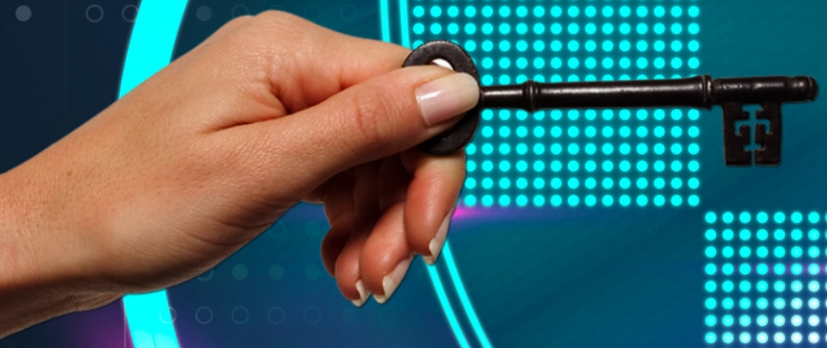
WHILOSOC

REVISTA DIGITAL N° 2

MARZO 2022



ÍNDICE

EDITORIAL

Autor: Margarita Vargas Martínez

Hablar de datos personales, qué querrá decir…les parece pensar en algún elemento con el cual nos identifiquemos, con los cuáles nos representamos y con qué otros nos destacamos de los demás. Les invito a abrir su mente y pensar…al nacer nos han dado un nombre, nos han asignado un número de rol único, rut, nos hemos identificado con ciertos elementos y características propias de nuestra naturaleza, como rasgos físicos, cualidades, colores de pelo, etc… con todo ello, nos hemos construido como seres distintos unos de otros. Al crecer originamos una historia, nos desarrollamos como personas y nos construimos con nuestras habilidades, elecciones, vivencias y gustos. Pensemos ahora, ¿cuánto de esta información queremos contar?, ¿cuánto queremos que se conozca en internet? Probablemente estén haciendo un recuento largo, a partir de la lectura de este texto. Esta invitación es la que quiero compartir, pensar en cuánto de nuestros datos, son para compartir por una red social, con los amigos, por email, o por algún otro medio…Ahora, qué pasa cuando los datos que nos pertenecen se mantienen a resguardo en otros lugares u organizaciones? ¿Pueden estas organizaciones dejar a libre albedrío información que nos pertenece o que no hemos permitido tener en su poder? ¿Qué hacemos con las organizaciones que poseen nuestra información, sin que sepamos de ello? ¿Cómo nos protegemos de estas situaciones? Preguntas como estas abren el debate de la importancia de los datos que nos caracterizan, la libertad y propiedad que nos da el derecho de señalar bajo consentimiento sobre quien maneje nuestra información y la manera cómo se trabaje con ella.

EDITORIAL

Características como estas, un poco aceleradas también por la pandemia y el uso explosivo de Internet nos dan a pensar, que el mundo y las necesidades humanas ya no solamente son físicas, sino que también se han vuelto como necesidades humanas, las del orden digital.

Desde la perspectiva regulatoria, en otras palabras, lo que el Estado debe favorecer a que se cumpla, todavía es una tarea pendiente y seguramente tardará un tiempo todavía en abrirse completamente la conversación. Pero, ¿qué pasa a nivel internacional? A nivel europeo, la situación es completamente diferente. Me atrevería a decir, varios años de ventaja. Existe un marco completo de cómo se deben proteger los datos y se exige su completo cumplimiento. ¿Qué sucede en Latinoamérica? Si bien existen iniciativas para abrir la conversación, todavía no podemos pensar en que exista un Marco similar al Europeo.

Por otro lado, ¿qué sucedería cuando existiera información publicada en Internet, que no queremos siga así?, ¿qué hacemos?...Ya se han visto exigencias en algunos países vecinos, en donde autoridades incluso, han pedido que la información que los involucra, sea eliminada desde Internet y en donde los Tribunales de Justicia han tenido que manifestar una postura sobre el tema. Ahora, si los datos nos identifican y nos representan, tendremos derecho a exigir que se permita el olvido de esa información.

Temas como estos y más, se han abordado en la 2da Edición de nuestra Revista, Whilosoc, en donde, los invito a leer y compartir y a comentar por nuestras redes.

El dato: La información que protegemos

Autor: Rosa Fuentes Valdebenito.

De acuerdo con la RAE, el dato, del latín datum, que significa "lo que se da"es "información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho"(https://dle.rae.es/dato).

Pero en la práctica, ¿qué entendemos por dato? El dato será el atributo de un objeto, persona, etc, como por ejemplo el color de un auto, la altura de una persona; también puede significar el valor de una variable, ya sea cuantitativa como la cantidad de hojas de un árbol, o cualitativa, el estado de completitud de un formulario, si se encuentra completo o no.

Por sí solo el dato no representa mucha significancia, pero un conjunto de datos en un contexto determinado, es decir cuando el dato está organizado, procesado, nos entregará información y esta información nos genera conocimiento. Es así, que el color de un auto, por sí solo no nos dice nada, no es relevante, pero en un contexto estadístico y sumado a la cantidad de autos vendidos al año (otros datos), nos puede indicar que en las preferencias de venta el color rojo ha disminuido y el blanco ha subido. Para nosotros esta información puede ser irrelevante, pero para una automotora, esta información se transforma en conocimiento útil y se tomarán decisiones corporativas respecto de esta información y, por ende, respecto de estos datos.

Es por esta transformación de dato a información y luego a conocimiento, que los ciberdelincuentes buscan nuestros datos, pero, ¿qué dato relevante puede tener una persona común y corriente?, más de lo que pensamos.

Poseemos datos personales, que son aquellos que nos individualizan como personas, nuestro nombre, rut, dirección, características morfológicas son los que nos hacen únicos en la sociedad, son nuestra identidad; datos laborales, que nos ubican en el ambiente laboral, dicen qué trabajo hacemos, dónde y qué tipo de empleado somos; datos médicos, que pueden ser objeto de discriminación frente a un trabajo o frente a la sociedad; datos económicos, que nos permiten acceder a la casa propia y que pueden mover la

El dato: La información que protegemos
Autor: Rosa Fuentes Valdebenito.

economía del país, de la misma forma que el aleteo de las mariposas provoca huracanes.

Si un ciberdelincuente tiene acceso a nuestros datos personales, puede tener acceso a nuestros datos económicos, y con ello, tanto nosotros como nuestros contactos, quedamos expuestos a ser víctimas de estafas.
Con nuestros datos laborales pueden acceder a nuestro lugar de trabajo. Cada uno de los datos que nos rodean pueden ser utilizados para generar daño o desestabilización, y nuestros datos están disponibles en el ciberespacio a través de nuestros teléfonos, redes sociales, bancos, colegios, hospitales, farmacia, etc., cada vez que entramos a un retail estamos ofreciendo nuestros datos.

¿Cómo los protegemos? Es importante estar al tanto de los datos que entregamos, a quiénes los entregamos, qué harán con nuestros datos y por cuánto tiempo lo almacenarán, en otras palabras, cómo gestionarán nuestra información.

Recordemos que nuestra información puede estar no solo en formato digital, sino que también en forma física. ¿Cuándo fue la última vez que destruyó una boleta de la luz antes de tirarla al papelero, o la etiqueta de la caja de pizza? En ambos casos datos personales quedan a disposición de cualquiera, al menos nuestro nombre, número de teléfono y dirección quedan en la basura, disponible para quien le interese realizar una práctica de ingeniería social: recolectar información para después atacar. Es por ello que es recomendable destruir todo documento que contenga nuestros datos antes de desecharlo.

Respecto de la información que manejan las empresas, parte de este manejo de datos se encuentra ahora regulado por el Reglamento General de Protección de Datos Personales, de la Unión Europea, producto de ello es que muchas aplicaciones durante los últimos años han cambiado sus términos legales y de privacidad, o en sus términos y condiciones al utilizar las cookies, o pequeños programas que recolectan/guardan información en nuestros dispositivos electrónicos.

Pero no basta con eso, sino con una actitud proactiva por nuestra parte, cuidando la clave de nuestra tarjeta al ingresarla en la maquinita de pago, o al dar nuestro RUT en el supermercado, o al dar nuestros datos en una encuesta telefónica de la cual no tenemos certeza que sea quien dice ser ni de la empresa donde dice trabajar.

Nuestros datos nos pertenecen, somos los dueños y los responsables de su seguridad, tenemos el deber de fiscalizar cómo se usan, quién los usa, para qué los usan, ya que a fin de cuenta, son nuestro tesoro.

DATOS PERSONALES, POLÍTICAS PARA EL FUTURO

Autor: Diego Cáceres Solís

En un día cualquiera, generalmente cualquier persona de este país puede recibir algún llamado telefónico ofreciendo algún tipo de servicio o producto. Este llamado, además, incluye un…Por ejemplo, en mi caso: "buenas tardes Sr. Diego Cáceres, lo llamo de una empresa X, ofreciendo un servicio" Dentro de mi ser, suele surgir la pregunta: ¿He dado mi teléfono y nombre a esta empresa? o…¿Cómo han logrado tener tan vital información personal?

…muchas preguntas y pocas respuestas…
Primero que todo, pasaré a explicar que son nuestros…"datos Personales" los cuales se podrían definir como cualquier tipo de información que puede ser usado para identificar de forma directa o indirecta a una persona, interesado, cliente o posible cliente. Algunos ejemplos sencillos de definir son: tu nombre, dirección de domicilio, número de teléfono, fotografías, etc. Algunos de ellos no tan sencillos de encontrar serían, por ejemplo, el correo electrónico o el nombre de usuario de algún servicio, por nombrar un par.

Actualmente, en nuestro país y tratando de dar una opinión bastante personal y de varios especialistas del área de la Ciberseguridad, debo reconocer que no se resguarda de forma adecuada el Derecho de Privacidad de los datos personales tal como sale descrito en nuestra Carta Magna que, está en servicio vigente actualmente. Recordemos que está en proceso la Convención Constitucional, la cual en unos meses debiese tener una nueva propuesta y ser ejecutado un Plebiscito para aprobar o rechazar dicha proposición.

Situación Actual

Las empresas o terceros que prestan algún tipo de servicio de utilidad pública se aprovechan a través de términos o condiciones que siempre al final de los contratos como usuarios, debemos aceptar de forma arbitraria para poder obtener el servicio. Por supuesto, es necesario nombrar que generalmente son bastante pocas las personas que se dan el trabajo de leer algún tipo de formulario o aviso al respecto, sino más bien, pasan al final del texto y dan clic en el botón de aceptar.
Estos términos o condiciones lo único que generan, son tratos o negocios entre varios de estos entes externos los cuales finalmente producen un intercambio de información logrando de una manera u otra obtener tus datos personales.

Otro punto a tocar, son las empresas que cuentan con muy poca (por no decir nula) seguridad digital, lo cual obviamente hace correr un riesgo bastante alto respecto al filtrado de información de los usuarios que contratan servicios con esa organización. Para que esto no ocurra, es necesario disponer o aumentar las penalizaciones o multas legales para estas entidades, objeto así se invierta en Seguridad de la Información, se cumpla la Triada de la Seguridad (Confidencialidad, Integridad y Disponibilidad) y finalmente, se proteja de manera directa los datos de sus usuarios finales.

DATOS PERSONALES, POLÍTICAS PARA EL FUTURO

Autor: Diego Cáceres Solís

Privacidad Digital

Sin duda también, tenemos que hablar de la privacidad digital, para ello tenemos que detenernos en el internet, concepto bastante grande, que engloba varios tipos de servicios en donde fluye una gran cantidad de información. Hoy en día, todas las personas, yo diría que, desde aproximadamente los 10 años de edad poseen un teléfono móvil con acceso a internet, en donde se van dejando rastros de nuestras búsquedas, redes sociales, comentarios en blog o foros, hasta el uso de un simple navegador web.
La Privacidad Digital, es el derecho de los usuarios en internet y el poder decidir qué es lo que se quiere que esté visible. La idea central, es evitar que terceros accedan a sus datos personales sin su consentimiento como también el tener el derecho a solicitar que se elimine toda aquella información que no se quiere ser vista o revisada por algún usuario externo, también llamado: Derecho al olvido.

Situación Ideal

Lo que se busca es mejorar la calidad de vida de las personas a través de un mayor y mejor control de acceso y derecho de los datos personales, elevando los estándares en materia de ciberseguridad, existiendo penalizaciones o indemnizaciones, dependiendo de las futuras leyes que se crearán tomando en cuenta este punto fundamental, que debe estar escrito de manera certera en nuestra Constitución.
Nuestra Carta Magna, en su posición de estructurar nuestro país, debe promover y ordenar respecto a temas como la Ciberseguridad y Datos Personales generando una cultura nacional y siendo el primer paso normativo en las futuras creaciones de políticas organizacionales.
Para finalizar, no está de más recordar a todos los lectores de este artículo y revista, que lean las condiciones y términos ofrecidos por las empresas, que tengan precaución con qué tipo de información publican en internet y además que verifiquen dentro de lo posible en los softwares a utilizar las configuraciones de accesibilidad o privacidad, objeto protegerse ustedes y a sus familias.

¿Es necesario invertir en seguridad de la información?

Autor: Oscar Bravo Lara

"Tranquilo, somos una empresa chica. Solo hackean a las grandes" "no te preocupes, a nosotros nunca nos va a pasar, si no somos un banco" "ya tenemos antivirus, ¿para qué más?" "no tenemos información importante que pueda ser de interés de terceros" Todo especialista en ciberseguridad ha escuchado en algún minuto alguna de estas excusas al presentar un presupuesto.

Con la expansión que últimamente han tenido la tecnología y las comunicaciones, el mundo empresarial ha optado por mover gran parte de sus operaciones al mundo digital. Ya sea mediante el uso de planillas u hojas de cálculos, correos electrónicos, mensajería instantánea o sistemas personalizados internos que facilitan las operaciones diarias. Esta 'migración' en general ha sido beneficiosa, pero también ha traído consigo múltiples potenciales riesgos.

Pero antes de entrar más en detalle, es importante revisar cuales son los principales pilares comprendidos en lo que se entiende por 'seguridad de la información' En primer lugar, dado que la tecnología ha permitido centralizar información, es importante asegurar que esta siempre se encuentre disponible (**Disponibilidad**, primer pilar básico). Enseguida, no es suficiente que dicha información se encuentre fácilmente a la mano, sino que además es necesario asegurar que esta solo sea accedida por personas expresamente autorizadas (garantizando su **Confidencialidad**, segundo pilar fundamental). Por último, es importante que la misma se mantenga inalterada frente a cualquier incidente (cumpliendo con el requisito de **Integridad**, último pilar base). Si alguno de estos pilares es afectado por cualquier razón, la confianza en la veracidad de la información se pierde.

Debido a esto, el gran objetivo de la seguridad de la información es garantizar que la información de cualquier empresa se mantenga disponible, inalterada y protegida en todo momento. Para ello, esta no solo cuenta con sistemas y softwares específicos, sino que también con otro tipo de herramientas y acciones, como el establecimiento de políticas, normativas o procedimientos internos, que permitan guiar y estandarizar el comportamiento de sus trabajadores, la instalación de antivirus, la implementación de IDS e IPS, la implementación de firewalls, la instalación de controles de contraseñas y controles de acceso físico, entre otras.
A la hora de implementar sistemas internos de ciberseguridad, es importante siempre saber que recurrir a una sola opción no garantizará una debida protección de datos. Al efecto, es necesario recurrir a una estrategia 'olística' en la cual se implementen distintas herramientas, como las mencionadas anteriormente. Esto es conocido como una estrategia de seguridad 'por capas' donde, en cada salto de 'capa' se agrega una nueva forma de protección, comenzando desde la protección física de las instalaciones hasta la protección del dato mismo que genera la información.
Este tipo de estrategias es lo que muchas empresas desconocen, quedando expuestas a potenciales incidentes como los siguientes:

Ataques Internos, en los cuales personas de la misma organización, voluntaria o involuntariamente, eliminan, modifican y/o desclasifican la información de la empresa; y

¿Es necesario invertir en seguridad de la información?

Autor: Oscar Bravo Lara

Ataques Externos, los cuales pueden ser a su vez focalizados o no focalizados. En general, en su gran mayoría este tipo de ataques son no focalizados, es decir, no van destinados a una empresa específica, sino que se propagan a través de la red, intentando infectar la mayor cantidad de dispositivos posibles (como en los casos de phishing y ransomware).

Hay que tener presente que en este último tipo de ataques (no focalizados) un atacante no se preocupa del rubro ni del tamaño que podrían tener sus potenciales víctimas al momento de actuar. Los malwares (ej. virus, troyanos, etc.) se liberan a la red con la esperanza de que alguien caiga. Si uno de éstos resulta ser una empresa chica, sin información 'interesante' no todo está perdido. Sus servidores pueden ser transformados en 'bots zombies' con los cuales realizar nuevos ataques en el futuro.

Dado lo anterior, es importante que las empresas comiencen a recapacitar y a tomar más en cuenta esta situación. Algunas recomendaciones prácticas para considerar en un inicio son:

Inversión en capacitación/concientización: Es fundamental hacer ver a los trabajadores que ellos son un eslabón más en la cadena de seguridad. Para ello, estos deben estar capacitados en los posibles ataques que pueden llegar sufrir y cómo actuar ante ellos;

Inversión en prevención: Enseguida, es importante implementar lo que se podría entender como herramientas 'no técnicas' para mitigar los ataques ya mencionados (internos y externos), dentro de las cuales se encuentran los distintos tipos de políticas (ej. políticas de contraseñas seguras, de respaldo de información, de uso de dispositivos propios, de uso dispositivos móviles, entre otras); y,

Inversión en seguridad: Finalmente, puede hacer la diferencia implementar adicionalmente las herramientas técnicas tales como sistemas de antivirus, sistema de detección de intrusos y tecnología SIEM (que permite revisar varios registros y poder detectar anomalías). Aquí es crucial tener en cuenta que la idea no es comprar tecnología simplemente por comprar. Hay que hacerlo considerando las necesidades, características y debilidades de cada empresa y su rubro particular.

La tecnología no para de evolucionar, y junto a ella surgen también nuevas formas de ataque. En los años 90, el simple hecho de tener antivirus bastaba para erradicar el 99.9% de las amenazas en internet, pero hoy ya no es el caso. Un estudio por parte de Kaspersky Lab y B2B, expuso que en el 2017 los ciberataques costaron más de 1.3 millones de dólares a empresas norteamericanas. Chile no está alejado de esta realidad. Según la empresa Kepler, los ciberataques en el país crecieron en un 40% a noviembre de 2017, y en un 60% a noviembre de 2018.

El robo de información es lamentable, pero hay medidas concretas que las empresas pueden tomar para evitarlo o mitigar sus efectos. Es fundamental tener en cuenta también que la información que una empresa maneja no es sólo la propia. Recuerde que los datos de sus clientes, quienes depositan su confianza en ellas, también forman parte de su información confidencial. Si alguna de ellas es atacada y esa información es robada, puede que la referida empresa se recupere de la pérdida monetaria que dicha incidencia produzca. Pero la confianza y el daño reputacional que ella sufra será más difícil de recobrar.

Fuentes Citadas:

https://www.latercera.com/pulso/noticia/ciberataques-pais-suben-60-2018-empresas-aumentan-inversion-25/458645/

Telegram vs Los Gobiernos

Autor: Luis Araneda V.

El uso de las RRSS ha crecido de forma exponencial durante los últimos 10 años y efectivamente desde hace al menos 3 años (inicio de la pandemia a nivel global) su uso y masificación ha crecido de una forma trepidante y literalmente a través de todo el globo.
El ser humano en su avanzar con el paso de los años, ha hecho cada vez más cercanas las herramientas que puedan ayudarlo a solventar sus necesidades de la forma más directa e inmediata posible.
De estas herramientas, el "Smartphone"(aunque irónicamente cada vez realizamos menos llamadas de voz) es de todas, la más potente, directa y eficiente que el ser humano podría tener en sus manos.
Desde poder comunicarse a Alemania o Japón, a poder revisar sus planillas de texto, el poder ver videos en altísimos formatos de reproducción (1080p a 4K en dispositivos que en ciertos casos, no son de gama alta), a poder dar a conocer nuestras opiniones y sentir, a través del "nuevo constructo tecno social" de nuestra época: las redes sociales en línea.
Uno podría pensar en el hecho de que no es algo nuevo, mal que mal, el ser humano desde su concepción como especie requiere de su relación con otros (símiles, pares, etc.) por ende el factor "social" innato del ser humano es sumamente fuerte, a pesar de exhibir en ciertas ocasiones, comportamientos "egoístas" en diferentes estratos de interacción como especie.
Pero la necesidad de pertenecer a "grupos" o sentirse en un entorno de comunicación e interacción entre personas, es algo que la humanidad como especie no puede dejar de lado y la tecnología en este caso, nos ha podido ayudar a crear estos increíbles "milagros", descritos anteriormente.

La pandemia del COVID-19 ha hecho que las mismas redes sociales, uno de los pilares del avance tecnológico y la globalización, sea un arma para combatir los efectos adversos de las políticas de aislamiento instaurados por los distintos gobiernos, en una forma de poder combatir la expansión de este virus; y las consecuencias en algunos países han sido devastadoras.
Una de ellas es el hecho de la salud mental en las personas y cómo éstas se han visto fuertemente impactadas por el hecho de no poder ver a sus amigos, familiares, cercanos y seres queridos.
Es entonces donde las RRSS aparecen en escena como posibles "salvadores", pero hay que recordar que en un mundo tan complejo y único como es la "internet", no todo es lo que parece.
Uno de los actores dentro de las redes sociales online es la aplicación "Telegram". Aplicación sería una forma simple de poder definir a Telegram, sin embargo, la realidad; como se dijo anteriormente, no siempre es "como la vemos".

Telegram vs Los Gobiernos

Autor: Luis Araneda V.

En realidad, Telegram es una plataforma de servicios, dentro de los cuales, la comunicación (o sea, las RRSS) es uno de sus principales componentes.
Sería fácil el poder dibujar similitudes entre otras opciones como Messenger (propio del "rey" de las redes sociales: Facebook) o WhatsApp (considerada como la "aplicación número 1" de mensajería instantánea a nivel mundial), sin embargo, a medida que empezamos a observarlas con mayor detenimiento los "parecidos" comienzan lentamente a desaparecer.
De acuerdo con la información que podemos obtener de la web sobre la "aplicación", Telegram fue lanzada en 2013 por los hermanos Nikolai y Pavel Durov. Anteriormente, ambos fundaron la red social rusa VK (competencia directa a Facebook), que abandonaron en 2014 tras denunciar que había sido tomada por los aliados del presidente Putin. Pavel Durov vendió la participación que le quedaba en VK y abandonó Rusia tras resistirse a las presiones del gobierno. Nikolai Durov creó el protocolo MTProto que es la base de la aplicación de mensajería, mientras que Pavel Durov proporcionó apoyo financiero e infraestructura a través de su fondo Digital Fortress. Telegram Messenger afirma que su objetivo final no es aportar beneficios, pero no está estructurado como una organización sin ánimo de lucro.
Desde el 2013, Telegram mantuvo una presencia moderada en internet, solo siendo usado por algunos grupos de usuarios, estos principalmente eran entusiastas de la tecnología o directamente, profesionales de la TI o ciberseguridad.
Tristemente a la vez, el programa se ha utilizado para actividades ilegales como la difusión de mensajes de odio, la pornografía ilegal, el contacto entre delincuentes y el comercio de bienes y servicios ilegales como drogas, contrabando y datos personales robados. Célebres son los casos como por ejemplo el uso de la plataforma por parte de ISIS desde Sept del 2015, en el 2020 el uso por parte de grupos neo-nazis, de extrema derecha, grupo de odio o que representaran ideologías de corte "fascista y autoritarios" para poder coordinar eventos, manifestaciones y reuniones secretas por parte de grupos norteamericanos (The Base, Proud Boys, etc.) así como en el "viejo mundo"; principalmente Inglaterra (TR.news, English Defence League y Britain First)
Muchos países han comentado su preocupación en referencia a las capacidades y uso mismo de la plataforma de "Telegram", ya que esta posee gran cantidad de características (grupos, canales, etc.) así como herramientas para poder utilizar de mejor forma el entorno que nos entrega la plataforma (bots, video llamadas, etc.), debido a que en muchos círculos, la aplicación es usada para poder evadir controles aplicados en ciertos estados a su ciudadanía, en el hecho de limitar "los contenidos que el pueblo puede ver", como lo es en el caso de naciones del medio oriente o China. Así como la presencia de la aplicación como protagonista principal en varios escándalos políticos a través del globo, como el cierre y apagón de la operación de bots políticos para las elecciones regionales de Rusia del 2021 o el celebérrimo escándalo de Puerto Rico "telegramGate"(también conocido como Chatgate o RickyLeaks) donde se filtraron cientos de páginas de un chat grupal entre Rosselló (Gobernador de Puerto Rico) y miembros de su equipo, el cual conllevó a la renuncia del entonces Gobernador.
En este mismo sentido, Telegram ha sido bloqueada temporal o permanentemente por algunos gobiernos, entre ellos Irán, China y Pakistán.

Telegram vs Los Gobiernos

Autor: Luis Araneda V.

El gobierno ruso bloqueó Telegram durante varios años antes de levantar la prohibición en 2020. Pavel Durov ha mencionado que quiere que "la aplicación tenga una herramienta anti censura para Irán y China, similar al papel de la aplicación en la lucha contra la censura en Rusia".

Una mención en particular son los "bots" que posee la plataforma. De acuerdo a la documentación oficial de Telegram, los bots son aplicaciones de terceros que se ejecutan dentro de Telegram. Los usuarios pueden interactuar con los bots enviándoles mensajes, comandos y peticiones en línea. Estos primeros son utilizados fuertemente por usuarios de la "red social" para poder conseguir información, archivos y datos de distintas posibles fuentes... Estas pueden obtenerse de forma abierta (mediante OSINT) o en ciertos casos, si hablamos de grupos privados o cerrados, directamente con el uso de técnicas de Ingeniería Social.

Uno de los gobiernos más preocupados de las "altas capacidades" que posee Telegram, es el gobierno Alemán, quien recientemente hace unas semanas, este mencionaba que estaba dispuesto a bloquear a Telegram, si este no hacía caso y no tomase la dirección de cumplir la normativa local que obliga a las RRSS a eliminar contenido ilegal por solicitud u orden de las autoridades correspondientes.

Es por ello que la Autoridad Criminal y Federal de Alemania (BKA) ha tomado la determinación de generar un grupo de trabajo (Task Force) encargada solamente de cubrir a Telegram y poder mejorar su capacidad de poder investigar cualquier tipo de delito dentro de esta plataforma, tal como se menciona en la declaración oficial de prensa de la agencia.

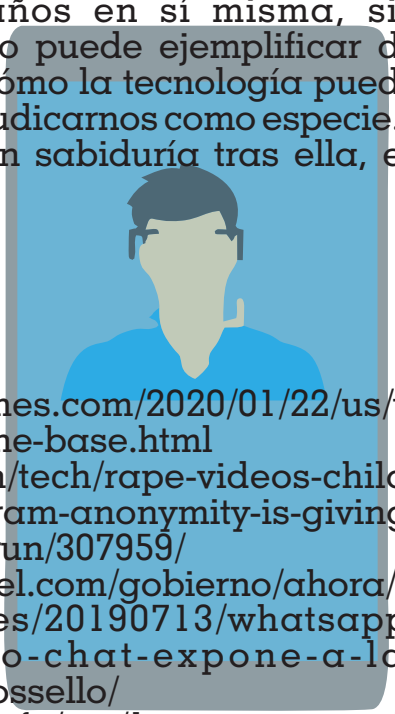
El mismo presidente de la BKA, Holger Münch acentúa que la pandemia ha contribuido al explosivo crecimiento del uso de las RRSS, así como también a la radicalización del pensamiento de personas y por ende el uso de redes o plataformas que puedan permitir el poder compartir este tipo de discursos.

Como comentario final, Holger Münch acotó: «El estado de derecho debe oponerse firmemente a este desarrollo. Estamos ansiosos por cooperar con Telegram, pero también tomaremos nuestras medidas si Telegram no coopera.»

Hemos de esperar que en el futuro, más naciones comiencen a tomar esta medida, ya que muchos de ellos están comenzando a observar el enorme potencial que pueden tener estas plataformas, tanto como para permitir su uso beneficioso en post de "comunicar a las personas y entregarles los medios para generar una "mejor internet", así como el posible y pernicioso uso que podrían darles ciertos grupos, con el propósito de poder esparcir "sus ideologías de odio, segregación y discordia".

Para cerrar, una potente frase la cual ya tiene muchos años en sí misma, sin embargo, esta no puede ejemplificar de mejor forma, el cómo la tecnología puede ayudarnos o perjudicarnos como especie.

"La tecnología sin sabiduría tras ella, es inútil..."



Luis Araneda V.

Fuentes:

https://www.nytimes.com/2020/01/22/us/white-supremacy-the-base.html
https://theprint.in/tech/rape-videos-child-porn-terror-telegram-anonymity-is-giving-criminals-a-free-run/307959/
https://www.noticel.com/gobierno/ahora/politica/top-stories/20190713/whatsapp-gate-2-0-nuevo-chat-expone-a-la-administracion-rossello/
https://www.rfi.fr/en/business-and-tech/20210918-telegram-messenger-blocks-russia-opposition-bot-during-vote
https://derechodelared.com/alemania-telegram-delitos/

PROYECTO DE LEY DATOS PERSONALES GOBERNANZA EN LA EMPRESA

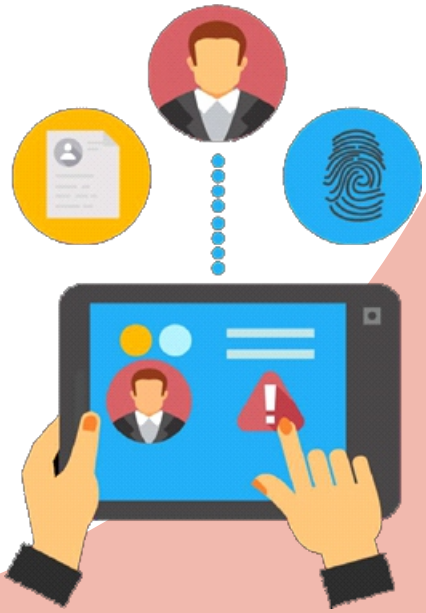
Autor: Juan Pablo López.

Hace unos días la Comisión de Hacienda del Senado celebró una Sesión en donde dieron cuenta las exposiciones del Ministro de Hacienda y del Consejo para la Transparencia en relación a las modificaciones legales de la normativa de datos en Chile. (Boletín 11144-07).
Más allá de alegrarnos que un proyecto de tal importancia en la actualidad avance en su tramitación, es importante hacer notar los aspectos que terminarán siendo decisivos para las organizaciones una vez que la nueva ley de Protección de Datos entre en vigor.

Seguramente parte del proceso será determinar los datos vitales para las empresas, pero el efecto inmediato será que los procesos tecnológicos deberán tener mayores y mejores formas de verificar que los datos, particularmente aquellos de carácter sensible o personales, sean adecuadamente obtenidos, resguardados y utilizados.

Entonces, ¿cómo se preparan las organizaciones para estos cambios normativos? Un punto de inicio es saber lo que tenemos, en qué cantidad y cómo los almacenamos. Ser capaces de conocer nuestra realidad nos abre la puerta al siguiente paso que es reconocer nuestros riesgos y definir qué haremos con ellos. Opciones para crear un sistema suficientemente robusto -desde el punto de vista del tratamiento de datos- implica un eventual cambio en la forma en que las organizaciones trabajan.
Clave será la manera en que las empresas logren integrar procesos de gestión. Adecuarnos a la normativa es siempre un desafío para las organizaciones. Entonces, volviendo a lo relevante, el principal riesgo estará dado por las nuevas sanciones que tendrán multas desde las 1 a las 10.000 UTM dependiendo de la clasificación de su gravedad y la reincidencia. ¿Podrán los equipos de tecnología y legales lograr un adecuado trabajo mancomunado para distinguirlos y gestionarlos? Es un desafío importante que cada empresa debería tener en mente.

Finalmente, desde el punto de vista del vigilante, pareciera ser que será el Consejo para la Transparencia quien deberá tener una doble función, con una mayor presencia en ambos aspectos. Si es una buena medida, lo analizaremos oportunamente.



Derecho al olvido en Chile, Utopía o realidad

Autor: Patricio Moraga Abarca.

En estos tiempos de grandes avances tecnológicos, donde los niños ya no usan juguetes de madera, si no sofisticadas herramientas tecnológicas, que hace cientos de años solo vivían en la imaginación de algún desfachatado escritor de ciencia ficción, las fronteras en la información se han disipado, o al menos, están más borrosas.

Esta es nuestra realidad, donde ya virtualmente no existen fronteras en la información y cada uno puede hablar al mundo entero si lo precisa.

Es en este contexto en donde nos encontramos actualmente, como nunca en la historia de la humanidad, nuestras acciones, opiniones e interacciones quedan de manera indeleble en internet y pueden ser accedidas por quien lo desee desde cualquier rincón del planeta.

Al igual que todo en el universo debe existir una dualidad, así como podemos ser parte de esta nueva forma de interrelacionarnos, debe existir y se hace cada vez más urgente que en nuestra legislación chilena se consagre el "**Derecho al olvido**"

En las varias legislaciones europeas y Norteamérica, ya existe este derecho y permite que los buscadores de internet no dirijan o muestren contenidos que se amparen en este derecho.

¿Pero qué es el Derecho al olvido?. En palabras de la Agencia Española de Protección de Datos:
"El derecho de supresión ('derecho al olvido') ... En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima"(Agencia Española de Protección de Datos, 2021)

Quizás puedas pensar en este nuevo "derecho al olvido"como algo trivial, pero en un mundo interconectado, es algo que raya en lo fundamental, pensemos en el siguiente caso:

«Tienes una vida relativamente tranquila y se te acusa de un crimen que no cometiste (cualquiera sea la naturaleza de este), es publicado en los Periódicos Digitales y Páginas de internet. Al verlo tus vecinos, compañeros de trabajo y amigos te marginan, pero después de pasar un tiempo se comprueba tu inocencia.»

Quizás en otro tiempo, pensaron en cambiar de vecindario y comenzar de nuevo; Pero ahora es un mundo "interconectado"(yo creo que entiendes a donde voy con este punto), los medios que difundieron tu supuesto crimen no

pondrán el mismo fervor al publicar que eras inocente, así que por la eternidad cuando alguien escriba tu nombre en cualquier buscador de internet, directamente en el resultado además de tu perfil de redes sociales aparecerán esas noticias donde se te acusaba del crimen del que eras inocente.

Desde mi punto de vista ahora miras con otros ojos este denominado "derecho al olvido" el cual podrías usar en este caso, para liberarte de la carga de esas acusaciones falsas, pero en nuestra legislación no existe dicho principio y lo más parecido que se puede efectuar en los tribunales Chilenos, es un recurso de protección, como el que interpuso el ex fiscal nacional Jorge Abbott contra Google, por aparecer en los resultados del buscador como "corrupto" lo cual terminó con el tribunal obligando a la gigante Google a desindexar los resultados. (Diario Constitucional, 2012)

En el año 2017 se ingresó un proyecto al congreso llamado "regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales."(Cámara de Diputados y Diputadas, 2017), con este se espera que se regulen estas materias y alcancemos al fin una figura que nos permita avanzar en la protección de nuestros datos personales y privacidad de nuestra información.

Referencias

Agencia Española de Protección de Datos. (17 de Mayo de 2021). *Derecho de supresión ("al olvido"): buscadores de internet | AEPD*. Recuperado el 2 de February de 2022, de https://www.aepd.es/es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido

Cámara de Diputados y Diputadas. (15 de mar de 2017). *Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales*. Recuperado el 2 de February de 2022, de https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=11661&prmBoletin=11144-07

Diario Constitucional. (30 de jul de 2012). *RECURSO DE PROTECCIÓN - DERECHOS Y GARANTÍAS CONSTITUCIONALES - ACTO ILEGAL Y ARBITRARIO - PROTECCIÓN DE LA VIDA PRIVADA, PÚBLICA Y HONRA DE LA PERSONA Y LA FAMILIA - DOMINIOS DE INTERNET - RECURSO ACOGIDO*. Obtenido de https://www.diarioconstitucional.cl/wp-content/uploads/2012/08/228-2012..pdf

Google. (2022). *Cómo retirar contenido de Google*. Obtenido de https://support.google.com/legal/troubleshooter/1114905

AWS "Princess" Macie, lecciones de la vida real

Autor: Jorge Andrés Flores

Cuando hablamos de la protección de datos personales en la nube, siempre me acuerdo de un artículo que leí en "The Guardian" (https://www.theguardian.com/technology/2008/jan/15/data.security)

hace millones de años atrás (es una exageración, quizás son más de 10) donde se hablaba de que los datos que las empresas reciben de sus clientes son cómo "desechos radiactivos" ... es algo a manejar con extremo cuidado.

Otra de las cosas que me vienen a la mente es la frase que escuché en un meeting en Puerto Rico hace cómo 5 años, cuando un CIO de una empresa bancaria muy importante en el Caribe dijo "A los CIOS ya no nos despiden cuando se cae un sistema, nos despiden cuando los datos privados quedan expuestos y hay un escándalo". Esa frase la repito en todas mis clases de seguridad en la nube.
¿Qué pueden decir las nubes públicas al respecto? Bueno, AWS (Amazon Web Services) tomó un paso adelante cuando entregó, cómo suele hacerlo, una de sus herramientas internas de detección de datos personales a la comunidad en la forma de un servicio de AWS. Pero las cosas no salieron cómo esperaban...
Cuando se lanzó, AWS Macie (su nombre ya es interesante, una referencia a princess macie) fue Fuente de muchas bromas en internet producto de su alto precio y dificultad de configuración. A más de US$ 8 por Giga y teniendo que configurarlo cuenta a cuenta y bucket a bucket, la verdad no daba muchas ganas de "setearlo". Así lo pensé la primera vez que lo vi... y seguí mi camino de "tener cuidado con los datos personales".

AWS "Princess" Macie, lecciones de la vida real

Autor: Jorge Andrés Flores

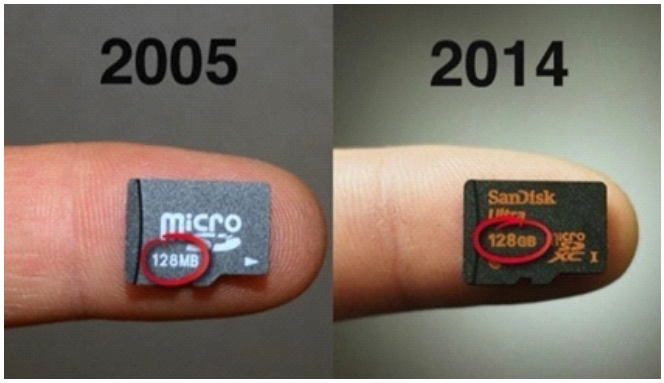
Hace unos meses lo revisité por una consultoría donde un cliente de un país donde hay un canal ( ) me pidió una estrategia de automatización para el control de datos personales. Dado que hablábamos de automatización y era un tema de seguridad y arquitectura, opté por buscar un fee que me permitiera ganar el proyecto y volver a experimentar con Princess Macie… perdón, con AWS Macie.
Esperen… ¿Que es AWS Macie?

¿Qué es AWS Macie?

AWS dice que Amazon Macie es un servicio de privacidad y seguridad de datos totalmente administrado que utiliza el aprendizaje automático y la correspondencia de patrones para descubrir y proteger sus datos confidenciales en AWS. En otras palabras, es un servicio automático que revisa el contenido de los buckets (y prontamente otros almacenamientos) en búsqueda de patrones personales.

Debemos contarle al inicio "que es para nosotros un dato personal", pero de allí en adelante aprende y hace este trabajo con rigurosidad alemana.

Es importante considerar que, con el crecimiento del volumen de información no estructurada, la tarea de custodiar este tema de manera manual es, en la práctica, imposible. Especialmente en la nube.



AWS "Princess" Macie, lecciones de la vida real

Autor: Jorge Andrés Flores

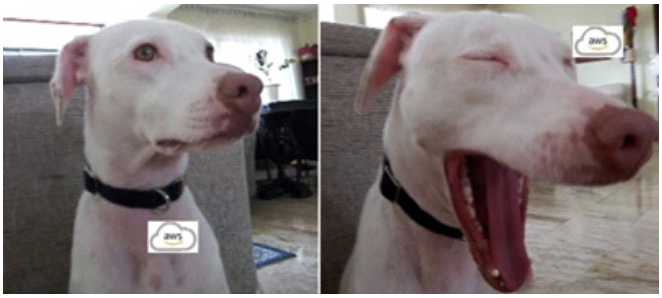
¿Pero… que ha cambiado en Macie desde esa primera vez?
Macie ha recorrido un largo camino desde la basura primera versión que lanzaron en 2018. Macie ahora permite que hacer delegación de administración (cómo muchos otros servicios de AWS). Tiene una buena API via Boto3 (¿por qué se llamará Boto3? Algún día lo googleare). Hubo una reducción de precio del 80% el año pasado llegando a US$1/GB (aún es super caro, cómo 10 o 100 veces más caro que guardar información en esa preciosura que es Glacier).

Además, agregaron criterios de filtro, por lo que puede crear trabajos de clasificación de datos confidenciales solo en depósitos públicos (ahorrándonos muchísimo dinero evitando pasar por aquellos buckets que por diseño pueden ser evaluados en su seguridad por otras herramientas más baratas cómo Config e incluso Inspector). La consola de Macie, aunque sigue siendo solo regional, proporciona buenas gráficas para la mirada de S3 y las proporciones para los buckets públicos y privados.

Así que mi primera mirada, en compañía de 2 litros de jugo de zanahoria con naranja (cómo siempre parto los proyectos) y de mi fiel perrita Manchitas (que algo de AWS habrá aprendido estos años), fue positiva: parece que no tendría que justificar tanto el modelo, podría costearlo efectivamente, y llegaría al nirvana de la automatización de revisiones de seguridad en las cuentas que mi cliente tecnológico-financiero quería.

Deteniéndonos un poco allí, sigue siendo duro vender este modelo: A $1 por GB, la clasificación de Macie sigue siendo, cómo dijimos antes, entre 10 y 100 veces más costosa que el costo de almacenar los datos. Este es un hueso duro de roer, los buckets públicos son un candidato obvio para el escaneo y establece un incentivo positivo para los equipos, que correrán con el costo en sus cuentas de AWS, para aprovechar mejores prácticas cómo CloudFront con Origin Access Identity (esto da para otro artículo).

Si podía decirle a mi contraparte que podía vender el proyecto cómo "Arregla los buckets o paga con sangre" podría ser un buen motivador.

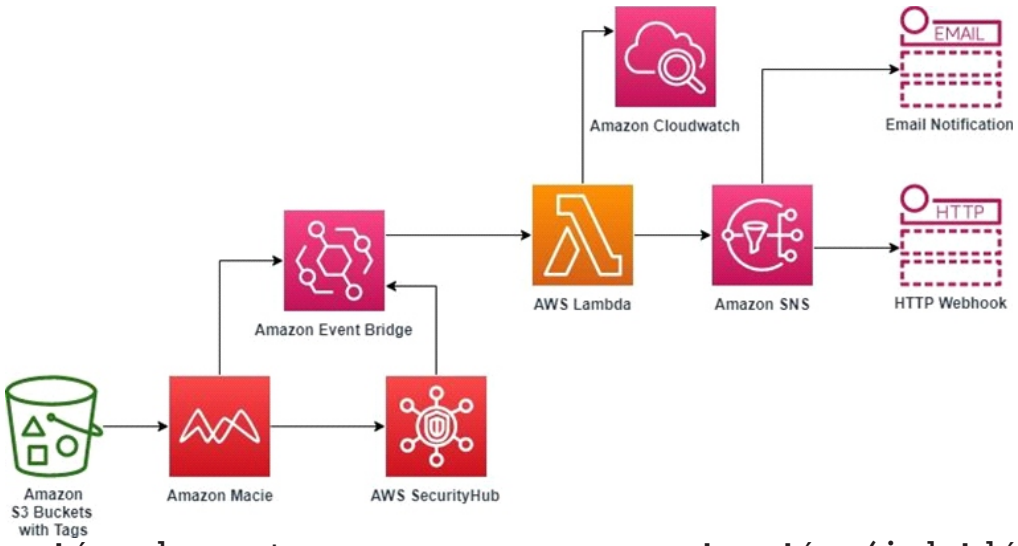


AWS "Princess" Macie, lecciones de la vida real

Autor: Jorge Andrés Flores

¿Qué aprendí del proceso?

Dos semanas después (no me critiquen, trabajo en los tiempos que me quedan) y 8 litros de jugo ingeridos, un modelo de automatización con Macie, Event Bridge (formerly parte de CloudWatch), Lambda, y SNS era realidad.



La descripción de esto es very straightforward: Los eventos de Macie son capturados por un evento en EventBridge que dispara una función de Lambda. Esa función gatilla la notificación en SNS y además establece las automatizaciones necesarias. También pueden saltarse la función de lambda y hacer una automatización de System Manager si es que el documento correspondiente existe. La notificación de SNS la pueden colocar cómo el siguiente target.

Del proceso me quedaron varias lecciones:

Trabajen con administración delegada.
Lo primero que se deberá hacer es habilitar la delegación, para eso tenemos que elegir una cuenta de AWS en su organización (¿olvidé decirles que siempre deben trabajar en modo organizations?) donde se enviarán todos los hallazgos de Macie. Aquí hay que setear adecuadamente los permisos y sobre todo partir con la correcta configuración de organizations).

Una vez que la cuenta que paga los bills delega a la cuenta de Macie (lo que debe hacerse para cada región habilitada), se debe configurar Macie para todas las cuentas secundarias en todas las regiones, de manera tal que pueda procesar dichas actividades. Es importante crear un bucket y una llave KMS CMK en su región principal para almacenar los hallazgos archivados (no olviden que debe estar encriptado).

AWS "Princess" Macie, lecciones de la vida real

Autor: Jorge Andrés Flores

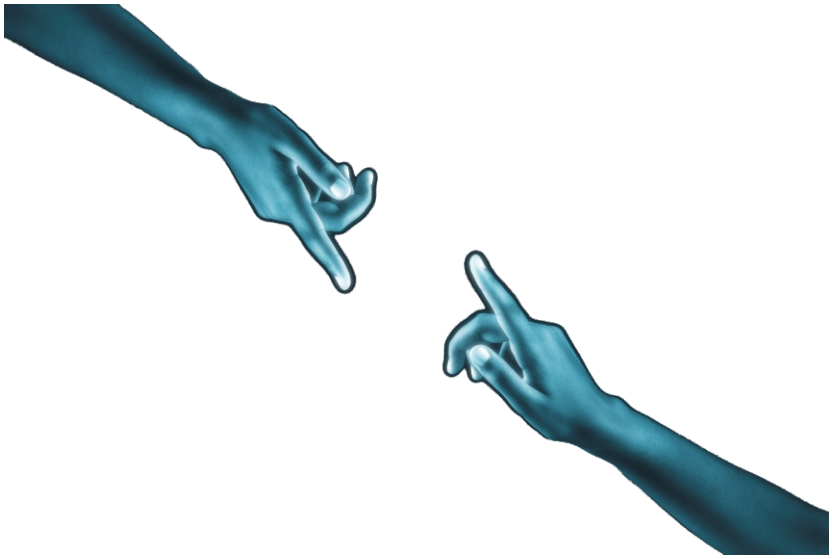
Estimen costos.

¿Hemos dicho que Macie sigue siendo caro? Yo creo que si … así que lo siguiente que hay que hacer es construir un estimado de costos por la ejecución de las automatización. Yo estaba obligado para colocarlo en el informe final de la consultoría, pero todos deberíamos hacerlo en los casos donde los servicios pueden aumentar significativamente los costos de la cuenta (les estoy hablando a ustedes, usuarios de IPs flotantes y appliances de proxys). Consideren que además de los costos por bucket, cada inspección tiene un costo adicional y el manejo de cuentas adicionales también.
https://aws.amazon.com/macie/pricing/

Entiendan los findings… de verdad.
Una vez que configuramos AWS Macie, algo tenemos que hacer con los hallazgos. En general, y si hemos configurado adecuadamente las búsquedas, tendremos muchos hallazgos y, lamentablemente, muchos serán falsos positivos. Tal cómo (call of) Guardduty, Macie envía eventos a ese servicio mágico que es Event Bridge (formerly CloudWatch Events) y de allí en adelante se llevan a cabo las funciones claves de seguridad de recordar y reaccionar.

En términos generales, hay dos tipos de hallazgos, aquellos relacionados con la configuración del bucket (Policy: IAMUser) y otro grupo para los temas de datos confidenciales (SensitiveData: S3Object).

A continuación, podemos ver un ejemplo del hallazgo tal cómo sería procesado por EventBridge (ejemplo completo en https://docs.aws.amazon.com/macie/latest/user/findings-publish-event-schemas.html#findings-publish-event-example-classification)n sangre" podría ser un buen motivador.



Privacidad y Protección – Uso de Datos – Uso de Información

Leocadio Marrero

Entrevista por Lidia Herrera Mateluna
Directora Carreras TIC's y Ciberseguridad
Inacap Valparaíso

CONCEPTOS Y DEFINICIONES

¿Qué es o cómo definimos DATO?

Dicho en términos económicos, diríamos que se trata de la unidad básica de un sistema, la materia prima. Por tanto, se trataría de hechos crudos que carecen de todo procesamiento.

¿Qué es INFORMACIÓN?

Es la materia prima procesada, organizada o estructurada que nos resulta de utilidad. Es capaz de transmitirnos un mensaje y, además, viene en auxilio de la incertidumbre, pues nos permite aumentar el conocimiento de una situación y, de esta manera, reducir nuestra incertidumbre.

¿Qué se entiende por **PRIVACIDAD DE DATOS, PROTECCIÓN DE DATOS Y SEGURIDAD DE DATOS?**

Pues va a depender del enfoque que queramos tener presente, no es lo mismo, si la visión la plasmamos desde la perspectiva de la seguridad, que cuando la plasmamos desde la perspectiva del derecho. Y, sin embargo, están relacionados. Me explico.

Desde la visión de la seguridad, la protección de datos se centraría en garantizar la integridad de los datos; la seguridad de datos se centraría en garantizar la confidencialidad y la disponibilidad de los mismos; y la privacidad de los datos estaría centrada en la clasificación de los datos y en su gestión interna y externa.

Ahora bien, desde la perspectiva del derecho, la protección de datos personales es un derecho fundamental relacionado con el concepto y derecho de intimidad pero cuyo ámbito excede al mismo ya que disfruta de naturaleza jurídica autónoma, entronca con la dignidad de la persona y genera una garantía de calidad de vida mínima. Por tanto, hablamos de un derecho que empodera al titular a controlar el flujo de informaciones que le concierne.

Y es precisamente ese derecho y esa capacidad de control, el que deriva en obligaciones hacia las organizaciones que necesitan recopilar datos personales para sus actividades. Esas obligaciones estarán encaminadas a: 1) garantizar la seguridad de los datos personales que se le entrega al recolector, en sus tres dimensiones (confidencialidad, integridad y disponibilidad) y, 2) garantizar la correcta gestión y respeto a los principios durante el ciclo de vida del dato y, por tanto, vestir de dignidad al titular de los datos.

Privacidad y Protección – Uso de Datos – Uso de Información
Leocadio Marrero

¿Qué se entiende por **PROTECCIÓN DE DATOS**?
¿Qué se entiende por **SEGURIDAD DE DATOS**?
Existen diferencias clave entre estos tres últimos conceptos, inclusive estos se superponen de cierta forma. ¿Cuáles serían? Obs:
https://www.computerweekly.com/es/definicion/Privacidad-de-datos-seguridad-de-datos-y-proteccion-de-datos

ENTRANDO EN MATERIA
¿Cómo podemos resguardar legalmente nuestros datos personales y/u organizacionales antes el uso de plataformas en internet para teletrabajo?
Hace falta un correcto análisis de riesgos. ¿Qué está en juego? Por un lado, las necesidades productivas de la empresa y la necesidad de evaluar el desempeño; por otro lado, las expectativas del trabajador de flexibilidad, comodidad y de privacidad, ya que, en la mayoría de los casos, el teletrabajo se presta desde el hogar del trabajador y digo bien hogar, ya que el trabajador hace su desempeño en el sitio que desarrolla su vida privada y/o familiar, por tanto, podría tener un impacto en otros miembros o componentes de la familia. Este elemento, por ejemplo, debería ser contemplado en el análisis de riesgos por parte de las organizaciones que, por motivo coyuntural por la pandemia, o por motivos estratégicos, hagan uso del teletrabajo.

¿Se puede aplicar lo mismo, dada los momentos actuales que vive la humanidad para la educación de los pequeños, adolescentes, los alumnos de educación superior, bajo la concepción de una clase virtual?
Me gusta la pregunta y el enfoque, muchas gracias. El entorno académico, especialmente cuando los alumnos son menores de edad, también deben ser contemplados en el análisis de riesgos, con la diferencia de que ese análisis debe realizarlo los estados que obligan a la escolarización del menor y que, por tanto, asumen la tutoría del alumno durante el horario académico. Por tanto, lo dicho anteriormente para el teletrabajo, debería ser contemplado a la hora de fijar el modelo, los medios y los objetivos del plan académico, no perdiendo de vista el público objetivo (menores de edad) ni las obligaciones legales que se asumen con la escolarización.
Y en ambientes de académicos con alumnos mayores de edad, nuevamente lo mismo, hay que realizar el análisis de riesgo, ponderar las necesidades de supervisión, monitoreo y calidad académica (control de exámenes, p.e.), con los derechos fundamentales de los alumnos y, cuando se quiera realizar alguna acción o implementar alguna tecnología, especialmente invasiva, se deberá optar por la menos lesiva como resultado de una evaluación de impacto de protección de datos.

Privacidad y Protección – Uso de Datos – Uso de Información

Leocadio Marrero

¿Cuál es el margen de la privacidad de datos y la libertad de información?

Se tratan de dos derechos fundamentales que deben convivir en un espacio reducido. El derecho a la información, al menos en el contexto constitucional español, incluye el derecho a expresar y difundir libremente los pensamientos, ideas y opiniones, así como a recibir libremente información veraz por cualquier medio. Ese derecho no es absoluto, cuenta con unos límites, como son el no uso del insulto y las calificaciones claramente difamatorias, o no desvelar aspectos de la vida privada o la intimidad, cuando no sean aspectos relevantes para la información.

Por tanto, es evidente de que ambos derechos, el de información y de protección de datos, parecen estar en constante tensión, puesto que la normativa de protección de datos busca, claramente, garantizar la privacidad de las personas y, por tanto, el conflicto puede surgir de forma inevitable cuando aparece el derecho a la información, porque las noticias e informaciones no viajan solas, viajan con información de carácter personal de los protagonistas de las mismas.

Es tremendamente curioso y muy revelador, que, precisamente, a raíz de una polémica protagonizada por el juez Samuel Warren, a finales del siglo XIX con la prensa norteamericana de aquel entonces, diera lugar al nacimiento del derecho a la privacidad. Parece que las cosas no han cambiado mucho desde entonces, pues ha sido el uso de las tecnologías en los medios de comunicación los que han 'asaltado' el vector de la privacidad de las personas en aras del derecho a saber.

¿Solución? Se necesita un "exquisito equilibrio" que garantice, por un lado, el derecho a la información y, por otro lado, el derecho a la protección de datos así como el derecho a la intimidad, ambos derechos independientes. Por ello, algo que podría venir a ponderar, especialmente en el los medios de comunicación, es la formación de los comunicadores en áreas del derecho y la ética que les afecta, así como entender los límites que el ejercicio, de cualquier profesión, especialmente de la periodística, tiene y que, por tanto, el "todo vale" no tiene cabida ni amparo en la actividad periodística ni en el derecho a la información.

¿Continuando con lo mismo, cuál es el margen entre privacidad de datos y la necesidad del sistema legal de obtener la información?

El derecho a la protección de datos plantea importantes condiciones y restricciones al ejercicio de las libertades informativas

porque estas implican la puesta a disposición del público de noticias e informaciones que pueden afectar a la privacidad de las personas a las que se refieren.

Privacidad y Protección – Uso de Datos – Uso de Información

Leocadio Marrero

Los datos personales son, actualmente, la savia de la información y la recogida, almacenamiento y difusión de esa información son actividades inherentes al ejercicio de las libertades informativas. Por ello, la normativa reguladora en materia de protección de datos tiene un impacto muy significativo en la actividad de los medios de comunicación con implicaciones tanto en la propia entidad como en el método de trabajo de los profesionales de la información como en la publicación y difusión de las noticias.
Los distintos pronunciamientos de los tribunales de justicia de los estados como internacionales están ayudando a visionar cuáles son los límites. Pero, ciertamente, estamos ante un escenario incómodo y estrecho y, por tanto, debemos conducirnos con cuidado, no todo puede ser derecho a la información y no todo es protección de datos…

¿Bajo lo indicado entonces, existe alguna instancia en que se pierda el derecho a la vida privada, al derecho al anonimato?
Si entendemos la vida privada, a los datos personales, sí que puede haber y debe haber esas instancias. Estamos ante un derecho fundamental que no es absoluto y que debe ser ponderado en equilibrio con otros derechos fundamentales. La pandemia de Covid19, por ejemplo, puede servir de ejemplo, ya que ha habido muchas actuaciones de los estados que han estado por encima del derecho a la protección de datos. ¿Por qué se ha producido? Porque en un ejercicio entre salud y protección de datos, prevalece la salud pública. Ya no solo en temas de Covid, pensemos en enfermedades peligrosas de fácil transmisión. Pues los estados modernos cuentan con leyes nacionales e internacionales en las que se deben comunicar los datos de aquellos pacientes a los que se han detectado determinadas enfermedades que forman parte de un catálogo. ¿Es un dato personal? Sí. ¿Es un dato sensible? Sí. ¿Necesita el estado el consentimiento del titular de ese dato para incorporarlo en su base de datos de alerta? No, porque prevalece el derecho de los demás sobre el individual, dicho de otra forma, prevalece el derecho a la salud pública sobre la protección de datos personales.

¿Qué determina que un dato sea sensible/personal/privado? Como por ejemplo en Chile, el ROL ÚNICO TRIBUTARIO (RUT) y el NOMBRE ya son públicos y este es solicitado en todo momento, en todas partes.
Es la propia naturaleza del dato y su impacto sobre el individuo lo que permite llegar a calificar un dato somo sensible. Desde la perspectiva del léxico jurídico, dependiendo del contexto normativo, nos podemos referir a 'categorías especiales de datos personales', o 'datos personales especialmente protegidos', que es como lo vierte el RGPD y la LOPDGDD respectivamente.

Privacidad y Protección – Uso de Datos – Uso de Información
Leocadio Marrero

Se trata, pues, de datos que, por referirse a aspectos especialmente sensibles de las personas físicas o que pueden servir de motivo para un trato discriminatorio o perjudicial para el interesado. Por tanto, requerirán de una mayor protección. Quiero incidir en su naturaleza, por eso en esa categoría entrarían origen étnico o racial, opiniones políticas, religiosas o filosóficas, afiliación sindical, datos genéticos, datos biométricos, datos de salud o datos de vida sexual. A nadie se le escapa la trascendencia que un mal uso de esos datos podría tener en la vida de una persona. De ahí que las legislaciones de protección de datos modernas requieren un consentimiento expreso reforzado para poder tratar esos datos y, la implementación de controles de seguridad reforzados.

En todo caso, y volviendo a la parte final de la pregunta, el número de identificación personal, como es el caso del RUT, estamos ante un dato personal que tiene la cualidad de identificar o de hacer identificable, directa o indirectamente, a su titular. Otra cosa distinta es si el RUT en sí mismo tiene la capacidad de tener el nivel de trascendencia antes descrito con un nivel de impacto en la vida de las personas equiparable a las opiniones políticas, datos genéticos o datos de salud, y, parece obvio que, siendo dato personal, no contiene en sí mismo esa capacidad de impactar en los individuos. Otro tema bien distinto es la 'cultura' de su uso que se ha extendido, por qué se recoge (finalidad), si hay o no base de legitimación, y si los recolectores actúan con lealtad, licitud y transparencia hacia el interesado.

COMO SUCEDE EN EL ÁMBITO INTERNACIONAL

¿Qué acciones se han realizado para regular los sistemas y contemplar la PRIVACIDAD, PROTECCIÓN y todo los relacionado para cumplir con la triada C-I-D?

Los principales cambios normativos con alto impacto en las organizaciones asocian la privacidad y la protección de datos, con la necesidad implícita de seguridad. De hecho se postula como un principio característico de la protección de datos. Por ejemplo, en el contexto del RGDP/GDPR, el artículo 32.B exige a la entidad que quiera tratar esos datos que entre las medidas técnicas y organizativas apropiadas que debe establecer para garantizar un nivel de seguridad adecuado al riesgo tratado, entre otras cosas, contar con 'la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento'.

Así que lo primero que se debe contemplar, antes de actuar, es que las distintas operaciones asociadas a la actividad de tratamiento supone un riesgo en sí mismo para las personas. Tomar conciencia de ello es el primer gran paso porque mientras no percibamos ese riesgo, no estaremos en la condición de mitigarlo.

Privacidad y Protección – Uso de Datos – Uso de Información
Leocadio Marrero

Lo segundo, y no menos importante, es que tenemos que entender que, aunque como organizaciones corremos un riesgo al recolectar y tratar datos personales, ese riesgo, el organizacional, no es el más importante aquí; el riesgo más importante es cómo impactan esas operaciones y actividades de tratamiento en los derechos y libertades de las personas.
Y, como tercer paso, contar con una metodología que nos permita gestionar esos riesgos de una forma eficaz y eficiencia, a la vez que nos dote de capacidad de evidenciar esa conciencia y de madurar el proceso con el paso del tiempo; y ahí viene en auxilio los marcos de gestión tales como los que propone la organización ISO en su norma ISO/IEC 27701 o ISO/IEC 29100.

¿Existe alguna guía recomendada para que un usuario sea capaz de gestionar su seguridad y su privacidad en el ámbito de las redes sociales o accesos a redes organizacionales, empresariales u otras?
Bueno, tal como he comentado antes, tenemos la enorme fortuna de que sí las hay. Además de tener los marcos antes descritos, contamos con otros como los que propone el órgano federal de USA en el NIST PRIVACY FRAMEWORK o más recientemente, CIS CONTROL con su propuesta de gestión de la privacidad.

¿Existe alguna organización que regule o establezca normativas generales y universales referente a Datos, seguridad, protección, etc.? ¿Qué países a la fecha son parte activa de este acuerdo?
Sí existen, de hecho, si tiramos de hemeroteca podemos ver cómo estableciendo una línea temporal, en al año 1980, el 23 de agosto, la OCDE estableció unos principios básicos sobre los que se debería construir el tráfico comercial y económico mundial cuando, para esas actividades, fuese preciso incluir datos personales y los mismos tuviesen que ser objeto de flujos de comunicación internacional. Esos principios fueron actualizados en el 2013. Y han sentado las bases para el desarrollo de distintos marcos legales internacionales, como fue en su día la Directiva 95/46, del 24 de octubre del Parlamento Europeo, que unificó el ejercicio y control de la protección de datos en Europa y sirvió de modelo a otros países, muy especialmente en Latam, para esbozar sus leyes nacionales.
También la OEA ha desarrollado trabajos intensos en esa dirección y en los últimos años han estado realizando aportes enriquecedores para ayudar los países miembros a tomar conciencia de la necesidad de ajustar las legislaciones nacionales, en unos casos, a legislar por primera vez y en otros, a modernizar sus marcos legales nacionales.

Privacidad y Protección – Uso de Datos – Uso de Información
Leocadio Marrero

Y, desde 2016-2018, el gran faro que ilumina a nivel mundial es el RGPD/GDPR, por su trascendencia internacional y su regulación, no sólo del derecho a la protección de datos en un mundo hiperconectado y digital, sino también como elemento que arroja luz sobre cómo se debe realizar el tránsito libre de datos personales dentro del espacio europeo. Esa capacidad de condicionar está cambiando las reglas de juego y está haciendo que los grandes y poderosos sectores mundiales cedan ante su poder regulatorio.

CONCLUYENDO
¿Es compatible la privacidad de datos con:

La ley de igualdad de género

Las instituciones relacionadas con análisis estadísticos por ejemplo en Chile INE

El derecho a secreto en las investigaciones legales/policiales

Con la ley de paternidad responsable

Las empresas audiovisuales, cine, televisión (Filman personas en la calle a diestra y siniestra sin preguntar a nadie)

El no uso de tarjetas, teléfono, RRSS, email..., puede una empresa obligar a alguien a entrar al sistema

Los casos de pederastas/violadores

Bueno, ahí hay muchas cuestiones que comentas, que tienen ciertos nexos comunes por su naturaleza, por ejemplo, datos de categorías especiales o sensibles, y como tal, sólo se podrán usar en aquellos casos que son pertinentes, en los que se cuente con una base legal de legitimación reforzada o por un mandato legal.

Luego hay cuestiones que son de dominio de los estados que entran en la espera del ejercicio de los poderes públicos o de su misión pública, como son los casos de las actividades policiales y/o judiciales. Estas actividades son legítimas para cualquier estado de derecho pero deberán realizarse con perfecto equilibrio con el respeto a los derechos fundamentales de sus administrados. En estas actuaciones, los estados deben ser ejemplo del respeto y locomotoras del impulso cultural de la privacidad en un mundo híper conectado.

Y, en lo que tiene que ver con las actividades privadas en el seno de las empresas y organizaciones, aquí nos encontramos ante la necesidad de equilibrar la situación, partiendo de la propia asimetría de la relación entre las partes. Los empleadores contarán con razones contractuales o legales para realizar ciertas operaciones de tratamientos; en otros casos, puede que el empleador se encuentre ante una causa legítima, por ejemplo, evaluar el desempeño del empleado; y habrá otros escenarios donde tenga cabida una relación simétrica y, por tanto, se requiera contar con un consentimiento del titular.

Privacidad y Protección – Uso de Datos – Uso de Información
Leocadio Marrero

En todo caso, el empleador tiene que estar en capacidad de demostrar por qué realiza esa operación, no desde su visión o necesidad, sino en perfecto equilibrio con el derecho fundamental a la protección de datos personales y a otros derechos y libertades individuales que puedan entrar en juego en esa ecuación. Cada caso debe ser analizado, evaluado y gestionado.

¿Se puede obligar a:

Alguien a dar consentimiento para obtener un dato personal/sensible?

o No, el consentimiento, como regla general, debe ser expresado de forma libre, específica, informada e inequívoca. No puede faltar ninguna de esas características.

Implementar bases de datos estadísticas y con el fin de no perder la información, existen casos de instituciones públicas/privadas que realizan tratamiento de datos, pero no realizan el borrado de datos personales?

o Debemos tener presente que uno de los principios que estructura la gestión y el gobierno en materia de protección de datos es el de limitación del plazo de conservación. Ese plazo debe ser informado, de forma transparente, en el momento de la recogida al interesado. Claro, puede que las instituciones, especialmente en el sector público o de investigación, precise mantener en el tiempo esa información por motivos estadísticos, históricos o para investigación. Cuando eso sea posible, debemos informar en la recogida al titular y, llegado el caso, vencido el plazo legal de conservación del dato, para poder integrarlo a nivel estadístico, debemos implementar medidas técnicas conducentes a desnudar de todo vestigio identificatorio de los datos, anonimizando el dato y evitando la reidentificación a posteriori. Y, en ese caso, revisar regularmente que la técnica de anonimización siga siendo válida, desde el punto de vista legal, y siga cumpliendo con la característica, desde el punto de vista técnica, de garantizar la no reidentificación.

¿Informar cuando un dato ya no pertenece a la institución?

El Reglamento general de protección de datos (RGPD) de la UE tiene como objetivo la regulación del tratamiento de los datos personales para proporcionar así uniformidad en la legislación sobre la protección de datos. ¿Cómo apoya a los países? ¿Qué exigencias se deben cumplir?

Antes de responder a la cuestión que planteas, una reflexión sobre el RGPD. El RGPD nació con la voluntad de que sus efectos se dejasen sentir mucho más allá de las fronteras de la Unión Europea. Eso se puede ver con claridad en el artículo 3 que define el Ámbito Territorial de la norma; en sus tres apartados deja muy claro que se regula todas las actividades de tratamiento realizadas en suelo de la UE, aunque se trata de personas no europeas, que transiten, física o virtualmente, por el espacio de la UE.

Privacidad y Protección – Uso de Datos – Uso de Información
Leocadio Marrero

Además, afecta a todas las entidades de la UE que actúen fuera de ella. Por tanto, la naturaleza de la territorialidad nos da un feedback importante del motivo de la aparición de la misma.

Se trata de una norma moderna con enfoque a riesgos, lo que vino a cambiar el criterio mantenido hasta ese momento, mucho más enfocado a cumplimiento, donde se pone al individuo, a la persona en el centro de la protección. Así se define en el Considerando 4 cuando se señala que el propósito del reglamento es "servir a la humanidad". Por tanto, el enfoque debe ser cambiado, no protegemos datos, no protegemos organizaciones, protegemos personas, es decir, servimos a la humanidad en su conjunto, y a la persona, en su plano individual.

El enfoque a riesgos obliga a las organizaciones a gestionar de forma adecuada los datos personales, lo que implica, necesariamente, implementar un marco de gestión, acorde al nivel de riesgo, que dote a las organizaciones de capacidad de 'demostrar' que el riesgo está adecuadamente tratado. Dota de flexibilidad a las organizaciones y se aleja de establecer el cómo para indicar el qué.

Por tanto, si me preguntas cuál es la exigencia principal, sin lugar a dudas es el principio del artículo 5.2 de accountability, o de responsabilidad proactiva, ahí radica el verdadero elemento diferencial y toda su esencia.

¿Cuáles son las recomendaciones que se pueden hacer desde el punto de vista legal si vemos vulnerados nuestros datos?

En esos casos, por desgracia muy habituales, especialmente en determinados sectores productivos y regiones, se hace necesario, primero, realizar un ejercicio de derechos, bien sean de acceso, rectificación, supresión, oposición, etc.. Claro, para que esos derechos puedan ser atendidos, las organizaciones deben contar, segundo, con procedimientos claros y operativos de atención de derechos; contar con un oficial de protección de datos o DPO se hace necesario, especialmente en organizaciones grandes o que gestionan volúmenes de datos personales. Y, como tercer elemento, debemos contar en el país con una autoridad de control independiente que sea tutor o garante del derecho a la protección de datos, con capacidad de exigir rendición de cuentas y de proteger verdaderamente este derecho fundamental. Para poder realizarlo, debe ser una autoridad independiente de los poderes públicos y, por tanto, libre de injerencias políticas y económicas.

¿Cuál es tu visión general de la protección de datos personales en las redes en Chile?

Los informes internacionales sitúan a Chile a la cabeza de la transformación digital en Latam, parece que esa es una realidad.

Privacidad y Protección – Uso de Datos – Uso de Información
Leocadio Marrero

La transformación digital conlleva la gestión de datos para generar productos y servicios personalizados a los clientes digitales. ¿Qué necesita el cliente digital? Necesita confianza y la confianza viene como resultado del ejercicio generoso de transparencia de las organizaciones, huyendo de cualquier matiz de opacidad; viene como consecuencia de la ética corporativa interiorizada en la cultura de la organización y comunicada a su clientela potencial; y de las políticas de gestión internas que pongan de manifiesto la voluntad inequívoca de aportar por el respeto de los derechos fundamentales. Claro está, y de las leyes, regulaciones sectoriales o contractuales.

Dicho lo anterior, Chile miró a la Directiva 95/46 para redactar su ley del año 1999, pero a la hora de gestionar el riesgo, es decir, el efecto de la incertidumbre sobre la consecución de los objetivos, Chile se quedó con la amenaza y no con la oportunidad. Me explico, tuvo oportunidad de ver en la regulación nacional una oportunidad para mejorar y modernizar la vida de sus ciudadanos, adoptando el espíritu de la Directiva 95/46; en cambio, hizo pero no hizo, se quedó a medio camino y cometió algunos errores, entre ellos, el propio nombre de la ley cita vida privada y no protección de datos, que sí es de lo que habla.

De todas formas, ha llovido ya mucho tiempo, más de dos décadas, y es el propio entorno económico, tecnológico y social el que ha dejado totalmente obsoleta la regulación nacional. Siendo honesto, en un ejercicio analítico de misión, visión y objetivos, la ley del 99 no ha cumplido con las expectativas en su momento y, actualmente, no cuenta con capacidad para regular de forma adecuada este derecho fundamental reconocido en la propia Constitución chilena en su numeral 19. Por tanto, se necesita una nueva regulación, una moderna, libre de sesgos o influencias de los poderes económicos y políticos, que ponga a la persona en el centro de la protección. En ese sentido, el marco propuesto por el RGPD puede servir, con sus errores y defectos, como un modelo sobre el construir la nueva ley o bien, seguir el modelo propuesto por la OEA que, dicho de paso, está alineado con los elementos más importantes del RGPD.

Por tanto, para lograr eso hace falta verdadera voluntad de los legisladores e independencia de estos para huir de los poderes y/o grupos de influencia y aprender de errores pasados.

¿Qué consejos puedes dar a nuestros lectores, pensando que existe una gran variedad de características en ellos?

El consejo es muy simple, tomar conciencia de lo que está en juego.

Tomar conciencia de que tenemos un derecho fundamental y que no se trata solo de nuestro derecho sino también del derecho de otros, pues se trata de un derecho colectivo. No es solo nuestro dato, sino lo que ese dato puede decir, ya no solo de nosotros, sino de nuestro entorno y de otras personas.

Privacidad y Protección – Uso de Datos – Uso de Información
Leocadio Marrero

Valorarlo, atesorarlo como algo que hemos logrado y que no podemos perder.

Comunicarlo a nuestro entorno familiar, social, laboral y económico.

Exigir su cumplimiento y no dejarnos seducir por las luces de neón de las ofertas y promociones, que esconden detrás sus verdaderas intenciones con dentelladas a nuestra privacidad.

https://www.linkedin.com/in/leocadio-marrero/
1. Lead Auditor ISO 27001 Sistemas de Gestión de Seguridad de la Información-BSI
2. Auditor ISO 27017 Seguridad en entornos Cloud-BSI
3. Auditor y Auditor Implementador ISO 27701 Sistemas de Gestión de Seguridad de la Privacidad- BSI.
4. RISK MANAGER ISO 31000 Sistemas de Gestión de Riesgos- PECB y Especialista en Gestión de Riesgos Legales ISO 31022
5. Gestión y Gobierno de la Ciberseguridad usando NIST CFM. USACH
6. CIBER SECURITY FUNDATION CSFPC
7. LEAD CYBERSECURITY PROFESSIONAL CERTIFICATE LCSPC
8. Profesor homologado de la Fundación Incyde y Director de programas de formación.
9. Profesor en la Escuela de Prácticas Jurídicas del Colegio de Abogados de Las Palmas.
10. Académico del Diplomado de Gestión y Gobierno de la Ciberseguridad en USACH.
11. Director del Diplomado de Privacidad y Cumplimiento en Capacitación USACH.
12. Especialista en Protección de Datos Personales; Implementador Líder ISO 27001 e Implementador Líder ISO 37301 por AENOR
13. DPO/DPD del ICALPA, Consejo Canario de Colegios de Abogados, COIICO, COAATGC, COITIC y otras entidades.
14. Especialista en Ciberseguridad Industrial en SGCI y Auditoría. Categoría Profesional Nivel Verde del CCI y Coordinador para Canarias del CCI.
15. Miembro fundador de APEP, Asociación Profesional Española de la Privacidad; del ISMS FORUM SPAIN y miembro del CCI, Centro de Ciberseguridad Industrial. Miembro de ISACA MADRID, de la AEC y de la aeDPD.
16. CIBERCOOPERANTE del INCIBE.
17. Consultor especialista en G.R.C.- Gobierno, Riesgo y Cumplimiento.
18. Gestión y Gobierno de la Ciberseguridad en COBIT2019. USACH
19. Implementador Líder ISO 27001. USACH
20. CDPSE. Ingeniero certificado de Soluciones de Privacidad de Datos. ISACA
21. Gestión Estratégica de la Ciberseguriad. USACH
22. Implementador Líder ISO 22301 Gestión de Continuidad del Negocio.USACH
23. Implantación de Sistemas de Canales de Denuncia ISO 37002
24. DIPLOMADO EN IMPLEMENTACIÓN DE SISTEMAS DE GOBIERNO Y GESTIÓN DE CIBERSEGURIDAD por USACH
25. Embajador Internacional de SOCHISI

Reseña Biográfica Autores

Patricio Moraga Abarca
Trabaja actualmente como Encargado de Informática en el área del servicio público. Con un gusto particular por compartir sus conocimientos mediante foros y redacción de artículos, es miembro fundador del Equipo de Hácking Ético, DolGuldur CTF Team, participando en distintas competencias a nivel internacional e internacional, destacando el 5to lugar obtenido en el CTF de la Kavacon - Uruguay, y el 2do lugar en el CTF del Innovapolinav. De profesión Programador, actualmente está cursando ingeniería Ciberseguridad y Diplomado de RED TEAM.

Rosa Fuentes Valdebenito
Trabaja actualmente como Encargada de Seguridad en el sector público y Docente en él área de la Carrera de Ingeniería en Ciberseguridad. De profesión Ingeniera en Informática, obtuvo el 2020 el grado de Magíster de Ingeniería en Seguridad de la Información. También cuenta con Diplomaturas en: Desarrollo Seguro; en Estrategia de Ciberseguridad e Inteligencia en Cibercrimen.

Oscar Bravo Lara
Ingeniero Civil Informático, Diplomado en Gestión de Seguridad de la Información de la Universidad Adolfo Ibañez y Máster en Ciberseguridad IMF Business School (Madrid, España). Cuenta con certificaciones en Ethical Hacking. Experiencia liderando proyectos de ciberseguridad, desarrollo y automatización de procesos bajo metodología Agile, con amplios conocimientos de ISO 27001 –27002, y Cobit. Destaca sus habilidades de liderazgo de equipos multidisciplinarios, capacidad de visualizar las potencialidades en equipos para lograr adecuada distribución de carga y eficiencia en procesos, capacidad de análisis estratégico y de visualización de áreas de mejora y vulnerabilidad, y foco en el cumplimiento de compromisos acorde a objetivos y presupuestos de la empresa. Inglés Avanzado.

Jorge Andrés Flores Zepeda
AWS Solution Architect, Security Specialist. Director del programa de Arquitectura y Seguridad en la Nube de Capacitación Usach. Director de los programas de Herramientas DEVOPS en la Nube y DEVSECOPS en la Nube de Capacitación Usach. AWS Fan!

Diego Cáceres Solís
Instructor CCNA Cyber Ops, Certificado Linux Essentials, Máster en Dirección de Ciberseguridad, Hacking Ético y Seguridad Ofensiva. Destacado Docente en asignaturas de Hardware de Computadores, Aplicaciones Computacionales, Informática aplicada a las TC, Administración de Servidores Linux, Windows, Programación Web (Html, CSS, JS, Java) y Programación Computacional (Java, Python, Mathlab), Academia Politécnica Naval.

Juan Pablo López Maluenda
Socio y Director Ciberlegal LION - Universidad Gabriela Mistral - Licenciado en Ciencias Jurídicas, Derecho de los Negocios, Civil, Comercial, Judicial, Litigios. Universidad de Chile - Diplomado de Postítulo en Ciberseguridad, Derecho Informático y Nuevas Tecnologías. Universidad Adolfo Ibáñez Curso Formando Directores de Empresas, Corporativo

WHILOSOC
REVISTA DIGITAL N° 2
Abril 2022

Opiniones y sugerencias al correo
whilosoc@protonmail.com
www.linkedin.com/in/whilosoc
https://whilosoc.cl/

Sebastián Vargas Yáñez
Presidente SOCHISI

SOCHISI
SOCIEDAD CHILENA DE SEGURIDAD DE LA INFORMACIÓN

Carlos Montoya Morales
Presidente WHILOLAB

WHILOLAB

EQUIPO Editorial

REVISTA WHILOSOC

Rosa Fuentes Valdebenito
Ingeniera en Computación e Informática
Magíster de Ingeniería en Seguridad de la Información
Colaboradora Whilosoc

Lidia Herrera Mateluna
Ingeniera en Sistemas de Información
Magíster en Diseño Instruccional
Colaboradora Whilosoc

Margarita Vargas Martínez
Ingeniero Civil Industrial | Ingeniero en Informática
Diplomada en Ciberseguridad
Colaboradora Whilosoc

Rodrigo Pérez Silva
Ingeniero Ejecución en Informática
Diplomado en Seguridad de la Información
Colaboradora Whilosoc

Mauricio Hernández Moraga
Ingeniero Ejecución en Informática
Colaborador Whilosoc

Juan Carvajal Fernández
Magíster en Innovación Educativa
Diseñador Revista