LOPEZ GALANES

¿Cuál es tu rol en el área de Seguridad Informática?

¿Cuál es el objetivo principal del área?

¿Por qué es importante aplicar estrategias contra la ciberseguridad en las empresas?

¿Qué tipos de estrategias aplican en Pampa Energia?

¿Cuál es el riesgo de los ciberataques?

¿Qué costos puede tener llevar a cabo una buena estrategia de ciberseguridad?

¿Qué consecuencias económicas puede tener un ataque para la empresa?

ENTREVISTA A LEANDRO POMPEO

¿Cuál es tu visión sobre la Ciberseguridad en la actualidad?

¿Qué riesgos se le presentan a las empresas?

¿Qué costos tiene una buena protección ante los ciberdelitos?

¿Cómo ves a las empresas argentinas frente a la ciberseguridad comparándolas con otros países más desarrollados en el tema?

3.9.3 – ANALISIS DE LA ENCUESTA

El objetivo de esta encuesta es poder medir cual es nivel de conocimiento e involucramiento que poseen las personas que trabajan dentro de una organización, con respecto a la ciberseguridad, los riesgos a los que se enfrentan y las consecuencias que puede traer un ciberataque.
La encuesta se llevará a cabo a través de Google Docs, las personas encuestadas serán aquellas personas que trabajen en cualquier área de una empresa y puedan estar expuestas a cualquier tipo de Ciberdelito.

- **LINK DE LA ENCUESTA** https://forms.gle/RLBFmnWsQrC6fVj16

4 – ANEXO

4.1 - Entrevista a Santiago Lopez Galanes

¿Cuál es tu rol en el área de Seguridad Informática?

Mi rol en el área es asegurar la protección contra amenazas y riesgos de seguridad y ciberseguridad, que pueden poner en peligro la continuidad de los niveles de disponibilidad, rentabilidad y conformidad legal de la organización, asegurando los datos y la información de valor con un Sistema de Gestión de Seguridad de la Información.

¿Cuál es el objetivo principal del área?

El objetivo principal del área de Seguridad Informática es proteger la información de la empresa, brindando en todo momento disponibilidad, confidencialidad e integridad de los datos, acompañando el negocio en la captura de valor. Para garantizar la total confidencialidad en el sistema de información, se aplican cuatro métodos que son relevantes para cualquier formato de información:

1. Restricción o cierre completo del acceso a la información
2. Cifrado
3. Almacenamiento disperso
4. Ocultar el hecho de la existencia de información

¿Por qué es importante aplicar estrategias contra la ciberseguridad en las empresas?

El tener una estrategia de ciberseguridad te da una idea de cómo encarar los riesgos a los que se enfrenta la organización. Es importante al encarar una estrategia, analizar la madurez de la empresa. Esto es entender cómo se encuentra posicionada la empresa, en cuanto a ciberseguridad, tanto en la parte de IT y en OT (activos críticos).

Se revisan las políticas de la compañía, como cuidar de los activos y cuáles son los riesgos.

¿Qué tipos de estrategias aplican en Pampa Energia?

En Pampa Energia, la madurez se mide a través de un framework llamado NIST. Dado el resultado, se hizo un benchmarking contra empresas similares en Latinoamérica para conocer la media ya que la madurez se mide del 1 al 5. Pampa comenzó estando en un nivel bajo cuando se hizo por primera vez en 2019 antes de la pandemia. La última medición posicionó a la empresa en un nivel medio. Esto permite armar un programa de Ciberseguridad y poder ver en que hacer foco. Actualmente se está realizando un plan para que en los próximos dos años nos posicionemos en un nivel medio – alto.

Por otro lado, hay que desarrollar correctamente el equipo de Ciberseguridad dentro de la organización, donde hay una persona encargada de todo lo que es proyectos de negocio, proyectos de IT, área de ciberseguridad. Además, hay una persona encargada de la parte de Compliance, que son los procesos y las certificaciones SOX, otra persona dedicada a la concientización en la empresa y por último una persona que se encarga en la protección de marca de Pampa. Esto se refiere a como se encuentra la organización en internet y en la Darkweb, para que si alguien quiere utilizar la marca para realizar algún tipo de fraude, se pueda detectar y frenar a tiempo.

¿Cuál es el riesgo de los ciberataques?

Hay diferentes tipos de riesgos, pero los dos más fuertes en la actualidad son el riesgo de reputación y el económico.

Por ejemplo, un ciberataque que puede ser un Ramsonware que es muy común hoy en día, en el cual te cifran la computadora con datos relevantes y te piden un rescate, eso afecta financieramente a la compañía. En el caso de Pampa Energia pueden afectar directamente a los sistemas de control, que son los sistemas que operan las plantas y esto puede provocar hasta cortes masivos por la detención de las operaciones. Por este motivo la reputación de la marca Pampa, se vería completamente afectada, perdiendo credibilidad en el mercado.

¿Qué costos puede tener llevar a cabo una buena estrategia de ciberseguridad?

En cuanto a costos es impredecible, debido a la gran variedad de riesgos y estrategias a tomar. Por eso depende mucho tu proceso de madurez y evaluar los riesgos a los que se enfrenta la empresa, ver por donde comenzar a preparar la seguridad siempre teniendo en cuenta la disposición de inversión de la compañía.

Muchas veces se invierte gran cantidad en dinero en tecnología, pero si esta se aplica incorrectamente se convierte en un gasto ineficiente. Por eso la concientización es un costo muy importante a tener en cuenta.

En base al EBITDA de la organización, se analiza cuanto se está dispuesto a invertir.

Depende el nivel de madurez y la probabilidad de ocurrencia de las amenazas, se aceptan riesgos y otros se tratan con mayor intensidad. Si la probabilidad de ocurrencia es baja, se invertirá menos en ese riesgo y se hará foco en otro.

¿Qué consecuencias económicas puede tener un ataque para la empresa?

Hoy en día un ciberataque puede dejar en bancarrota a la compañía ya que puede haber perdidas por millones de dólares. Un ataque a los principales activos de la empresa podría parar todas las plantas de energía ocasionando desbastadoras pérdidas económicas y de reputación. La brecha de las consecuencias económicas es muy grande, puede ir de un soborno a un empleado del sector más bajo de la pirámide de la organización, hasta un director o a la compañía en general.

4.2 - Entrevista a Leandro Pompeo

¿Cuál es tu visión sobre la Ciberseguridad en la actualidad?

Considero que es una pregunta muy ambigua, dado que desde mi punto de vista, dependiendo del actor puede tomar un visión u otra. Por ejemplo, es sabido que las grandes corporaciones y los estados de diversos países están invirtiendo muchísimo dinero, tanto para la defensa como para el ataque. Ahora si uno considera empresas de proporciones más pequeñas o países con menor capacidad de inversión en este mundo uno puede llegar a notar mayor desconocimiento lo cual incrementa el riesgo sobre el mismo.

¿Qué riesgos se le presentan a las empresas?

Considero que esto depende mucho del bien de la empresa, pero para empezar, toda aquella empresa en donde su bien o parte del mismo (información contable, financiera, etc.) se encuentra o "forma parte" de un medio digital, es altísimo. He tenido la oportunidad de

trabajar en diversos proyectos como forense informático en compañías en donde la información vital de la misma había sido comprometida y como uno puede llegar a imaginar, en caso de no lograr revertir la situación, las perdidas en algunos casos eran prácticamente del 100%, lo cual puede generar el quiebre de una compañía.

¿Qué costos tiene una buena protección ante los ciberdelitos?

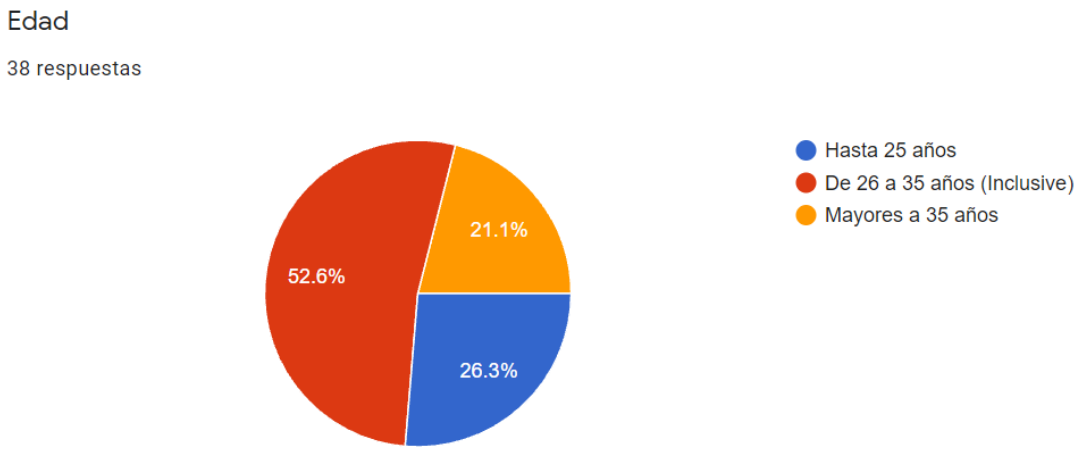
Es una pregunta muy relativa. El costo en general va muy de la mano del bien a proteger, y de cuan temprano o tarde se ataque el tema de la seguridad en el proyecto en cuestión. Generalmente esto suele llegar luego de que el producto se vuelve productivo y rentable, lo cual yo considero tarde. Un buen desarrollo de un proyecto es aquel en donde la seguridad es un factor fundamental desde el primer día.

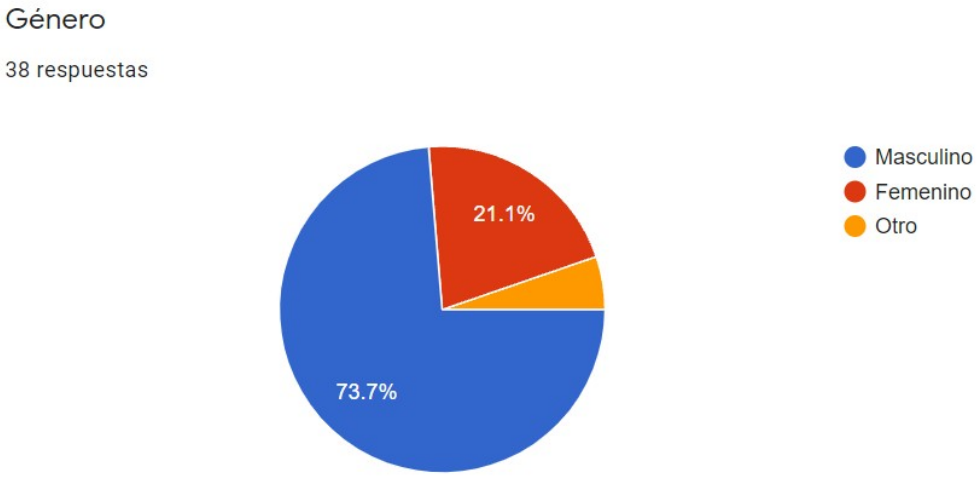
¿Cómo ves a las empresas argentinas frente a la ciberseguridad comparándolas con otros países más desarrollados en el tema?

Algunas empresas hoy en día, sobre todo las dedicadas a las finanzas están haciendo mayor incapie e invirtiendo más en ciberseguridad, pero aún desde mi punto de vista considero que en su gran mayoría la inclusión de la misma, es de pobre a nulo.

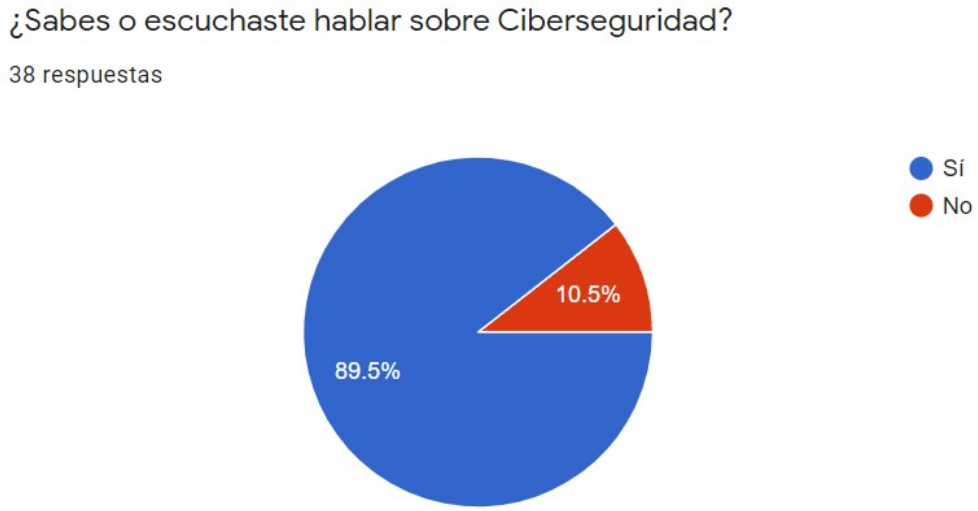
4.3 ENCUESTA

Los siguientes datos demográficos nos muestran que la mayor cantidad de respuestas obtenidas en la encuesta son de personas entre 26 y 35 años y en su mayoría son hombres. Estos porcentajes se ven reflejados dentro de las organizaciones.

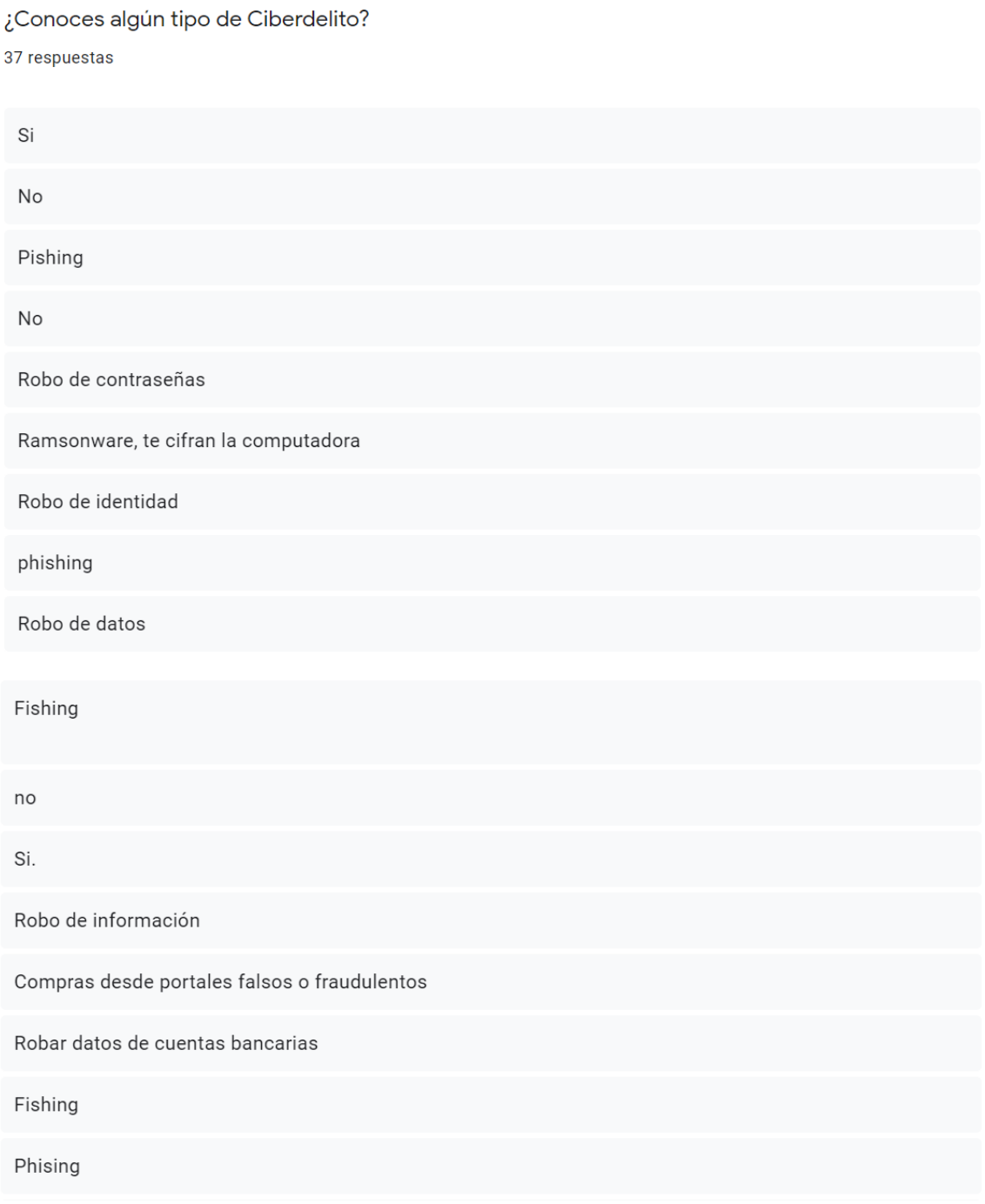




En la siguiente pregunta, identificamos de la población encuesta, cuales son los que conocen acerca de Ciberseguridad. Un 89.5% tiene un mínimo conocimiento o alguna vez escucho hablar del tema, el 10.5% lo desconoce.



En el próximo ítem, les pedimos a los encuestados, que indiquen algún tipo de ciberdelito en caso de que conozcan. Un gran porcentaje aportó con “Phishing”, robo de datos e información.



En la siguiente pregunta, pudimos comprobar que la mayoría afirma que las consecuencias pueden ser el robo de datos, estafas a cuentas bancarias y pérdidas de dinero. Aunque otro porcentaje un poco menor, desconoce las consecuencias que puede tener un ciberataque.

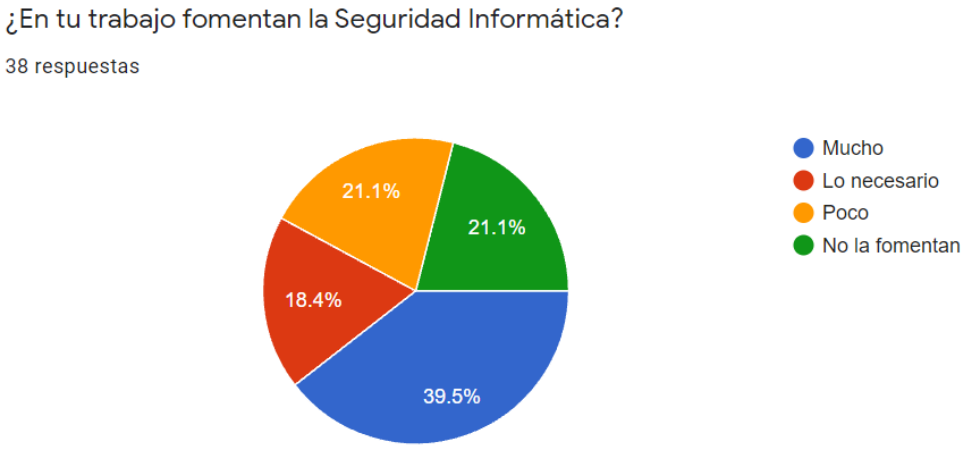
¿Sos conciente de las consecuencias que pueden traer los ciberdelitos? Por favor mencionar una en caso de saberlo.

38 respuestas

- No
- No
- no
- si, robo de dinero
- grandes consecuencias economicas
- Robar identidad
- Datos privados y robos multimillonarios
- No
- El robo de datos personales
- Lo mismo que cualquier delito dependiendo su indole
- Si, en mi trabajo nos hackearon y nos robaron mucha información.
- Perdida de datos bancarios
- Información confidencial de toda la compañía
- Si
- Cometerlos: preso
  Sufrirlos: pérdida de datos
- Robo de información personal
- Cárcel

No se
Estafas en cuentas bancarias
Robo de información
Mi compañía sufrió un ciberataque hace 1 año y estuvimos 1 mes sin operar.
Economicas
Si
Robo de cuentas bancarias
Pérdida de datos sensibles
Para el que los ejecuta normal mente son penas de varios años dependiendo el grado del delito

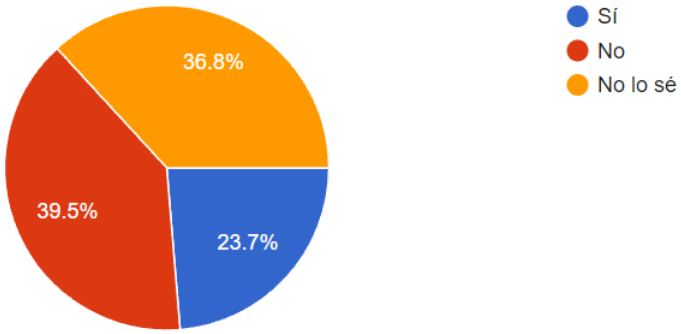
En el siguiente gráfico mostramos los porcentajes a los que apuntamos en el objetivo de esta investigación. Podemos observar que más de la mitad de los encuestados afirma que en sus trabajos fomentan lo justo, poco y directamente nada, acerca de ciberseguridad. Queda en evidencia la falta de conciencia por parte de las empresas.



En esta pregunta, vemos que es muy bajo el porcentaje que afirma que su información personal y la de la compañía se encuentran completamente protegidos, la mayoría opina que no.

¿Crees que tu información personal y la de la empresa se encuentra completamente protegida?

38 respuestas



En la última consigna, les pedimos que mencionen alguna medida que aplicarían en la empresa para comenzar a concientizar a los empleados, de las cuales rescatamos: Cursos y capacitaciones, campañas de concientización mediante mails, charlas informativas y simulacros de ciberataques.

Mencionar una medida que adoptarías en la empresa para concientizar a los empleados sobre Ciberseguridad.

38 respuestas

- cursos periódicos
- Campañas difusivas para concientizar
- Intentaria darles algun ejemplo donde se sientan identificados para que vean la magnitud del problema y entiendan de la importancia de atenderlo rapido en caso de que suceda
- Contraseña de 2 factores
- Pagar o poner a disposición una capacitación sobre el tema
- Actualizarse constantemente
- Que no usen herramientas de trabajo para cosas personales.
- no sé

Capacitarlos con personas encargadas sobre la protección de datos personales

Resguardar datos en la nube

Haría una charla para concientizar o pondria carteles informativos sobre el problema

Siempre frecuentar sitios abalados por entidades confiables. De lo contrario nunca ingresar informacion

Actualmente tenemos varias medidas, entre ellas la App de Authenticator.

simulacros de ciber ataques

Cursos obligatorios mensuales para los empleados y tomando algunos tests

Creación de contraseña robustas, backups

Invertir en seguridad de sistemas

Cursos obligatorios para concientizar sobre el tema

charlas trimestrales o semestrales de ciberseguridad obligatorias

Charlas informativas, videos cortos con info, recordatorios de activación de doble autenticación, prestar atención a cuentas oficiales y truchas.

Revisar el origen de los mails

Simulacro de estafa tanto empresarial como personal particular

5 – CONCLUSION

Durante el desarrollo del trabajo de investigación pudimos comprender el impacto que tuvo, tiene y tendrá la Ciberseguridad en las empresas. Fuimos analizando toda su problemática en general, desde su historia y evolución hasta sus consecuencias en la actualidad.

A medida que los Ciberdelitos se propagaban en sus inicios, crecía la variedad de estos ataques y aumentaban los riesgos en las organizaciones. Realizamos una breve cronología con su historia y antecedentes.

Analizamos el contexto actual a nivel mundial, y la situación en Argentina. Se pudo confirmar la falta de información y concientización en las organizaciones y sus empleados con respecto a Ciberseguridad. Esta escasez de conocimientos e ignorancia conlleva a consecuencias millonarias para las empresas y países de todo el mundo, ya sea potencias, países desarrollados y subdesarrollados.

Con el paso de los años, la incorporación de nuevas tecnologías, la globalización y la gran variedad de accesibilidades que se van desarrollando, los ciberdelitos aumentan y los atacantes buscan nuevas formas de infiltrarse y obtener sus beneficios. Por ende, las organizaciones deberán capacitarse cada vez más, los riesgos van a crecer y las estrategias tendrán que minimizar los márgenes de error con respecto a la ciberseguridad.

En cuanto a riesgos, es importante aplicar una buena estrategia de seguridad, tener en claro como se analizan para poder actuar de la forma más certera posible. Es importante detectar los principales activos y zonas a las que reforzarían la seguridad. Conocer las vulnerabilidades de la empresa y ser prácticos con las amenazas, ya que al existir muchas, tenemos que saber elegir cuales son las que tienen mayor probabilidad de ocurrencia y mayor impacto.

Verificando la hipótesis y el objetivo del trabajo, podemos confirmar y concluir con la importancia de la concientización e información en las empresas, para poder evitar la pérdida de información confidencial, ya sea de los propios empleados o de la compañía, y proteger los activos principales evitando consecuencias económicas desbastadoras y de reputación.

Es esencial que las organizaciones, PYMES y grandes empresas tomen conciencia y comiencen a darle la prioridad que merece la Ciberseguridad, comenzando con la difusión y la implementación de prácticas en las cuales se pueda llegar a los empleados. Promover una sinergia con respecto al plan de Seguridad Informática y generar cultura entorno a la confidencialidad de datos, sin dudas ayudará de gran manera a las compañías y podrán prevenir infinidad de ataques.

6 – BIBLIOGRAFÍA

Medidas para proteger la empresa – KPMG

https://assets.kpmg/content/dam/kpmg/mx/pdf/2018/04/ciberseguridad-servicios.pdf

Consulta: 01/09/2021

Definición de Ciberseguridad

https://nic.ar/es/enterate/novedades/que-es-ciberseguridad

Consulta: 01/09/2021

Evolución de los Ciberdelitos

https://es.eserp.com/wp-content/uploads/2019/09/conceptualizacion-evolucion-y-clasificacion-del-ciberdelito-empresarial.pdf

Consulta: 01/09/2021

Tipos de Ciberdelitos - Interpol

https://www.interpol.int/es/Delitos/Ciberdelincuencia

Consulta: 03/09/2021

Costos de Ciberseguridad

https://www.welivesecurity.com/la-es/2017/03/22/economia-de-la-ciberseguridad

Consulta: 03/09/2021

Costos de Ciberseguridad

https://www.cronoshare.com/cuanto-cuesta/servicio-ciberseguridad-empresas

Consulta: 03/09/2021

Consecuencias económicas

https://confilegal.com/20170725-los-danos-economicos-derivados-la-ciberdelincuencia/

Consulta: 03/09/2021

Ejemplos de virus

http://www.pandasecurity.com

https://www.elandroidelibre.com

Consulta: 10/09/2021

Cisco (2014): Informe anual de seguridad.

https://hackingetico.com//wp-content/uploads/2014/03/cisco2014_infosec_report. pdf

Consulta: 10/09/2021

Cisco (2015): Informe anual de seguridad

http://www.cisco.com/c/dam/global/es_es/assets/pdf/ asr_final_os_ah_es.pdf

Consulta: 10/09/2021

Coz F., Fojón E., Heradio, R. y, Cerrada, J. (2012): Evaluación de la privacidad de una red social virtual. RISTI, Edición Nº 9.

ITER CRIMINIS (2016): Deep Web

http://itercriminis.com/analisis-sobre-los-negocios-ilegales-en-ladeep-web/

Consulta: 13/09/2021

Situación en Argentina

Secuestros virtuales a empresas: una peligrosa amenaza global que tiene cada vez más impacto en Argentina - Infobae

Consulta: 13/09/2021

Riesgos - KPMG

Auditoría interna y los riesgos de la ciberseguridad (assets.kpmg)

Consulta: 13/09/2021

Amenazas y riesgos

https://www.ceupe.com/blog/cuales-son-los-objetivos-de-la-seguridad-de-la-informacion.html

Consulta: 15/09/2021

Gestion del riesgo

Gestión del riesgo de la ciberseguridad y un marco para realizar inversiones (infocyte.com)

Consulta: 15/09/2021

Como evaluar riesgos

El reto de evaluar los riesgos de ciberseguridad (theconversation.com)

Consulta: 15/09/2021